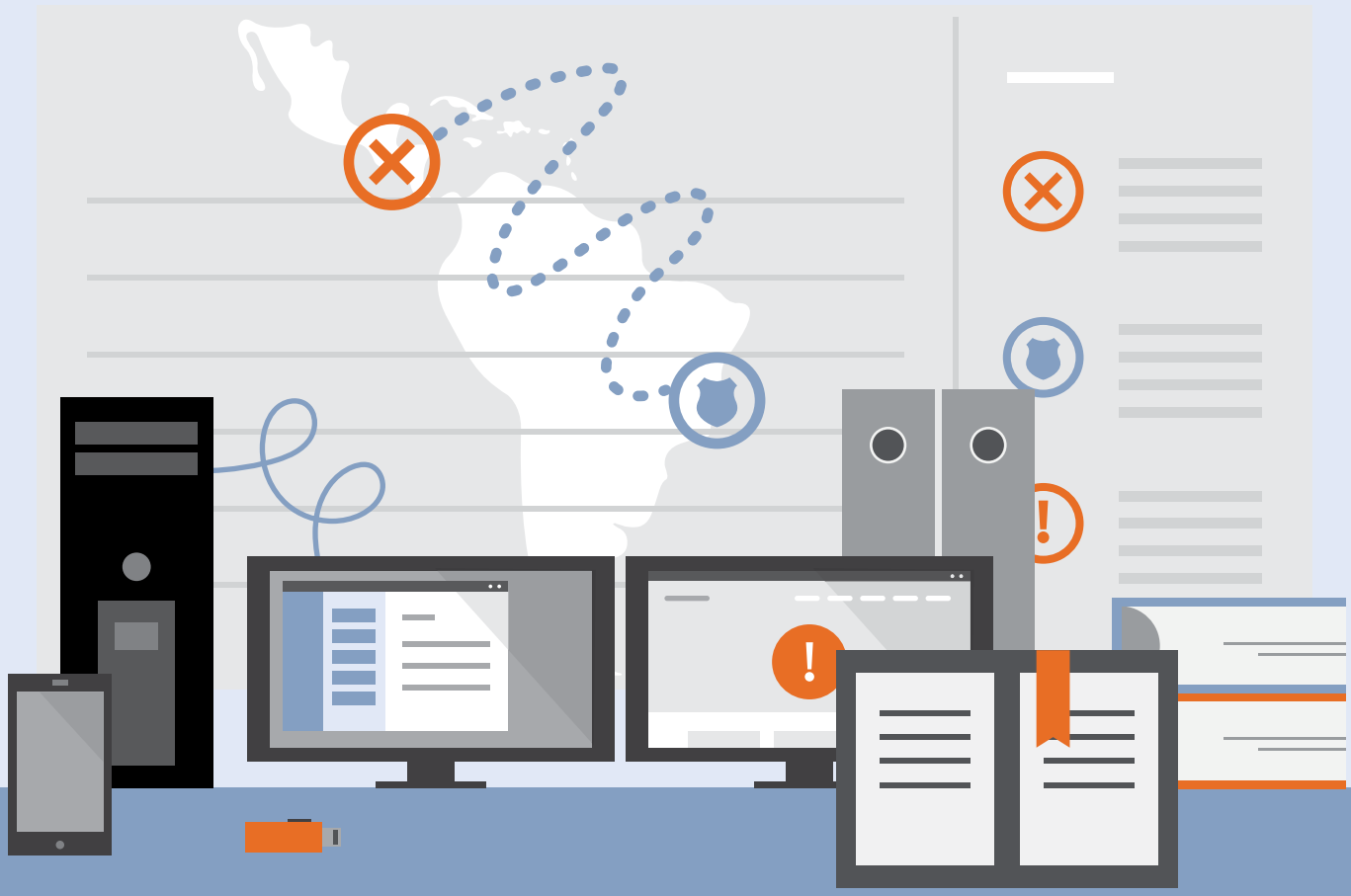
# Buenas Prácticas
## para establecer un CSIRT nacional



Organización de los Estados Americanos | Más derechos para más gente

La Organización de los Estados Americanos (OEA) es el principal foro político de la región, que promueve y apoya la democracia, los derechos humanos, la seguridad multidimensional y el desarrollo integral en las Américas. La OEA busca prevenir conflictos y lograr la estabilidad política, la inclusión social y la prosperidad de la región por medio del diálogo y de la acción colectiva, como la cooperación, la implementación de mecanismos de seguimiento de los compromisos de los Estados miembros y la aplicación de la Ley Interamericana y de la Ley Internacional.

Esta guía fue creada gracias al apoyo financiero del Gobierno de Canadá.



**Aviso importante**

El contenido de esta publicación no refleja necesariamente las opiniones o políticas de la OEA, de sus Estados miembros ni de las organizaciones colaboradoras. Esta guía ha sido puesta a consideración de diferentes expertos internacionales en seguridad cibernética y miembros de la Red Hemisférica de CSIRT de la OEA; y está sujeta a actualizaciones periódicas.

Este documento es una iniciativa del Programa de Seguridad Cibernética de la OEA, que cuenta con el apoyo financiero de los gobiernos de Canadá, el Reino Unido y los Estados Unidos de América.

Abril de 2016

1889 F Street, N.W., Washington, D.C., 20006
Estados Unidos de América
www.oas.org/cyber/

# Buenas prácticas
## para establecer un CSIRT nacional

Organización de los Estados Americanos | Más derechos para más gente

Un equipo de respuesta a incidentes en seguridad informática (CSIRT por sus siglas en inglés) es una organización cuyo propósito principal consiste en brindar servicios de respuesta a incidentes de seguridad informática a una comunidad en particular.

En esta guía se analizan varios tipos de CSIRT, entre ellos los CSIRT a nivel nacional, que responden a incidentes en seguridad informática a nivel de un estado-país.

El presente documento analiza el proceso de gestión de un proyecto para la creación y la puesta en marcha de un CSIRT nacional, incluidos distintos criterios y consideraciones necesarias para definir su constitución, misión, visión, alcance, servicios, tiempos, y aspectos legales e institucionales u organizacionales. Esto incluye un examen de los requerimientos de recursos humanos, tanto en términos de contratación como de formación continua, que son necesarios para establecer el personal de un equipo nacional de respuesta a incidentes.

Asimismo, la guía presenta descripciones detalladas de infraestructura, que incluye hardware, software y procedimientos técnicos.

Finalmente, se analizan diferentes políticas y procedimientos necesarios para realizar una operación fluida CSIRT. En este sentido, la guía revisa y subraya marcos existentes de CSIRT, como aquellos desarrollados por la European Union Agency for Network and Information Security[01] (ENISA) y GÉANT. También se analizan directrices para la adhesión y la participación en determinados organismos internacionales, como el Foro de Equipos de Respuesta a Incidentes y de Seguridad (FIRST).

# Contenido


Forma de uso de esta guía

## 1 PLANIFICACIÓN

**Definición** 12

Ámbitos de actuación de los CSIRT 14
El papel de un CSIRT nacional 16
Partes interesadas 17

**Constitución** 28

Documento de constitución 29
Marco institucional 34
Marco legal

**Alcance** 38

Comunidad objetivo 39
Servicios 41
Servicios reactivos 42
Servicios proactivos 43
Servicios de valor agregado 44
Evolución de los servicios de un CSIRT 44

**Organización y RRHH** 45

Estructuras organizacionales 46
Tamaño de la organización 47
Funciones y responsabilidades 48
Estructura organizacional 50
Tamaño y cantidad de recursos 56

Cronograma 58

Conclusión de la planificación preliminar 62

## 2 EJECUCIÓN

**Selección de recursos humanos** 66

Dirección 68
Operaciones 68
Investigación y Desarrollo 69
Tecnología de Información 69

**Requisitos de formación** 70

Seguridad cibernética general 72
Capacitación en respuesta a incidentes en seguridad cibernética 72
Cursos de análisis de *malware* y forense 73

**Instalaciones e infraestructura TI** 74

Instalaciones CSIRT 75
Diseño básico de la red CSIRT 77
Equipo básico sugerido 78

**Políticas y procedimientos operacionales** 80

Políticas mínimas obligatorias 81
Otras políticas 81

## 3 CIERRE

Finalización formal de las actividades 85

## ANEXOS

**Muestra de la política de uso aceptable** 88
**Política de divulgación** 90
**Formatos de respuesta a incidentes** 92
**Referencias citadas** 103


# Forma de uso de esta guía

Esta guía analiza varios tipos de CSIRT, entre ellos los CSIRT a nivel nacional, que responden a incidentes a nivel estado-nación. Por lo general, estos monitorean y responden a incidentes en las redes gubernamentales y también sirven como un coordinador de seguridad de la información para el sector privado u otros sectores e instituciones. Y pueden o no prestar servicios de respuesta a incidentes a usuarios finales o al sector privado.

Todos los aspectos relacionados con los CSIRT, similares a la seguridad de la información en sí misma, requieren del amplio entendimiento de una serie de diferentes disciplinas, aparte de la tecnología. También incluyen temas adicionales como la gestión de recursos humanos, los procesos legales, la planificación financiera, las adquisiciones y muchas otras. La supervisión y la gestión de proyectos son particularmente importantes en la creación y el despliegue de los CSIRT, ya que necesitan funcionar de una manera estructurada, gradual y estratégica durante las fases de planificación, que requiere la colaboración entre los diversos grupos de interés.

En esencia, la presente es una guía para la creación de un CSIRT nacional en la gestión de un proyecto. Está destinada específicamente a que el gerente de proyecto la utilice como ayuda y referencia en todo el proceso de implementación. Se divide en tres secciones principales: planificación, ejecución y cierre, que describen los principales objetivos y los resultados de cada fase y presentan materiales de apoyo en el proceso. Sin embargo, como se muestra en cada capítulo, los gerentes de proyectos deben crear un equipo multidisciplinario para ayudar en todas las partes del proceso en que se requiere especialización.

Cada país tiene una estructura política, una cultura, una geografía, un marco jurídico y recursos diferentes. En virtud de lo anterior, esta guía no pretende establecerse como una plantilla definitiva, sino más bien como un documento que pueda adaptarse a las condiciones locales, cuando sea necesario.

# 1 PLANIFICACIÓN

# A Definición

## ¿Qué es un CSIRT?

Tradicionalmente se define un CSIRT como un equipo o una entidad dentro de un organismo que ofrece servicios y soporte a un grupo en particular [02] (comunidad objetivo) con la finalidad de prevenir, gestionar y responder a incidentes de seguridad de la información. Estos equipos suelen estar conformados por especialistas multidisciplinarios que actúan según procedimientos y políticas predefinidas, de manera que respondan, en forma rápida y efectiva, a incidentes de seguridad, además de coadyuvar a mitigar el riesgo de los ataques cibernéticos.

Con el paso del tiempo, el concepto de CSIRT evolucionó para lograr satisfacer el aumento de servicios requeridos por la comunidad. Los primeros equipos prestaban servicios para responder a ataques e incidentes básicos, pero más recientemente algunos CSIRT se han propuesto seguirles el paso a unos adversarios más grandes y más nebulosos, ofreciendo asesoramiento en el análisis de riesgos, los planes de continuidad de negocio, el análisis de *malware* y muchas otras áreas. A la hora de ampliar la oferta de servicios de un CSIRT, ENISA recomienda incluir el análisis forense y la gestión de vulnerabilidades. Nuevamente, el nivel y el tipo de servicios que se ofrecen serán diferentes en función de a quién servirá el CSIRT y cuáles serán sus mandatos.

Los equipos que surgieron principalmente para responder a incidentes han evolucionado y ahora con frecuencia están orientados a ser un modelo integral de gestión de seguridad de la información. En efecto, mientras que el alcance de los CSIRT se limitaba en gran medida a prestar servicios de “respuesta”, hoy en día cada vez más adoptan una postura proactiva. Se centran en la prevención y en la detección de incidentes, lo que logran por medio de una mezcla de habilidades y formación de la conciencia, alertas y monitoreo, así como de la difusión de información relacionada con seguridad de la información, el desarrollo de planes de continuidad de negocio, y el desarrollo de documentos de mejores prácticas y de análisis de vulnerabilidades, entre otros.

# Ámbitos de actuación de los CSIRT

Existen centenas de CSIRT en el mundo que varían en su misión y en su alcance. Una de las maneras más importantes de clasificar a los CSIRT es agruparlos por la comunidad o por el sector al que le prestan servicios. A continuación se presentan algunos de los principales tipos de CSIRT que se encuentran operando:

### CSIRT ACADÉMICOS

Estos equipos de respuesta atienden comunidades académicas, universidades, facultades, escuelas o institutos. Su tamaño y sus instalaciones pueden variar en función de la comunidad y frecuentemente aúnan esfuerzos con otros CSIRT académicos y se pueden especializar en investigaciones.

### CSIRT COMERCIALES

Por diversas razones, incluyendo limitaciones de recursos humanos o muchas otras, algunas empresas optan por externalizar los servicios de CSIRT en lugar de internamente crear y gestionar las funciones de respuesta a incidentes. Esto ha dado lugar a un mercado robusto para CSIRT comerciales, que ofrecen servicios pagos de respuesta a incidentes para clientes. La relación entre un CSIRT comercial y su cliente a menudo se rige por acuerdos de nivel de servicio (SLA por sus siglas en inglés), que son necesarios para establecer lineamientos de respuesta a incidentes y asegurar que la información se maneja de acuerdo a las necesidades del cliente.

### CSIRT DE INFRAESTRUCTURAS CRÍTICAS

En algunos casos, hay CSIRT establecidos específicamente para la protección de los activos de información críticos y la infraestructura crítica de la nación, sin importar si es operado por el sector público o privado, o para la administración de transporte, la generación de energía, las comunicaciones u otros procesos. Dado que las instituciones que dependen de este tipo de CSIRT pueden pertenecer a más de una comunidad (por ejemplo, tanto militar como de infraestructura crítica), es vital establecer protocolos de interacción con otros equipos involucrados.

### CSIRT GUBERNAMENTALES

Los CSIRT gubernamentales sirven a las instituciones del Estado con el fin de garantizar que la infraestructura de TI del gobierno y los servicios que les ofrecen a los ciudadanos tengan niveles de seguridad adecuados. Los CSIRT gubernamentales adaptan sus estructuras al gobierno. Pueden satisfacer las necesidades de las comunidades de los gobiernos locales o regionales, o comunidades específicas de los sectores. Los CSIRT gubernamentales pueden funcionar de manera independiente o interactuar para combinar estrategias y esfuerzos y compartir recursos y conocimientos. Al interior de un país, por ejemplo, el Ministerio de Educación y el Ministerio de Turismo podrían operar CSIRT independientes y también colaborar regularmente y compartir información.

### CSIRT NACIONALES

Además de servir a una comunidad definida, el CSIRT de un país por lo general asume el papel de coordinador nacional de respuesta a incidentes y es el punto de contacto[03] para incidentes nacionales e internacionales. La función y la comunidad objetivo de un CSIRT nacional varía en función de sus roles y de la existencia de otros centros de respuesta. Por ejemplo, si no hay un CSIRT designado para infraestructura crítica, el CSIRT nacional podría asumir responsabilidades normalmente asignadas a un equipo de respuesta de infraestructura crítica. Se puede considerar un "CSIRT de último recurso", o uno que se encarga de los asuntos de respuesta a incidentes que no están bajo la supervisión de otra entidad[04]. Es muy común que varios CSIRT sean parte de la comunidad a la que sirve el CSIRT nacional.

### CSIRT DEL SECTOR MILITAR

Esos CSIRT proporcionan servicios a las instituciones militares de un país. Sus actividades se limitan generalmente a la defensa o a las capacidades cibernéticas ofensivas de una nación. Además de las tecnologías de respuesta a incidentes normales, a menudo tienen conocimiento específico de las TIC para uso militar, incluyendo, por ejemplo, armamento y sistemas de radares.

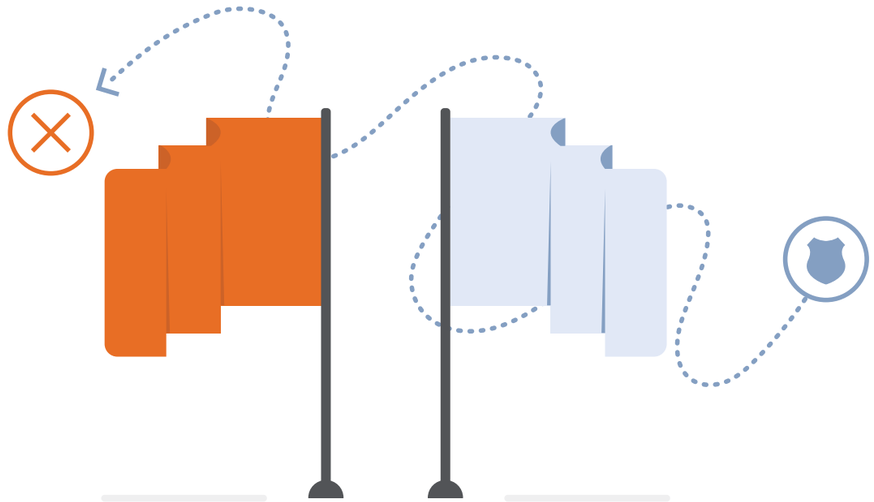
### CSIRT DE PROVEEDORES

Son CSIRT que prestan servicios relacionados con productos específicos de un fabricante, desarrollador o proveedor de servicios. El propósito de este tipo de CSIRT es mitigar el impacto de las vulnerabilidades o problemas de seguridad relacionados con sus productos. Los ejemplos incluyen HP CSIRT (Hewlett Packard), Banelco CSIRT (Banelco Bank), o Adobe PSIRT (Adobe) entre otros.

### CSIRT DEL SECTOR DE PEQUEÑAS Y MEDIANAS EMPRESAS (PYME)

Su tamaño y su naturaleza a menudo no les permiten a las PYME implementar equipos de respuesta a incidentes individuales. Por lo tanto, hay una necesidad de crear CSIRT que entiendan y respondan a las necesidades de esta comunidad de negocios; por ejemplo, en España se encuentra el INTECO-CERT Corporation, que se centra en ayudar a las PYME y a los ciudadanos.

# El papel de un CSIRT nacional



Un CSIRT se compone de personas cuyo trabajo es prevenir y responder a incidentes de seguridad informática. Por supuesto, el nivel y el tipo de respuesta efectuada por un CSIRT particular dependerán de muchos factores.

Una analogía frecuentemente referenciada, propuesta inicialmente por la Universidad Carnegie Mellon, presenta una comparación entre los CSIRT y un cuerpo de bomberos. Según lo explicado por el Manual de CSIRT de CMU, de la misma manera que un equipo de bomberos responde a una emergencia de incendio, un CSIRT debe responder y gestionar la solución a un incidente informático. Aún más, la analogía señala que además de sus funciones de respuesta, los bomberos realizan actividades como educación, análisis de riesgos o promoción de regulaciones, actividades preventivas que los CSIRT también llevan a cabo. Por último, los bomberos suelen investigar cómo y por qué ocurrió un incendio con el fin de evitar que suceda de nuevo, que es una función realizada por casi todos los CSIRT, independientemente de su clasificación.

Como se mencionó anteriormente, un CSIRT puede tener diferentes formas de organización: puede ser una institución independiente, privada o pública, un departamento de otra organización o simplemente un grupo de personas distribuidas en diferentes organizaciones.

Cada CSIRT define cómo desarrollará sus actividades. Puede que tenga que trasladarse a la escena de un incidente para realizar una respuesta, o de lo contrario puede supervisar de forma remota la gestión de incidencias mediante la coordinación con las partes interesadas.

Como se ha descrito anteriormente, un CSIRT nacional actúa como punto de encuentro a nivel internacional de un país. Por ejemplo, si un CSIRT del país "A" detecta un tráfico malicioso procedente de un banco en el país "B", le enviará una comunicación al CSIRT nacional del país "B", que luego adelantaría directamente las gestiones para abordar la fuente del tráfico malicioso y así resolver el problema. En este ejemplo, también es importante tener en cuenta que, además de la recepción de la solicitud por parte del CSIRT "A", el CSIRT "B" coordinaría el proceso de respuesta a incidentes que debería realizarse en el interior de sus propias partes interesadas. Estas son funciones de suma importancia en un CSIRT nacional: actuar como punto de contacto del país a nivel internacional en materia de seguridad cibernética y coordinar y llevar a cabo actividades de respuesta a incidentes de seguridad informática a nivel nacional.

Al establecer un CSIRT, los funcionarios a menudo se centran únicamente en las capacidades de respuesta a incidentes técnicos en lugar de contemplar asuntos más generales de la organización. Para asegurar que se aborden ambos objetivos principales de los CSIRT nacionales, una parte importante de esta guía se dedica a la planificación y al desarrollo de un modelo para un CSIRT nacional.

# Partes interesadas

| Entrada | Herramientas | Salida |
|---|---|---|
| - Equipo de proyecto | - Tormenta de ideas<br>- Mapas mentales<br>- Análisis de partes interesadas | - Listado de partes interesadas y sus roles, su interés, el soporte y la influencia en el proyecto |

Para planificar la creación de un CSIRT nacional, el primer paso que debe dar el equipo consiste en identificar a las partes interesadas.

Como se explicó anteriormente, el principal rol de un CSIRT nacional es coordinar a las partes interesadas del país en actividades de respuesta a incidentes de ciberseguridad. Por este motivo, es fundamental que se identifiquen claramente quiénes son las partes interesadas.

Las partes interesadas son las personas o las organizaciones que se verán afectadas de alguna manera por la implementación de un CISRT nacional. Estas partes tendrán diferentes niveles de interés en el proyecto, un determinado rol en el ciclo de vida del CSIRT nacional y un determinado nivel de poder sobre la ejecución del proyecto y el funcionamiento del CSIRT.

Una vez identificadas las partes interesadas, se pueden clasificar según su rol, su responsabilidad y su interés hacia la iniciativa del CSIRT. Con esto se trazará una estrategia para comprometerse con ellas y gestionarlas.

Aunque se puedan identificar otros, las principales partes interesadas[05] en actividades de seguridad cibernética son:

**Las partes interesadas son las personas o las organizaciones que se verán afectadas de alguna manera por la implementación de un CISRT nacional.**

## Poder Ejecutivo del Estado

El gobierno participa como parte interesada en varios papeles. Procesa información altamente sensible para el país: de sus ciudadanos y de los sectores de seguridad pública (finanzas, defensa, salud y educación, entre otros). Debido a la importancia de la información que maneja, el gobierno necesita mantener sus sistemas seguros y suele ser el principal "cliente" de un CSIRT nacional ya que puede ser víctima de un ataque que tendría consecuencias potencialmente graves.

Igualmente, los gobiernos son responsables de la regulación y de la generación de leyes, normas y otras iniciativas de importancia nacional. En este sentido, el gobierno es un instrumento muy importante para las actividades de regulación para la prevención de incidentes de seguridad cibernética. El gobierno tiene la responsabilidad de determinar los niveles de riesgo aceptables en los sectores antes mencionados, incluyendo los relacionados con incidentes informáticos. Así, el gobierno actúa tanto a la manera de un patrocinador como de un promotor CSIRT.

## Poder Legislativo del Estado

Además de ser un cliente –en el sentido de que el CSIRT nacional puede proteger sus redes y su información–, la legislatura crea leyes que promueven la seguridad de la información, establece límites para un CSIRT y es también un socio estratégico clave.

## Poder Judicial del Estado

Además de fortalecer los aspectos legales de la criminalización de los delitos cibernéticos, las instituciones judiciales proporcionan claridad en las áreas de la ley que puedan afectar a las operaciones del CSIRT. En este sentido, es una parte interesada clave.

## Fuerzas del orden

Las fuerzas del orden deben garantizar que se implemente la legislación sobre delincuencia cibernética en un país. La Policía realiza investigaciones sobre delitos cibernéticos y a menudo hace el enlace con un CSIRT nacional en este sentido. Pueden proporcionar información valiosa sobre actividad cibernética maliciosa y cooperar con los organismos policiales de otros países. Los organismos encargados de hacer cumplir la ley a menudo cuentan con una unidad de delito cibernético especializado con los procedimientos y las herramientas necesarias para obtener pruebas de ataques cibernéticos.

## Ministerio de Defensa

En muchos países, el Ministerio de Defensa administra la información valiosa o sensible del país. Además, supervisa los asuntos de defensa cibernética, lo que lo convierte en un socio clave en las operaciones del CSIRT y la respuesta a incidentes.

## Academia

La comunidad académica tiene mucho que aportarle a un CSIRT. Por un lado, a menudo es el sector de facto que encabeza los esfuerzos para el desarrollo de recursos humanos y la capacitación de jóvenes en distintas facetas de la información y seguridad informática. También puede realizar investigaciones en las mismas áreas. Es un socio clave en todo el ciclo de vida de un CSIRT nacional.

## Proveedores de servicios de Internet

Los Proveedores de Servicios de Internet (ISP por sus siglas en inglés) les permiten a los gobiernos, las empresas y los ciudadanos conectarse y utilizar Internet. Como tales, tienen una amplia gama de responsabilidades relacionadas con el uso de esta red y el alojamiento web. Son activos críticos en el mantenimiento de la seguridad de la información y la respuesta a los incidentes de seguridad cibernética. La cooperación de los ISP es clave para el funcionamiento del CSIRT, especialmente cuando se necesita hacerles modificaciones a las redes de Internet, tener planes de contingencia o identificar amenazas y vulnerabilidades.

## Sector privado

El sector privado participa desde dos puntos de vista. Por un lado, están las empresas privadas que operan en sectores críticos para el Estado. Su compromiso tendría consecuencias negativas para la economía, la seguridad pública o la seguridad nacional. Por otro lado, están las muchas empresas que fabrican y desarrollan tecnologías utilizadas en TI y seguridad de la información. Las empresas que operan infraestructuras críticas serán los clientes clave, a menudo convirtiéndose en socios de confianza con los que se coordinará estrechamente la respuesta a incidentes. Mientras tanto, los fabricantes de tecnología colaboran en la formación, el soporte, las actualizaciones y los parches de vulnerabilidad. En ambos casos, es esencial la interacción con ellos.

## Sector financiero

Se puede subdividir el sector financiero en varios subgrupos, entre ellos: bancos, bancos centrales (o reguladores), casas de bolsa y de cambio. Cada uno de estos sectores tiene requisitos particulares, como socios, clientes, e incluso patrocinadores.

## Sociedad civil

La sociedad civil incluye asociaciones profesionales, organizaciones sin ánimo de lucro y grupos de usuarios, entre otros. Estos grupos reunirán a perfiles específicos de técnicos y profesionales y también proporcionarán formación y orientación; y pueden ayudar con los esfuerzos de sensibilización. A menudo son socios estratégicos influyentes.

## Grupos especializados nacionales e internacionales

Pueden existir grupos especializados como CSIRT particulares o específicos a nivel local e internacional, en foros internacionales, como el Foro de Equipos de Respuesta a Incidentes y de Seguridad (FIRST), o en organizaciones multilaterales que realizan actividades de seguridad cibernética, como la OEA.

Todos los interesados desempeñarán papeles ligeramente diferentes en la creación, el desarrollo y la operación de un CSIRT nacional. Se pueden agrupar más o menos en función de sus contribuciones:

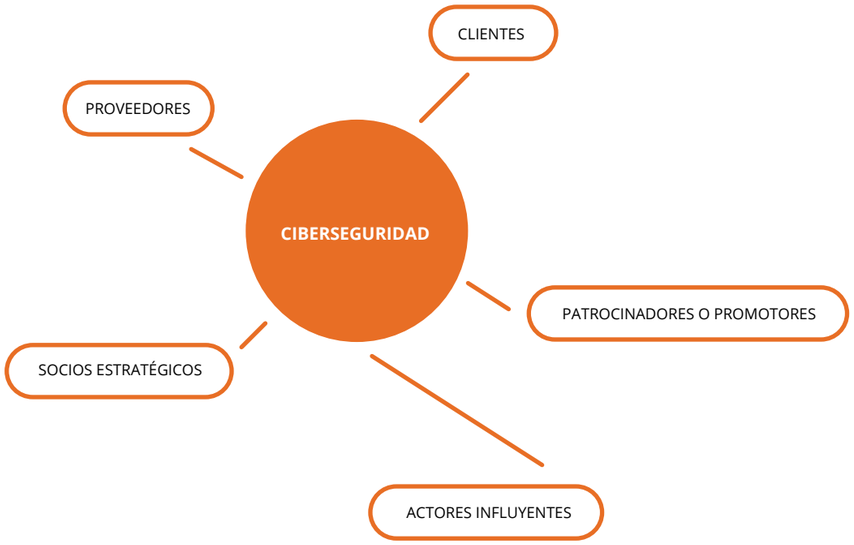
**Patrocinadores o promotores**
Personas u organizaciones que promueven la existencia de un CSIRT nacional y lo apoyarán política y económicamente.

**Clientes**
Organizaciones que utilizarán los servicios del CSIRT nacional.

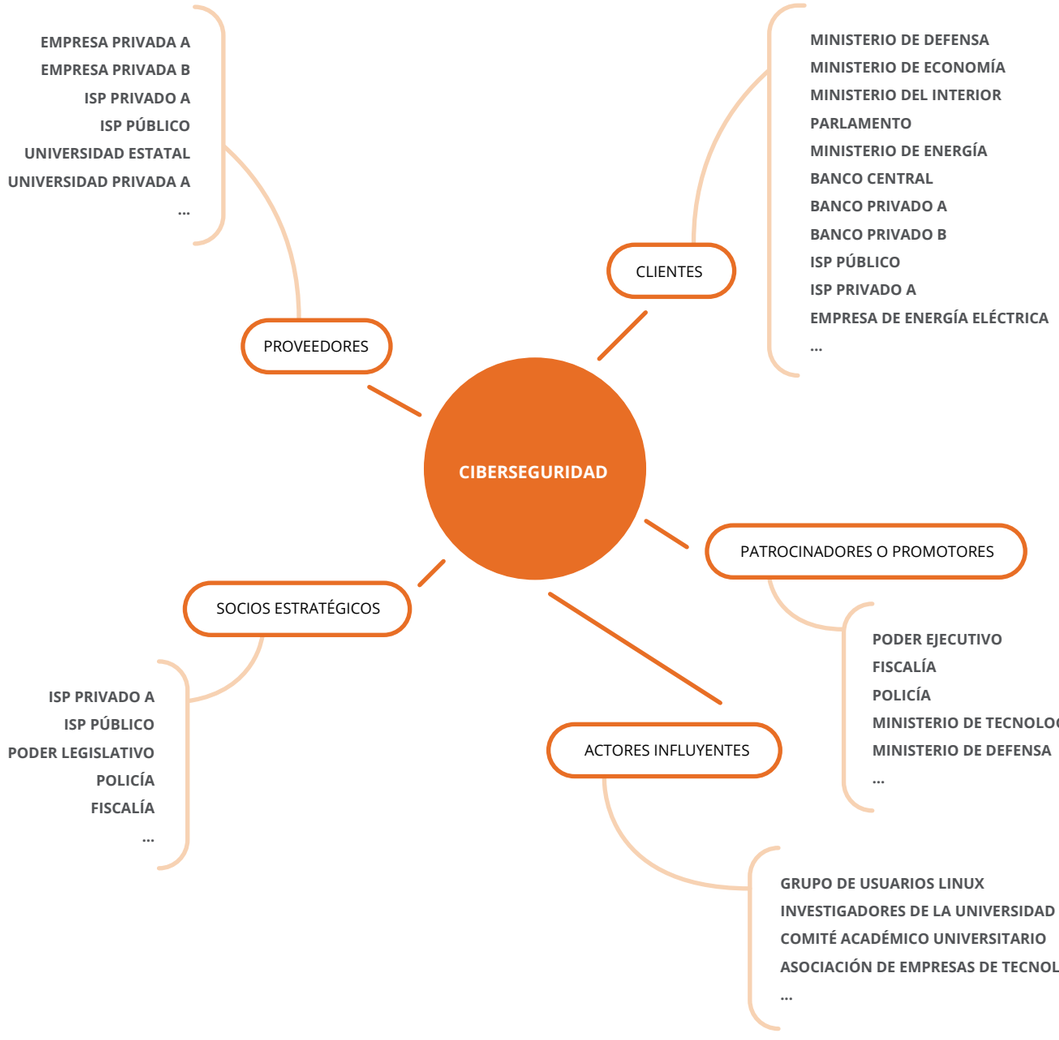
**Proveedores**
Organizaciones que ofrecen productos o servicios al CSIRT nacional, tales como herramientas, servicios profesionales, formación, etcétera.

**Socios estratégicos**
Personal u organizaciones que son estratégicos para el buen desarrollo del CSIRT. En general, estos aliados ejecutan actividades de interés para el CSIRT que este no puede realizar por sí solo. Un ejemplo podría ser el mundo académico o los reguladores de sectores específicos.

**Influyentes**




Es importante identificar el papel de cada parte interesada, teniendo en cuenta que esto definirá el modo en que un CSIRT la involucrará. La relación entre el CSIRT y cada uno de sus grupos de interés será diferente y por lo tanto implicará un estilo distinto de interacción. Por ejemplo, la colaboración con un ISP o con una fuerza del orden probablemente se guiará por contratos o acuerdos oficiales. Las asociaciones con instituciones de la sociedad civil o del gobierno, por otro lado, pueden ser más informales, aunque no menos importantes.

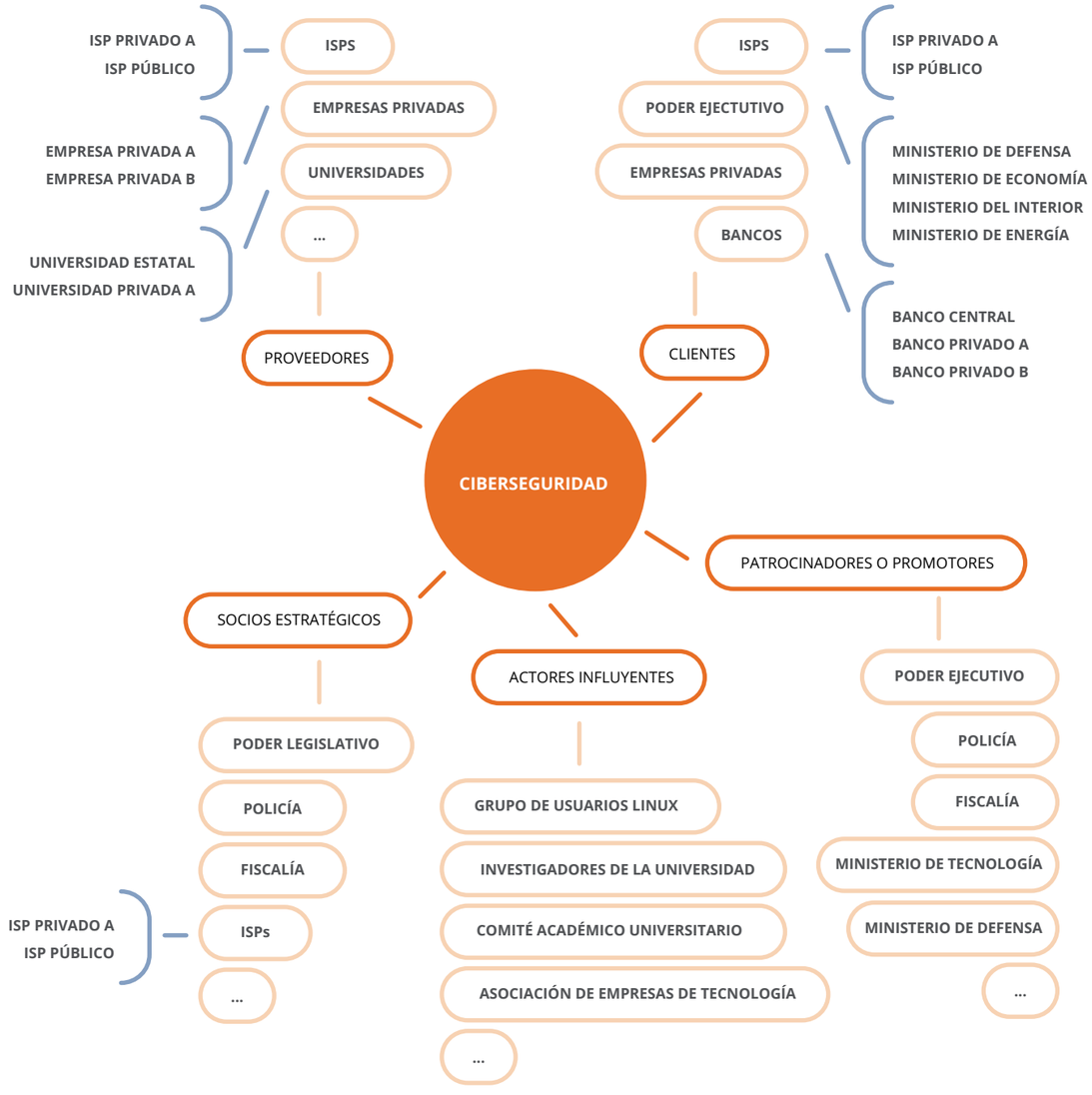



## Metodología para identificar a las partes interesadas

Para identificar a las partes interesadas, el gerente del proyecto CSIRT deberá conformar un pequeño equipo que represente una variedad de intereses y de organizaciones. Lo anterior asegurará que haya múltiples perspectivas y especializaciones en el proceso de selección y participación de los interesados. Si es posible, en un esfuerzo por preservar la objetividad, debe haber al menos una persona del equipo que sea más neutral, o no necesariamente una parte de la comunidad de interesados. El proceso mismo de definir las partes interesadas debe consistir en una sesión preliminar de lluvia de ideas seguida de entrevistas informativas.

Como se explicó anteriormente, los interesados pueden agruparse de acuerdo con el papel que van a desempeñar. El primer paso es hacer una lista de los diferentes grupos. Se pueden utilizar mapas mentales como una herramienta para ordenar esta información, lo que ayudará al equipo del proyecto a visualizar la información fácilmente.

Los diagramas de abajo muestran la estructura inicial de un mapa mental para comenzar la lluvia de ideas y la identificación de las partes interesadas.




Una vez que se definen los grupos, una lluvia de ideas ayuda a categorizar los actores nominados en cada grupo.

El diagrama anterior muestra un ejemplo de un mapa mental en la mitad del proceso de organización.

Como se ve en el diagrama, una parte interesada puede ocupar varias funciones simultáneamente. Esta situación suele presentarse tanto dentro del gobierno como en el sector privado, la academia y la sociedad civil. El ejemplo más claro de esto se observa en el interior de un ISP y el gobierno. Estos grupos son socios estratégicos sin los cuales sería casi imposible establecer y operar un CSIRT nacional. Al mismo tiempo, son los destinatarios de servicios CSIRT ya que pueden convertirse en víctimas de un incidente de seguridad cibernética o ataque cibernético. Las agrupaciones pueden dividirse a su vez en subgrupos, como se ve a continuación:

Por último, se generará una lista de las partes interesadas y sus roles en un documento formal.

Esta lista deberá contener cada uno de los grupos involucrados, la justificación de su participación en el proyecto CSIRT y un punto de contacto de designación oficial.

## Entrevistas con las partes interesadas

Una vez preparada la lista de los actores, roles y subgrupos, habrá reuniones con cada uno de los subgrupos con el fin de acercarse a ellos y entender mejor sus necesidades, lo que esperan del CSIRT nacional y en general cuál es su postura en cuanto a seguridad cibernética. Las reuniones individuales con cada subgrupo ofrecen un ambiente idóneo para el intercambio de opiniones y permiten la transparencia durante el proceso de creación.

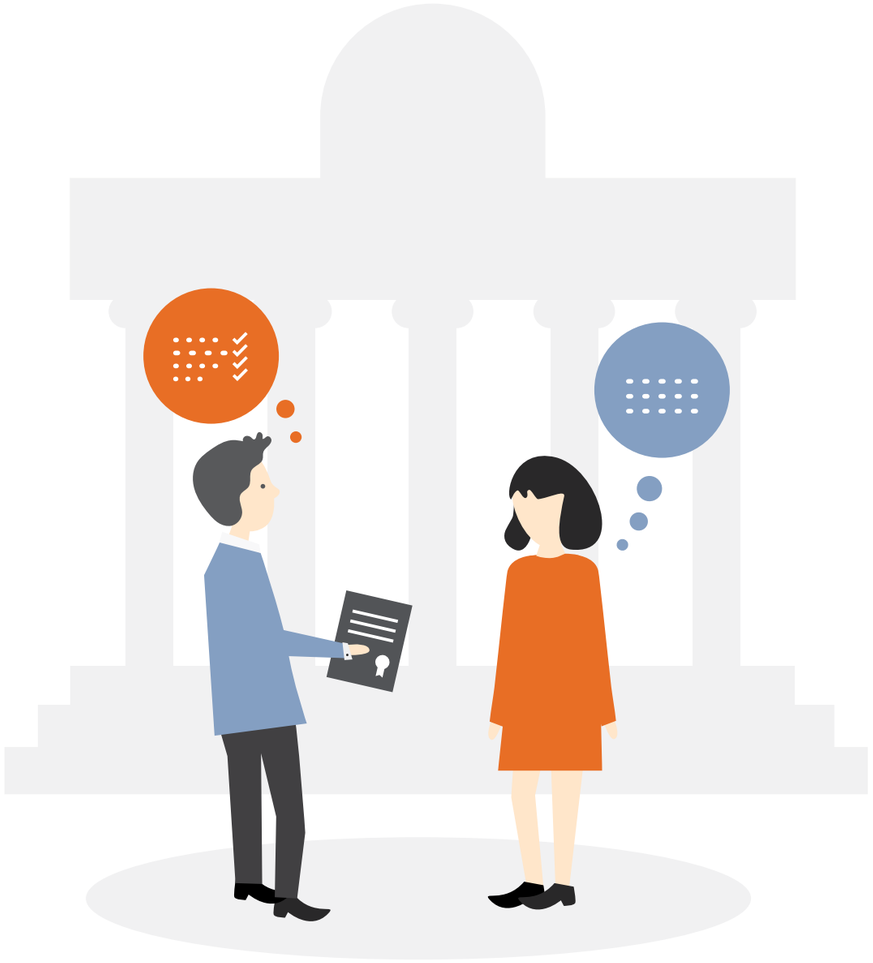
Durante estas entrevistas, es importante presentarles el tema de los CSIRT a las partes interesadas, ya que muchos de ellos no tienen experiencia al respecto, sobre todo en función del público y el nivel general de desarrollo de la seguridad cibernética dentro de un país y del gobierno. El director del proyecto y el equipo CSIRT deben preparar preguntas para ayudar a los interesados a establecer su posición, tales como:

Después de realizar las sesiones de discusión, el equipo del proyecto podría distribuir un cuestionario para que las partes interesadas contribuyan.

**Las reuniones individuales con cada subgrupo ofrecen un ambiente idóneo para el intercambio de opiniones y permiten la transparencia durante el proceso de creación.**

La información se analizaría después de las discusiones y la recogida de las encuestas, lo que le permitirá al equipo del proyecto crear un mapa más robusto y claro de las partes interesadas. Todo este proceso se podría repetir para asegurar que todos los actores estén comprometidos y el mapa de funciones y responsabilidades de las instituciones colaboradoras esté completo y preciso.

- ¿Siente que hay una necesidad de crear un CSIRT nacional? ¿Por qué?
- ¿Cuál debería ser el papel de un CSIRT nacional?
- ¿Qué servicios debería proporcionar un CSIRT nacional?
- ¿Hay alguna área en particular de gobierno donde se deba ubicar el CSIRT nacional?
- ¿Cómo beneficiaría potencialmente un CSIRT nacional a su organización?
- ¿Para su organización, cómo podría valorar el trabajar con un CSIRT nacional? ¿Se regiría la relación por medio de un contrato, Acuerdo de Confidencialidad (NDA), Acuerdo de Nivel de Servicio (SLA), o algún otro medio?
- ¿Su organización está dispuesta a cooperar activamente con un CSIRT nacional? ¿Cuáles son los límites de la cooperación?
- ¿Qué otras organizaciones o individuos cree usted que deberían participar?



# Análisis de las partes interesadas

Del análisis de las partes interesadas en la implementación del CSIRT nacional, surgirá una imagen que mostrará el nivel de interés de cada actor en el proyecto y cómo cada uno tiene la capacidad de influir en el desarrollo del equipo de respuesta. Los resultados del análisis producirán directrices que describen la forma más adecuada para gestionar el proyecto y sus socios para obtener mejores resultados.

Hay dos métodos populares para la clasificación. El primero consiste en establecer una escala del nivel de apoyo para el proyecto de la parte interesada, basado en las entrevistas, por ejemplo, mediante la definición de tres niveles simples de apoyo: se opone a la iniciativa; es neutral; o apoya la iniciativa.

El segundo método consiste en establecer un mapa de cuadrantes en que la parte interesada en cuestión será clasificada de acuerdo con el nivel de interés en el proyecto y el nivel de influencia que tiene sobre este.

Una vez que las partes interesadas se encuentran en sus respectivos cuadrantes, habrá un mapa claro de cómo gestionar a cada uno con eficacia. En este punto hay un mapa con los interesados identificados, su interés en el proyecto, su actitud hacia dar apoyo a la iniciativa, ya sea buena o mala, y su nivel de influencia. Las partes interesadas pueden ser gestionadas usando los diagramas precedentes.[06]

Una vez que el proceso de identificación y análisis de las partes interesadas ha terminado, usted tendrá una lista estructurada de todas las partes interesadas, de sus respectivas funciones, niveles de interés en el proyecto, y su actitud hacia ella, así como cada una de sus capacidades para influir en el CSIRT. En última instancia, esta información será útil para permitir que el equipo del proyecto identifique las fuentes de asistencia, financiación, asesoramiento o cualquier otro elemento beneficioso para el desarrollo del CSIRT. Al mismo tiempo, se revelarán los potenciales "clientes insatisfechos" o instituciones que podrían complicar las actividades del CSIRT.

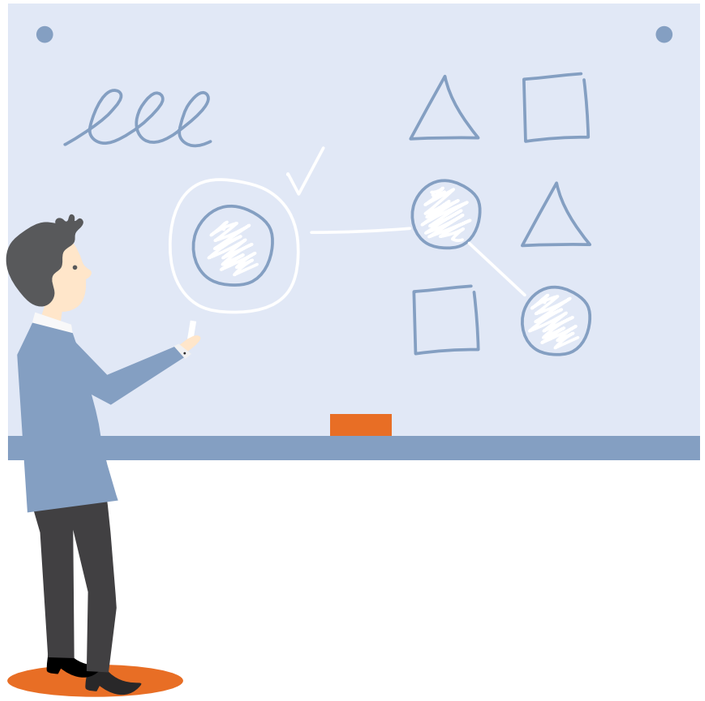
# B Constitución

Luego de identificar a las partes interesadas, el equipo de proyecto deberá generar la documentación necesaria para constituir el CSIRT nacional.

En esta sección se creará un documento de constitución del CSIRT nacional, en el que se definirán su misión, su visión, su marco institucional y su marco legal.

| Entrada | Herramientas | Salida |
|---|---|---|
| - Equipo del proyecto<br>- Documento de involucrados | - Mesas de trabajo moderadas<br>- Consultas a expertos | - Documento de constitución<br>- Misión y visión<br>- Marco institucional<br>- Marco legal |

## Documento de constitución



Para crear un CSIRT es necesario definir el marco que guiará y regirá el funcionamiento del equipo. El marco o documento de constitución cubrirá, entre otros, los siguientes aspectos:[07]

- La naturaleza y los objetivos del CSIRT.
- La comunidad objetivo (gobierno, sector privado, o ambos).

Un CSIRT nacional debe identificar claramente **su misión y su visión**. Estos dos aspectos no solo servirán de guía a los que trabajan en el equipo, sino que servirán como referencia a cualquier persona que reciba sus servicios o colabore con él. En resumen, la misión y el objetivo son las razones por las cuales existe el CSIRT.

El **marco institucional** de un CSIRT establecerá su configuración. Un CSIRT puede constituirse como una empresa independiente para proporcionar servicios en el ámbito privado, como una unidad dentro de una organización pública o privada para prestar servicios internos o externos, o como una organización en sí misma que no depende de ningún grupo o entidad en particular. Esta guía se centrará en una estructura organizativa para un CSIRT nacional.

Por último, es probable que sea necesario un **marco legal** para proteger el CSIRT y sus operaciones, teniendo en cuenta que un equipo de respuesta con responsabilidades a nivel nacional se ocupará de muchos temas sensibles, posiblemente con implicaciones en la seguridad nacional, la economía macro, o la seguridad pública. Esta guía presentará y analizará los pros y los contras de varios tipos de marcos legales para un CSIRT nacional.

# Misión y objetivo

La misión explica **por qué** existe una organización. Ella debe detallar, tanto para los actores internos como para los externos, lo que hace la organización, para quién y qué valores la motivan[08]. Normalmente, no incluye el "cómo" logra lo que se propone, ya que esto puede cambiar con el tiempo, y la misión en sí misma debe ser específica, claramente definida e invariable, por lo cual los verbos se usan generalmente en infinitivo y en presente. En el contexto de un CSIRT nacional, el objetivo de la organización debe ser concreto, explícito y utilizar palabras claras.[09]

## QUÉ

En la descripción de **qué** hace el equipo, se acostumbra a utilizar términos o frases como "coordinar", "promover regulaciones", "dirigir esfuerzos", "proteger, prevenir o articular actividades como respuesta a incidentes", "seguridad cibernética", "sistemas de información o activos", etcétera.

## PARA QUIÉN

En la descripción de **para quién** se realizan las actividades, los términos utilizados a menudo son "país", "estado", "gobierno" y "sector", entre otros.

## VALORES

En cuanto a los **valores** que impulsan la misión, el motivo debe declararse con claridad, por ejemplo mediante el uso de términos como "desarrollo", "bienestar", "seguridad" o "gestión de riesgos". Valores como la seguridad, la confianza o la responsabilidad, entre otros, también se pueden invocar.

A continuación se presentan algunos ejemplos de declaraciones de misión de CSIRT en todo el continente americano.

### Misión del National Cyber Security and Communications Integration Center Mission | NCCIC, EE.UU.

Reducir la probabilidad y la gravedad de los incidentes que puedan comprometer significativamente la seguridad y la resiliencia de las redes de tecnología de la información y las comunicaciones críticas de la nación. Para ejecutar su misión de manera efectiva, el NCCIC se centrará en tres prioridades estratégicas básicas y objetivos operativos asociados. El NCCIC implementará esta estrategia mediante la ampliación y la consecución de las capacidades, los productos y los servicios que se requieran para cumplir con cada una de sus prioridades estratégicas en los próximos cinco años. Muchas de estas actividades se coordinarán, desarrollarán y ejecutarán en colaboración con los socios operativos de la NCCIC en beneficio de toda la comunidad de interesados cibernéticos y de las comunicaciones.

Cabe señalar que cada una de las misiones establece claramente el objetivo principal del CSIRT y a quién servirá. Más tarde, esta declaración de la misión se utilizará como referencia para expresar el alcance del CSIRT nacional en detalle.

### Misión del ColCERT | Colombia

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) tendrá como responsabilidad central la coordinación de la ciberseguridad y de la ciberdefensa nacional, las cuales estarán enmarcadas dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y la defensa nacional.

### Misión del VenCERT | Venezuela

La misión asignada al VenCERT para contribuir al objetivo general de Sistema Nacional de Seguridad de la Información se puede detallar en los siguientes puntos:

- Prevención, detección y gestión de los incidentes que afectan los Sistemas de Información del Estado y entidades gestoras de infraestructuras críticas de la nación.
- Punto principal de coordinación nacional de otros centros de gestión de incidentes en el país y en el extranjero.
- Asesoramiento, apoyo y formación en materia de seguridad a los diferentes responsables de TIC en organismos del Estado o de entidades gestoras de la gestión de infraestructuras críticas nacionales.
- Coordinación de iniciativas públicas o privadas relativas a seguridad de las TIC en el Estado, materializadas por medio de proyectos de I+D, formación y sensibilización, elaboración de políticas, normas o guías, tanto para beneficio de la comunidad (gestores de IC del Estado y nacionales) como para la mejora de los servicios prestados en el VenCERT.

El VenCERT se erige, por tanto, como el CERT gubernamental venezolano, y su principal objetivo es la prevención, la detección y la gestión de los incidentes generados en los sistemas de información de toda la Administración Pública Nacional y sectores públicos a cargo de la gestión de infraestructuras críticas de la nación.

### Misión del CERTuy | Uruguay

Proteger los activos de información críticos del Estado y promover la conciencia en seguridad de la información de manera que prevenga y responda a incidentes de seguridad.

## Visión

La visión establece la dirección, en el largo plazo, que tomará la organización y cómo espera ser vista por los externos, sean clientes, pares o *sponsors*. Se refiere a la reputación de la organización y su propósito en el futuro. La visión establece la ruta que tomará la organización a largo plazo y sirve para guiar las decisiones estratégicas.[10] Bill Gates expuso una de las más famosas visiones TIC de todos los tiempos, que se caracteriza por su claridad, su brevedad y la ambición: "Una computadora personal en cada escritorio".

La visión está estrechamente relacionada con la cultura de cada nación, y el CSIRT puede incorporar ciertos rasgos de un país, como la reputación, la eficiencia, la fiabilidad, la eficacia, la rendición de cuentas y la innovación. Sin embargo, la visión es importante, no solo para los actores externos, sino también para las operaciones reales de un CSIRT u organización, ya que establecerá los valores de la organización[11]. La visión de una organización no debería cambiar con el tiempo.

Estos son ejemplos de visiones de algunos de los CSIRT nacionales en la región.

### Visión del VenCERT | Venezuela

Los servicios del VenCERT permitirán proteger y garantizar la defensa y la seguridad de la nación, así como la suprema vigilancia de los intereses generales de la República, la conservación de la paz pública y la recta aplicación de la ley en todo el territorio nacional, conforme a las competencias establecidas en la Constitución de la República Bolivariana de Venezuela, para el Poder Público Nacional.

### CERTuy Vision | Uruguay

Ser un centro de respuesta a incidentes en seguridad informática confiable y un referente a nivel nacional y regional.

### NCCIC | USA Vision

La visión del NCCIC es una infraestructura cibernética y de comunicaciones segura y resistente que apoya la seguridad nacional, una economía vibrante y la salud y la seguridad del pueblo estadounidense. En el esfuerzo para lograr esta visión, el NCCIC hará lo siguiente:

- Se centrará en la coordinación proactiva de la prevención y la mitigación de las amenazas cibernéticas y de telecomunicaciones que representan el mayor riesgo para la nación.
- Buscará la integración operativa "de todo el país" mediante al abordaje y la profundización de la participación de sus socios para gestionar las amenazas, las vulnerabilidades y los incidentes.
- Romperá las barreras tecnológicas e institucionales que impiden el intercambio colaborativo de información, conocimiento de la situación y la comprensión de las amenazas y de su impacto.
- Mantendrá una disposición constante para responder de inmediato y de manera eficaz a todos los incidentes cibernéticos y de telecomunicaciones que afecten la seguridad nacional.
- Servirá a las partes interesadas como un centro nacional de excelencia y experiencia en materia de seguridad cibernética y de telecomunicaciones.
- Protegerá la privacidad y los derechos constitucionales del pueblo norteamericano en la realización de su misión.



## Metodología propuesta para la definición de la misión y la visión

Dado que la misión y la visión definen la perspectiva del CSIRT en el mediano y largo plazo, es importante que estas partes del plan del CSIRT cuenten con el apoyo de buena parte, sino con el total, de los grupos de interés identificados en el capítulo anterior. En este sentido, es útil formar un grupo de trabajo compuesto por una pluralidad de partes interesadas para determinar estos dos componentes críticos de un plan de CSIRT. Los delegados del grupo de trabajo deben ser designados por su alta dirección para asegurar que los productos finales tienen la autoridad y la aprobación oficial de las instituciones participantes. Al mismo tiempo, el número de representantes que componen el equipo de redacción debe ser lo suficientemente pequeño para que el progreso sea eficiente y que participen solo aquellos con el mayor interés e influencia en el proyecto.

Una vez que se elabora una lista adecuada de partes interesadas, se deben establecer varios grupos de trabajo para trabajar de forma independiente en la misión y en la visión. Una persona actuará como moderador, y una variedad de preguntas ayudará a los asistentes a lo largo de la discusión.

Al igual que en la redacción de la misión, para la creación de la visión, los moderadores pueden plantear preguntas para guiar a los delegados.

- Cuál considera usted que es el propósito principal de un CSIRT nacional?
- ¿Qué necesidades cubriría?
- ¿A quiénes debería darles servicio?
- ¿Qué tipo de servicios ofrecerá?
- ¿Qué consideraciones restringirían sus operaciones?
- ¿Qué metas o factores de éxito deben considerarse para el CSIRT nacional?

Después de recoger las opiniones de los participantes, el moderador ayudará con la redacción para finalizar declaraciones claras y concisas. Una vez completado este paso, los resultados deben ser distribuidos a un grupo más amplio de partes interesadas. También es importante documentar el proceso y asegurar que se tomen las actas en todas las reuniones que indiquen claramente cómo se llevaron a cabo las actividades y quiénes participaron en ellas.

**Los delegados del grupo de trabajo deben ser designados por su alta dirección para asegurar que los productos finales tienen la autoridad y la aprobación oficial de las instituciones participantes.**

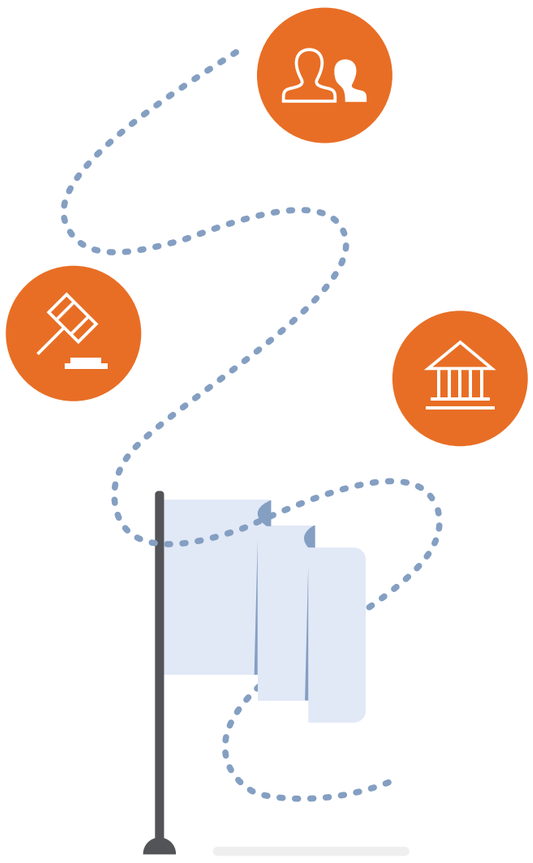
Una vez terminado, se utilizarán la misión y la visión durante el ciclo de vida del CSIRT nacional.

- ¿Cómo espera que sus clientes/la comunidad vean al CSIRT nacional?
- ¿Qué valores espera que este inspire?
- ¿En qué sentido ayudará a mejorar la calidad de vida de las personas? ¿Por qué? ¿Cómo?
- ¿Cómo se adaptará el CISRT nacional a los cambios de tecnología y de administración?
- ¿Cómo conseguirá destacarse en su entorno?

# Marco institucional

El marco institucional del CSIRT nacional es clave para su creación y su funcionamiento a lo largo de su ciclo de vida. Como se indicó anteriormente, se pueden configurar CSIRT nacionales de diferentes maneras, pero tendrán rasgos en común. Es importante que el país adopte una estructura CSIRT que se ajuste a sus realidades legales, políticas y culturales.

El marco institucional de un CSIRT nacional establecerá las directrices para las siguientes consideraciones:



- Responsabilidades
- Autoridad
- Interacción con los interesados
- Recursos financieros
- Recursos humanos
- Infraestructura
- Resiliencia

Un CSIRT nacional con una función de coordinación debe estar ubicado en una oficina u organismo que tiene contacto e influencia con una gama de partes interesadas. De lo contrario, será difícil de ejecutar y comunicar el trabajo del equipo de respuesta. Al igual que con la mayoría de las cosas que se describen en esta guía, la ubicación del CSIRT dependerá de la estructura de su gobierno. En América Latina, los CSIRT se encuentran en una variedad de instituciones. En Brasil, Panamá y Uruguay, por ejemplo, los equipos están en los órganos ejecutivos bajo la Presidencia. En Colombia y en Perú, los Ministerios de Defensa y de Seguridad manejan la respuesta nacional a incidentes. Sin embargo, en otros países como Paraguay, el CSIRT opera desde el Ministerio de Tecnología. Que un equipo forme parte del gobierno no debe, de ninguna manera, impedirle el intercambio de información y de estrategias con el sector privado y con otros actores. De hecho, muchos CSIRT forman comités o juntas directivas compuestas por selectos actores que debaten y discuten las decisiones clave que enfrenta el equipo de respuesta. Mientras que algunos CSIRT aceptan las decisiones de sus comités como obligatorias, otros los utilizan simplemente como un foro para el debate y la colaboración, y la decisión final la tiene en última instancia el equipo.

Un aspecto a menudo pasado por alto a la hora de establecer un CSIRT es la financiación. Parece obvio, pero un equipo nacional de respuesta a incidentes sin una fuente constante de financiación no podrá funcionar más allá del corto plazo. Por esta razón, mientras que asegurar financiación semilla o inicial es fundamental, el equipo del proyecto debe también hacer proyecciones de cuánto dinero será necesario, después de asegurados los costos iniciales, para financiar el sostenimiento del equipo[12].

## Metodología para la creación del marco institucional

Una vez establecidos los grupos de interés, la misión y la visión, el equipo del proyecto debe identificar dónde se establecerá el CSIRT nacional. El equipo debe estar ubicado en una institución que

- tenga la capacidad de establecer o influenciar políticas relacionadas con seguridad de las TIC a nivel nacional;
- resida lo suficientemente cerca de los más altos niveles de gobierno para que pueda contar con su apoyo cuando sea necesario;
- sea capaz de obtener financiación;
- tenga jurisdicción y autonomía apropiada cuando sea necesario.

Debido al carácter transversal de los temas con los que trabaja un CSIRT, se formará un grupo multidisciplinario para determinar dónde se ubicará el CSIRT. Debe estar compuesto de expertos en:

- Seguridad informática y respuesta a incidentes.
- Políticas públicas en tecnología y telecomunicaciones.
- Seguridad y defensa nacional.
- Ley pública.
- Marco legal.

En función de las instituciones gubernamentales del país, el equipo del proyecto debe recomendar:

- Si el CSIRT será una organización independiente, cuyo único propósito es ser un CSIRT nacional, o una división dentro de otra organización.
- Si el CSIRT será exclusivamente una organización estatal o incluirá la participación del sector privado, la academia o la sociedad civil.
- Si hay participación de terceros, exactamente cómo se llevará a cabo y cuál será el modelo de negocio asociado.
- ¿Cómo se verá la estructura de financiación de la organización y cómo se asegurará?
- ¿Cómo se formará el comité de dirección/coordinación y qué facultades tendrá?

Igual que con otros procesos, las discusiones deben ser anotadas con el fin de promover la transparencia y aumentar el apoyo de los grupos de interés. Las recomendaciones finales acordadas por este grupo de trabajo, junto con la misión y la visión, se unificarán en un solo documento, que luego será revisado por expertos legales para establecer su aplicación.

**Debido al carácter transversal de los temas con los que trabaja un CSIRT, se formará un grupo multidisciplinario para determinar dónde se ubicará el CSIRT.**

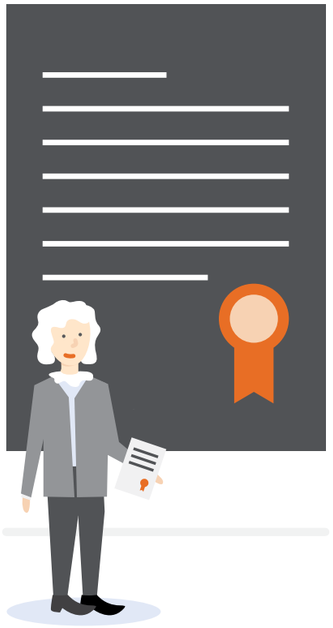
# Marco legal

Por último, es muy importante definir la autoridad legal bajo el cual se establecerá el CSIRT nacional. Debe conformarse de acuerdo con las normas legales del país en cuestión y debe garantizar la implementación. Si no se ha adoptado correctamente, un marco legal deficiente puede conducir a juicios o complicaciones en la respuesta a incidentes cibernéticos. Por esto es tan importante que la misión, la visión y el marco institucional sean evaluados por expertos legales, ya sea del gobierno, de la academia o de ambos, específicamente para responder a las siguientes preguntas.

- ¿Es aceptable el CSIRT desde el punto de vista legal? ¿Se contradice alguna ley o permite que haya vacíos legales que puedan ser explotados y tengan un efecto negativo en el equipo de respuesta y sus deberes?
- ¿Qué instrumento se utilizará para el marco institucional? ¿Legislación, decretos o resoluciones?
- ¿Puede el CSIRT emplear todas las medidas legales para garantizar la financiación?
- ¿Cómo se contratarán los recursos humanos?

Las conclusiones del análisis jurídico deben aparecer como un apéndice o un anexo al documento de establecimiento del CSIRT.

Los siguientes son ejemplos de diferentes marcos legales que institucionalizan a los CSIRT en la región.



**CSIRT | Panama**

Decreto Ejecutivo No. 709
de 26 de septiembre 2011

**ColCERT | Colombia**

Colombia: Documento CONPES 3701

**CERTuy | Uruguay**

Ley 18.719 año 2008.
Decreto poder ejecutivo 451, año 2009

**ICIC CERT | Argentina**

Resolución de Jefatura
de Gabinete de Ministros 580/2011

# C Alcance

Una vez que se establecen la misión, la visión y los marcos institucionales y legales del CSIRT, es importante definir su ámbito de aplicación, en concreto mediante la determinación de los servicios que se prestarán y a quién(es).

El alcance será determinado por las necesidades de recursos humanos, capacitación técnica, infraestructura, herramientas y presupuesto.

| Entrada | Herramientas | Salida |
|---|---|---|
| - Documento de constitución<br>- Misión<br>- Visión | - Análisis de requerimientos de servicios<br>- Consulta a expertos<br>- Análisis de recursos | - Comunidad objetivo<br>- Definición de servicios |

## Comunidad objetivo

La comunidad objetivo CSIRT es el grupo de personas o entidades que recibirán los servicios por parte del equipo, es decir, los clientes.

El CSIRT debe definir claramente cuál es su público objetivo, incluyendo si los diferentes miembros de la comunidad recibirán diferentes niveles de servicio o no. Esto puede variar dependiendo de si la criticidad de los sistemas o infraestructuras es administrada y operada por un miembro particular de la comunidad, o si un CSIRT existente ya le presta servicio a una determinada entidad. Por ejemplo, las instituciones militares a menudo supervisan sus propias redes y pueden no requerir los servicios de un CSIRT nacional. Por tanto, es crucial que un CSIRT determine para quién trabaja, qué otros equipos participan y en qué medida sirve a la comunidad. La comunidad objetivo puede incluir otros CSIRT, ISP, operadores de centros de datos y otros actores cuya confianza y cooperación será de suma importancia para un resultado exitoso.

## Modelos de autoridad con la comunidad objetivo

Varios modelos de autoridad vinculan el CSIRT con su comunidad. Estos modelos definen las atribuciones y las obligaciones del CSIRT cuando se enfrenta a un incidente ocurrido en su comunidad.

Hay cuatro tipos de autoridad comunes que un CSIRT puede ejercer sobre su comunidad:[13]

### Autoridad completa

El CSIRT tiene autoridad para realizar todas las acciones necesarias inherentes a la gestión de un incidente, y los miembros de la comunidad están obligados a implantar las medidas propuestas por el CSIRT.

### Autoridad compartida

La toma de decisiones frente un incidente es conjunta entre los miembros de la comunidad afectada. El CSIRT apoya a los actores involucrados en un incidente y colabora con los equipos y con experticia.

### Autoridad nula

El CSIRT no tiene autoridad sobre la toma de decisiones frente a incidentes. Provee asesoramiento, información y experiencia, pero las decisiones son tomadas por los afectados.

### Autoridad indirecta

El CSIRT no tiene autoridad sobre la comunidad, sin embargo, puede ejercer presión indirecta sobre ella. Por ejemplo, por medio de entes reguladores, o de otras organizaciones con las que el CSIRT haya establecido vínculos de confianza.

# Servicios

Los servicios de un CSIRT están fuertemente relacionados con su misión, la comunidad objetivo y el conocimiento, las habilidades y las capacidades de los recursos humanos a su disposición.

Estos servicios pueden ser proporcionados en su totalidad por personal de CSIRT, con la asistencia de las partes interesadas, o por medio de otros actores con los que el CSIRT tiene acuerdos, como empresas de *software* o *hardware*. En cada caso, el CSIRT debe evaluar la mejor manera de ofrecer el servicio en una situación dada, dependiendo de la disponibilidad de recursos y de la especialización.

**En cada caso, el CSIRT debe evaluar la mejor manera de ofrecer el servicio en una situación dada, dependiendo de la disponibilidad de recursos y de la especialización.**

Los servicios prestados por el CSIRT suelen agruparse en tres tipos: servicios reactivos, servicios proactivos y servicios de valor agregado.[14]

### Servicios proactivos

- **Servicios de monitoreo y alertas**
  - Monitoreo externo.
  - Monitoreo interno.
  - Desarrollo de herramientas de seguridad.
  - Reportes y alertas de seguridad
- **Servicios de investigación y desarrollo**
  - Auditorías de seguridad.
  - Escaneo de vulnerabilidades.
  - Escaneo de artefactos maliciosos.
  - Monitoreo de tecnología.
  - Análisis de artefactos.
  - Análisis forense.

### Servicios reactivos

- **Gestión de incidentes**
  - Análisis post mortem
  - Asistencia en el sitio
- **Respuesta a vulnerabilidades**
- **Respuesta a artefactos maliciosos**

### Servicios de valor agregado

- **Capacitación y educación**
- **Concientización**
- **Análisis de riesgos y continuidad de negocio**
- **Apoyo a emprendimientos de seguridad**

# Servicios reactivos

Los servicios reactivos son los servicios más importantes que ofrece un CSIRT. En esencia, los "servicios reactivos" responden a los incidentes de seguridad cibernética que ocurren en la comunidad del CSIRT o en su propia infraestructura. Se puede brindar una respuesta derivada de una solicitud de asistencia. Los principales tipos de servicios reactivos son la gestión de incidentes, la respuesta de la vulnerabilidad y la respuesta a artefactos.

## Gestión de incidentes

El servicio de gestión de incidentes se compone de varias fases: la notificación y la recepción de un incidente, clasificación o *triage*, respuesta, análisis y resolución. El CSIRT debe primero determinar el tipo, el impacto potencial y la gravedad de un incidente, seguido de cerca por la designación de un equipo de respuesta que diseñe un plan de acción que restaurará los servicios o los sistemas a su funcionamiento normal o que mitigará el impacto de un evento de seguridad cibernética. En ciertos casos, esto requerirá que el personal del CSIRT visite el sitio del evento de seguridad.

Muchos actores suelen participar en respuestas a incidentes cibernéticos, incluyendo pero no limitado a los ISP, otros CSIRT, proveedores de tecnología, agencias del orden público, actores internacionales, equipos legales, departamentos de prensa y diferentes áreas de una organización afectada. El CSIRT coordina las actividades de respuesta y las comunicaciones de los distintos grupos de interés para optimizar esfuerzos y reducir los tiempos de resolución de incidentes. Para lograr esto, el CSIRT debe conocer las necesidades y los requerimientos de cada una de las partes interesadas con el fin de gestionar positivamente la interacción entre ellos.

## Respuesta a vulnerabilidades

Esto comprende una variedad de procesos de gestión de vulnerabilidades, incluyendo parches, la aplicación de contramedidas y otras estrategias de mitigación. A medida que están disponibles nuevos parches para las vulnerabilidades detectadas, el CSIRT debe notificar a todas las partes interesadas y distribuir parches o describir las técnicas para la aplicación de contramedidas, mientras coordina y confirma que se están tomando las medidas adecuadas.

## Respuesta a artefactos maliciosos

Un artefacto malicioso es un archivo o un objeto en un sistema que está involucrado en un ataque a una red o sistema, o se utiliza para evadir los controles de seguridad o medidas. La gestión de los artefactos maliciosos requiere extraerlos de un sistema afectado o informar a las partes interesadas sobre cómo hacer la gestión.

# Servicios proactivos

Estos servicios tienen como objetivo mejorar los procesos de infraestructura y de seguridad de la comunidad objetivo para prevenir incidentes de seguridad o reducir su impacto cuando se producen. Los principales tipos de servicios proactivos consisten en la realización del seguimiento, la distribución de alertas y el ofrecimiento de servicios de investigación y desarrollo.

## Servicios proactivos

### 1 Primer nivel

Uno de los servicios más básicos que ofrece un CSIRT es el monitoreo y las alertas, implica la implementación de sistemas que ayudan a detectar eventos de seguridad, realizan correlación de eventos, producen informes automatizados y escanean en búsqueda de vulnerabilidades en la comunidad objetivo. Para llevar a cabo estas funciones, el CSIRT puede desarrollar sus propias soluciones internas o emplear herramientas y sensores comerciales de fuente abierta o de terceros. La información producida por las iniciativas de monitoreo y alerta impulsará la toma de decisiones estratégicas y mejorará los procesos de respuesta a incidentes.

### 2 Segundo nivel

Un CSIRT más desarrollado ofrecerá servicios de vigilancia y de alerta más avanzados. Estos hacen un seguimiento a los sistemas y a las infraestructuras de la comunidad objetivo en mucha más profundidad, pero por lo general proporcionan el mismo tipo de alertas y correlación de incidentes, como el monitoreo y alerta de primer nivel. Un seguimiento más de cerca de los sistemas de cliente permite la detección temprana de eventos de seguridad, vulnerabilidades o artefactos maliciosos. Para llevar a cabo este tipo de monitoreo en profundidad, en general se requiere de la interconexión del sistema o la instalación de sensores de seguridad en la infraestructura de la comunidad.

## Investigación y desarrollo

### 1 Primer nivel

Estos servicios les permiten al CSIRT y a su comunidad mantenerse al tanto de los avances en el campo de la seguridad de la información y de la respuesta a incidentes. En concreto, se les permitirá estar al día sobre las alertas, las amenazas en evolución, los vectores de ataque que emergen, las mejores prácticas y nuevas normas en los servicios, así como sobre el mantenimiento y la operación de dispositivos, las estrategias de defensa y varios otros temas.

### 2 Segundo nivel

A medida que madura un CSIRT, va desarrollando capacidades más robustas de I+D. Con la información que recopila y genera, el CSIRT puede realizar auditorías de seguridad y evaluaciones en sus propios sistemas o en los de la comunidad objetivo. Esto puede incluir el análisis de la infraestructura o la aplicación, la revisión de las políticas de seguridad, el análisis de vulnerabilidades, las pruebas de penetración y el cumplimiento de los estándares o normas internacionales.

A medida que la tecnología evoluciona, las amenazas y las vulnerabilidades cambian. El CSIRT debe poder detectar amenazas o vulnerabilidades emergentes inherentes a las nuevas tecnologías y distribuir información relevante que pueda mejorar los niveles de seguridad.

### 3 Tercer nivel

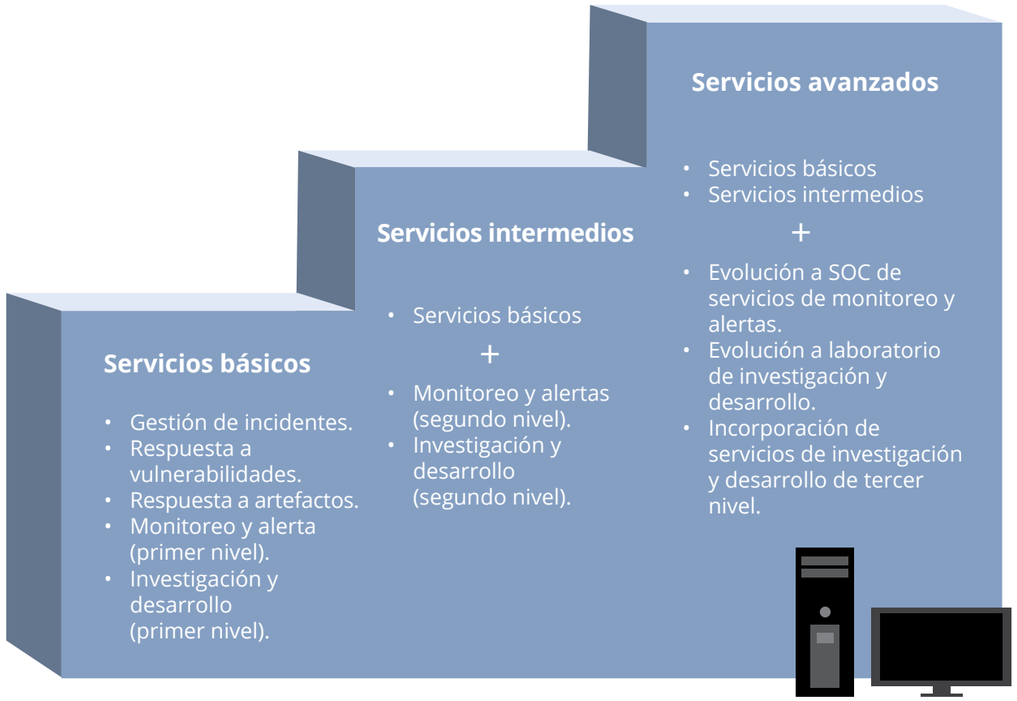
Los CSIRT más avanzados continuarán desarrollando las capacidades de I+D, por ejemplo, el análisis de los códigos maliciosos, a fin de poder determinar la naturaleza, el comportamiento y el propósito de un artefacto específico.

## Servicios de valor agregado

Estos servicios complementan los avisos de monitoreo y alerta emitidos por el CSIRT. En general, los servicios de valor agregado consisten en eventos y cursos de formación en seguridad, iniciativas de sensibilización, análisis de competencias y laboratorios de seguridad. Mediante la realización de este tipo de eventos, el CSIRT también genera confianza dentro de la comunidad y crea conciencia del propósito y la función del equipo de respuesta, lo que le permite operar con mayor eficacia. Uno de los aspectos más importantes de las actividades de capacitación eficientes es identificar las carencias y las necesidades de información de la comunidad objetivo. Gran parte de esto se conocerá en la actividad normal cotidiana del CSIRT y en la interacción con sus clientes.

## Evolución de los servicios de un CSIRT

Los servicios ofrecidos por un CSIRT dependerán de su tamaño, infraestructura, recursos y de las capacidades de los miembros de su equipo. Se pueden dividir en básicos, intermedios y avanzados, y es probable que crezcan a medida que el equipo madure con el tiempo.






# D Organización y RRHH

**Para situar el marco institucional en la práctica y llevar a cabo los servicios requeridos por la comunidad objetivo, el CSIRT necesita una estructura organizativa definida, incluyendo funciones y responsabilidades detalladas de su personal.**

| Entrada | Herramientas | Salida |
|---|---|---|
| - Misión<br>- Visión<br>- Comunidad objetivo<br>- Servicios | - Análisis de estructuras de CSIRT<br>- Recursos materiales disponibles | - Organigrama<br>- RRHH |

# Estructuras organizacionales

Existen cuatro estructuras CSIRT principales[15 16]:

## Equipo de seguridad localizada

Esta es la estructura CSIRT menos formal. La teoría que sustenta el "equipo de seguridad" sencillo es que los eventos de seguridad se resuelven con el personal existente en las organizaciones. Los miembros del equipo de seguridad no son necesariamente especialistas en respuesta a incidentes o seguridad de la información; pueden ser administradores de sistemas, bases de datos o tienen conocimientos especializados en los diversos componentes o productos que intervienen en los sistemas de TI como cortafuegos y *routers*, entre otros. En la mayoría de los casos, el equipo de seguridad no tendrá todos los conocimientos y la experiencia necesaria para llevar a cabo operaciones de seguridad sólidas. Por ejemplo, puede resolver un incidente, mas no determinar su causa, y así deja a la organización expuesta a ser explotada de nuevo. La naturaleza de un "equipo de seguridad" por lo general impide la aplicación de mejores prácticas, investigación y desarrollo, monitoreo y actividades de alerta de seguridad.

## Equipo de respuesta a incidentes centralizado

En esta estructura hay un solo equipo responsable de la gestión y respuesta de incidentes de seguridad por medio de una serie de ubicaciones que pertenecen a una organización más grande. Este modelo sería apropiado, por ejemplo, en una empresa. Esta estructura es apropiada para organizaciones cuya infraestructura de TI no está dispersa geográficamente.

En estas estructuras, hay un equipo de respuesta definido con personal dedicado y capacitado en el manejo de seguridad de la información y la respuesta a incidentes de seguridad. Estos equipos interactúan con especialistas en los productos o servicios.

## Equipos de respuesta a incidentes distribuidos

Grandes organizaciones con infraestructuras de TI distribuidas geográficamente o varias unidades de negocios en particular a menudo adoptan estructuras de respuesta a incidentes distribuidos. Estos se componen de un centro de respuesta integral dividido en varios equipos, uno de los cuales coordina las actividades de los demás. Las funciones de respuesta a incidentes se dividen según el área de conocimiento de cada equipo, en función de la ubicación geográfica donde se producen los incidentes, o en función del sector de la comunidad objetivo afectado.

El papel del equipo de coordinación es esencial para garantizar unos procedimientos de respuesta efectivos y estandarizados, mantener estadísticas de incidentes, aumentar la sinergia y promover el trabajo colaborativo por medio del intercambio de las mejores prácticas y lecciones aprendidas y cómo asignar adecuadamente los recursos de seguridad.

Otra de las funciones vitales del equipo coordinador es facilitar la interacción y la cooperación entre los equipos.

## Equipo coordinador

Este modelo es similar al modelo de equipos de respuesta distribuidos, pero a nivel de centros de respuesta. La diferencia es que el coordinador de centro de respuesta no necesariamente tiene que intervenir en las gestiones de otros equipos coordinados.

Este tipo de modelo surge de la necesidad de los centros de respuesta de interactuar de forma coordinada para lograr un objetivo común, o generar sinergias entre los centros de sectores similares o regiones, empresas o agencias de un mismo gobierno.

Su principal función es la de coordinar la eficacia de la respuesta y la interacción mediante la coordinación de gestiones y colaboración, proporcionar análisis de incidentes y de vulnerabilidades, boletines de noticias, estadísticas y documentación de las mejores prácticas, entre otras.

Es importante tener en cuenta que con el fin de definir el modelo de CSIRT por implementar, es esencial analizar los servicios que desean ofrecer. Ciertos modelos de CSIRT no son adecuados para la prestación de algunos de los servicios antes mencionados, en particular los servicios que requieren recursos permanentes.

Es importante definir el tipo de modelo de CSIRT por implementar, ya que esto tendrá una consecuencia directa sobre el tamaño de la organización.

# Tamaño de la organización

La estructura organizativa de un CSIRT, como cualquier organización, depende precisamente de lo que hará y cómo pretende lograr sus objetivos. Algunas de las preguntas que deberá responder el gerente de proyecto del CSIRT para determinar cómo se organizará el equipo son:

- ¿Qué servicios quiero ofrecer y en qué momentos?
- ¿Qué tan grande es la comunidad objetivo?
- ¿Cuál es la distribución geográfica de mi comunidad objetivo?

El lugar donde esté ubicado el CSIRT también será determinante en la forma en que se estructurará. Asimismo, vale la pena mencionar que su modelo organizativo, junto con los servicios que ofrezca, podrá cambiar en el tiempo.

# Funciones y responsabilidades

Para definir la estructura organizativa de un CSIRT, uno debe tener una idea clara de las distintas funciones y responsabilidades dentro de un equipo de respuesta.[17]

### DIRECCIÓN

- Dirección estratégica del centro.
- Supervisa a todo el equipo.
- Entrevista y contrata a nuevos miembros del equipo.
- Asiste a las sesiones del consejo asesor de seguridad.

### GERENTE TRIAGE

- Clasifica y prioriza los eventos.
- Asigna casos a personal técnico.

### GERENTES (MANDOS MEDIOS)

- Da soporte a la Dirección.
- Lidera el equipo en las actividades diarias.
- Asigna deberes y tareas.
- Conduce la gestión de claves.
- Autoriza los permisos de acceso a la información.

### GESTOR DE INCIDENTES

- Analiza incidentes, monitoreo, registro y respuesta.
- Coordina respuesta a incidentes.
- Colabora con otros grupos de respuesta o técnicos para resolver un incidente.

### CLASIFICADOR DE EVENTOS

- Provee asistencia inicial de respuesta a incidentes.
- Clasifica y prioriza la información recibida de un caso.

### ANALISTA/INVESTIGADOR

- Realiza investigaciones específicas.
- Desarrolla material técnico para el uso interno o de formación.
- Realiza tareas de monitoreo.
- Desarrolla herramientas.

### GERENTE DE COMUNICACIONES

- Desarrolla y publica documentos CSIRT.
- Mantiene el sitio web del CSIRT y el perfil de los medios sociales.

### ADMINISTRADOR DE RED

- Gestiona y mantiene la infraestructura de red del CSIRT.
- Ayuda en la respuesta a incidentes en casos relacionados a redes.

### ADMINISTRADOR DE SISTEMAS

- Administra y mantiene los sistemas del CSIRT.
- Asiste en la respuesta a incidentes cuando se necesita experticia en sistemas.
- Gestiona el acceso a la información.

### ASISTENTE

- Asiste al personal en la realización de las tareas asignadas, según sea indicado.

### REPRESENTANTE

- Representa al CSIRT en eventos.
- Si le es indicado, puede capacitar a otros actores.

### VOCERO

- Canal de comunicación autorizado con la prensa.

### CUSTODIO DE REGISTRO

- Acceso a repositorios seguros de información.

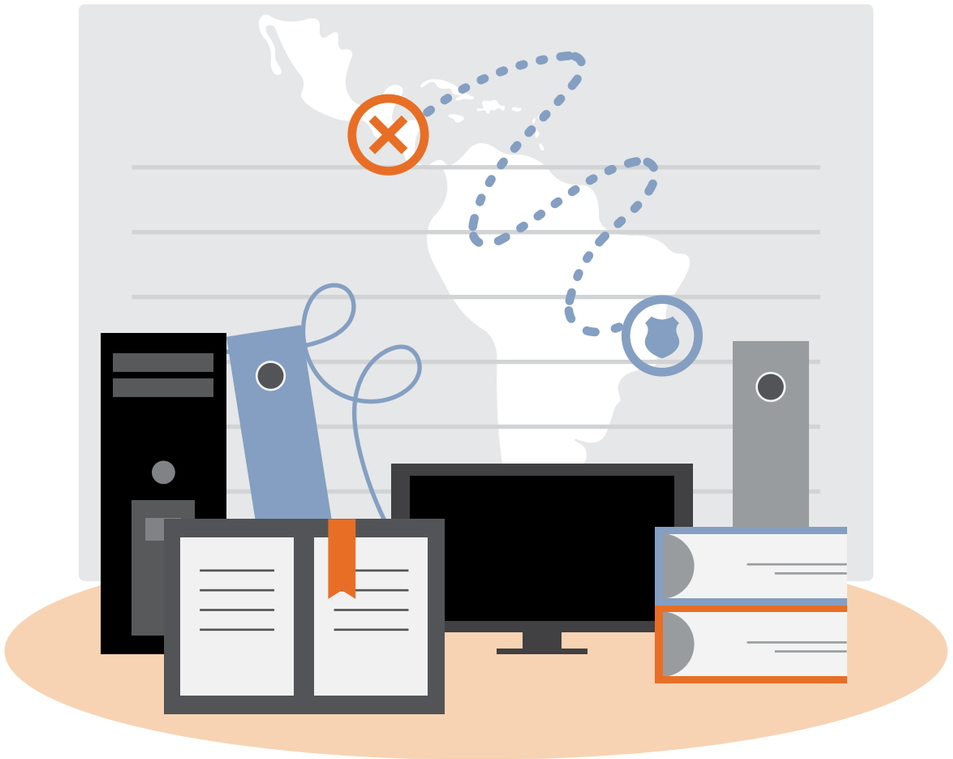
Estas funciones se distribuirán entre diferentes personas y áreas de trabajo. En la mayoría de los CSIRT, la gente estará a cargo de varias funciones a la vez. En este caso, es fundamental que exista una política y práctica de la separación de funciones.

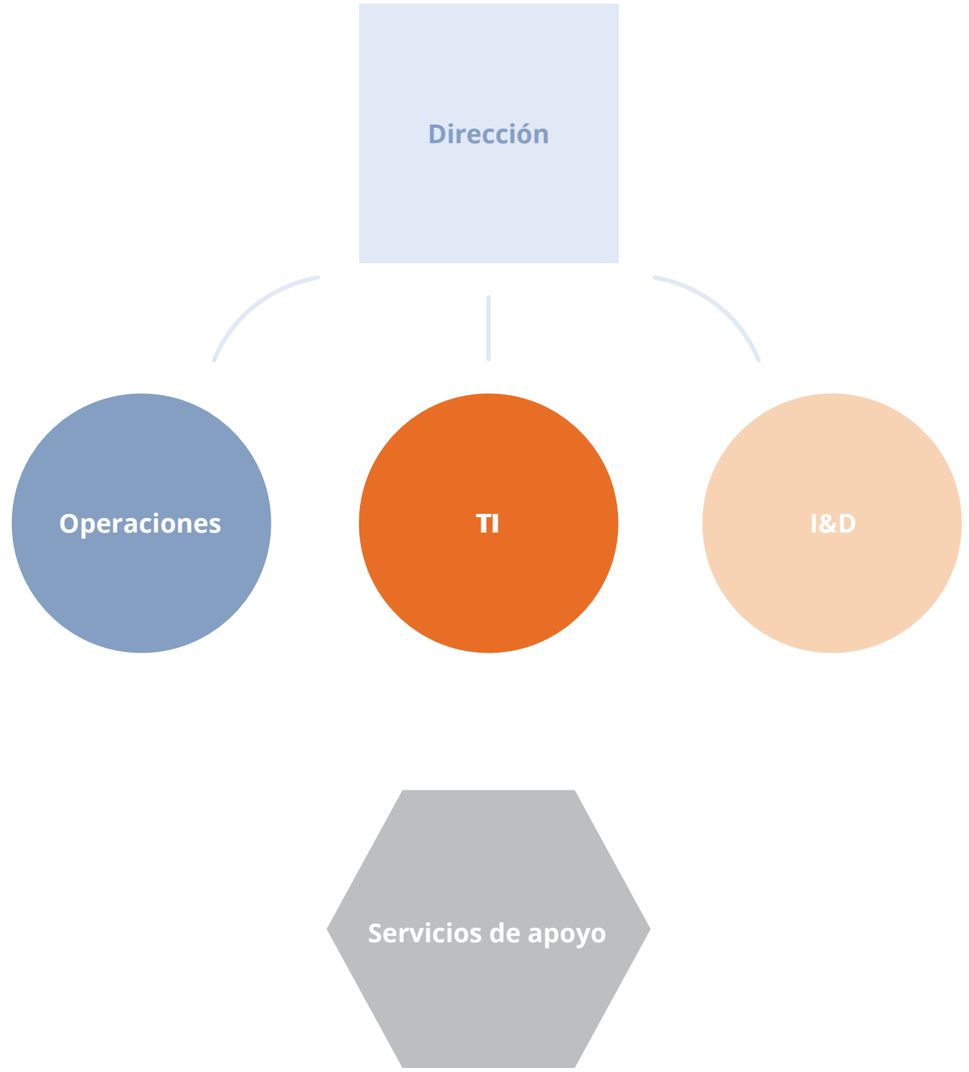
Aquí es como se asignan estos roles a diferentes áreas del CSIRT.

.

# Estructura organizacional

Como se mencionó anteriormente, los servicios iniciales recomendados para un CSIRT nacional son la gestión de incidentes, la gestión de vulnerabilidades, el monitoreo del sistema, la publicación de alertas y la formación.






Esta estructura anterior es la mínima estructura inicial recomendada para un CSIRT nacional, que puede crecer con el tiempo, según sea necesario. Varios CSIRT en las Américas, como los de Panamá, Paraguay y Uruguay, comenzaron con las estructuras organizativas similares a esta y han mostrado un crecimiento significativo.

Bajo este modelo, cada área es responsable de las siguientes tareas:

Servicios de apoyo:
Marketing/comunicaciones
Apoyo jurídico
Gestión de prensa
Administración y finanzas

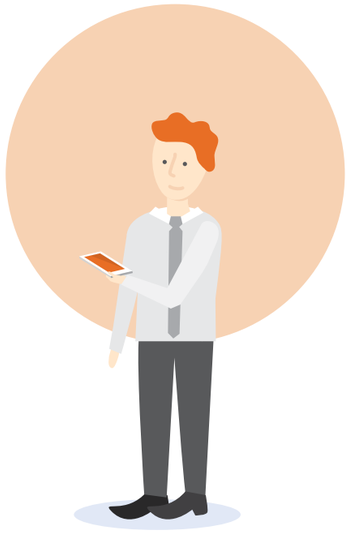
**Bajo este modelo, cada área es responsable de las siguientes tareas:**

## Dirección

- Dirección estratégica.
- Supervisión de actividades.
- Vinculación externa: otros CSIRT, organizaciones y consejo asesor.
- Gestión presupuestal.
- Enlace con el público/medios.

La **Dirección** del CSIRT establece principalmente las líneas de la organización y lleva a cabo la planificación estratégica. También establece acuerdos de cooperación con otras organizaciones y sirve de enlace con el Comité Directivo CSIRT. El director del CSIRT también actúa como portavoz a la prensa.

## Operaciones



- Gestión de incidentes.
- Monitoreo.

El área de **Operaciones** es la parte crítica del CSIRT. Aquí es donde se realiza la gestión de incidentes, el monitoreo y el análisis de incidentes. Puede tomar algún tiempo para que el área de Operaciones comience a recibir un gran número de incidentes a medida que se dan a conocer tanto el CSIRT como los servicios que les ofrece a los mandantes.

## TI

- Gestión de la infraestructura de TI.
- Apoyo a operaciones.
- Apoyo a I&D.

**Investigación y Desarrollo** es el área del CSIRT que implementará las funciones secundarias de los equipos, como el desarrollo de herramientas, la realización de cursos de formación y la investigación de nuevas tendencias y amenazas de la seguridad cibernética. El área de I+D estará ocupada desde el inicio del CSIRT ya que estará a cargo de la mayor parte de la planificación, la capacitación y el desarrollo de cualquier solución necesaria elaborada internamente. Esta área trabajará en estrecha colaboración con el área de TI.

## I&D

- Observatorio tecnológico.
- Análisis estadístico de incidentes y tendencias.
- Desarrollo de sistemas y herramientas.
- Capacitación.
- Investigaciones especiales.
- Apoyo a operaciones.

La sección de **TI** implementa y administra todos los sistemas que controlan y manejan el correo electrónico, página web, servidor de archivos, el sistema de gestión de tickets, la supervisión del sistema, la red y los servidores de seguridad del CSIRT. Al igual que el departamento de I+D, la sección estará ocupada desde el principio con la implementación y el ajuste de la arquitectura del CSIRT.

## Servicios de apoyo

- *Marketing*/comunicaciones.
- Apoyo jurídico.
- Gestión de prensa.
- Administración y finanzas.

Los **servicios de apoyo** que supervisan la gestión de prensa, las consideraciones legales y la administración y las finanzas son esenciales para el funcionamiento de cualquier CSIRT. Estas actividades deben tenerse en cuenta en un CSIRT nacional, aunque pueden ser subcontratados o provistos externamente.[18]

A medida que el equipo de respuesta madura, es probable que cree nuevas áreas y funciones. Entre las posibles áreas nuevas están:

## Laboratorio

Esta área, que puede estar bajo la Dirección o de I+D, llevará a cabo las actividades forenses o el análisis de *malware* y proporcionará servicios de investigación a otras áreas.

## Centro de Operaciones de Seguridad

Si la hoja de ruta del servicio indica que tiene un centro de operaciones de seguridad, se puede crear una zona SOC, que puede depender directamente de la Dirección o de Operaciones.

## Sistemas de Gestión de Seguridad de la Información (SGSI):

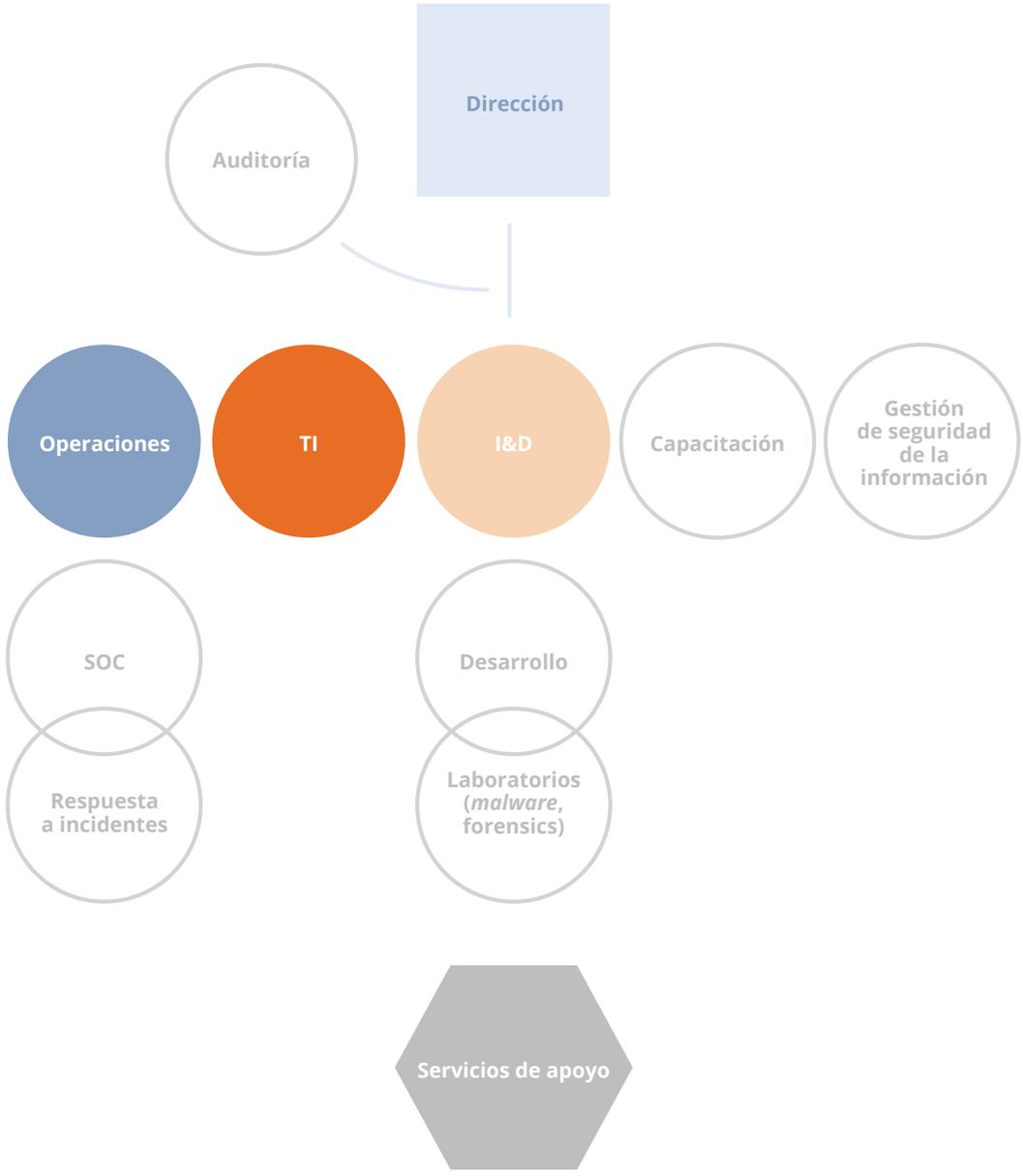
Si el objetivo es establecer servicios de apoyo para la implementación de SGSI, se puede establecer un área específica para ello.

## Formación

Si el CSIRT y su comunidad objetivo tienen suficientes solicitudes para la formación, se puede establecer un departamento de formación dedicado.

**A medida que crece el tamaño del equipo, puede llegar a tener que incorporar un departamento de auditoría para verificar si las políticas y los procedimientos en el CSIRT se siguen de acuerdo con el nivel deseado por la comunidad objetivo.**

Con servicios adicionales, el diagrama de flujo del CSIRT sería:

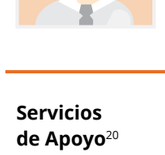


# Tamaño y cantidad de recursos

Una vez definida la estructura deseada, el Gerente de Proyecto del CSIRT vinculará y contratará a personal con las habilidades requeridas por las funciones que se van a realizar. Independientemente de la posición que ocuparán, el personal debe tener una amplitud de conocimientos a fin de evitar puntos únicos de falla en el CSIRT.[19] Además, no se espera que el personal del CSIRT dedique el 100% de su tiempo a una sola actividad, sobre todo en el momento inmediatamente posterior a su lanzamiento. En ciertos casos, equipos exitosos pueden comenzar con tres personas, por ejemplo, un director, un gerente de TI y un líder que cubra múltiples funciones, incluidas operaciones y de I+D, que también apoya al administrador de TI. En la primera fase de desarrollo del CSIRT, el soporte de TI tiene prioridad. La capacidad de respuesta a incidentes (Departamento de Operaciones) crecerá a medida que el CSIRT aumente su tamaño de personal, asegure el financiamiento y sea plenamente operativo.

**Independientemente de la posición que ocuparán, el personal debe tener una amplitud de conocimientos a fin de evitar puntos únicos de falla en el CSIRT.**

La tabla que se muestra a continuación es un ejemplo de cómo un CSIRT que inicia con nueve personas puede distribuir sus roles y sus funciones. La información se obtuvo por medio de consultas con los CSIRT de la región, que si bien varían en sus circunstancias y sus experiencias, sirven como modelos para el éxito.

| Departamentos CSIRT | Personal | |
|---|---|---|
| | **1.a Fase – Implementación:**<br>9 (6 empleados + 3 personal de apoyo) | **2.a Fase – Operación:**<br>15 (12 empleados + 3 personal de apoyo) |
| **Dirección**  | **1** Director/coordinador | **1** Director<br>**1** Coordinador |
| **Apoyo de TI**  | **1** Líder<br>**2** Especialistas técnicos | **1** Líder<br>**2** Especialistas técnicos (administrador de redes, administrador de sistemas) |
| **Investigación y Desarrollo**  | **1** Líder<br>**1** Especialista técnico | **1** Líder<br>**2** Especialistas en seguridad (analista/investigador, custodio de registros) |
| **Operaciones**  | **1** Líder<br>**1** Especialista técnico | **1** Líder<br>**3** Especialistas en incidentes (clasificación, *triage*, manejo) |
| **Servicios de Apoyo**[20]  | **1** Abogado (apoyo legal)<br>**1** Reportero (comunicaciones)<br>**1** Analista financiero | **1** Abogado (apoyo legal)<br>**1** Reportero (comunicaciones)<br>**1** Analista financiero |

### Notas

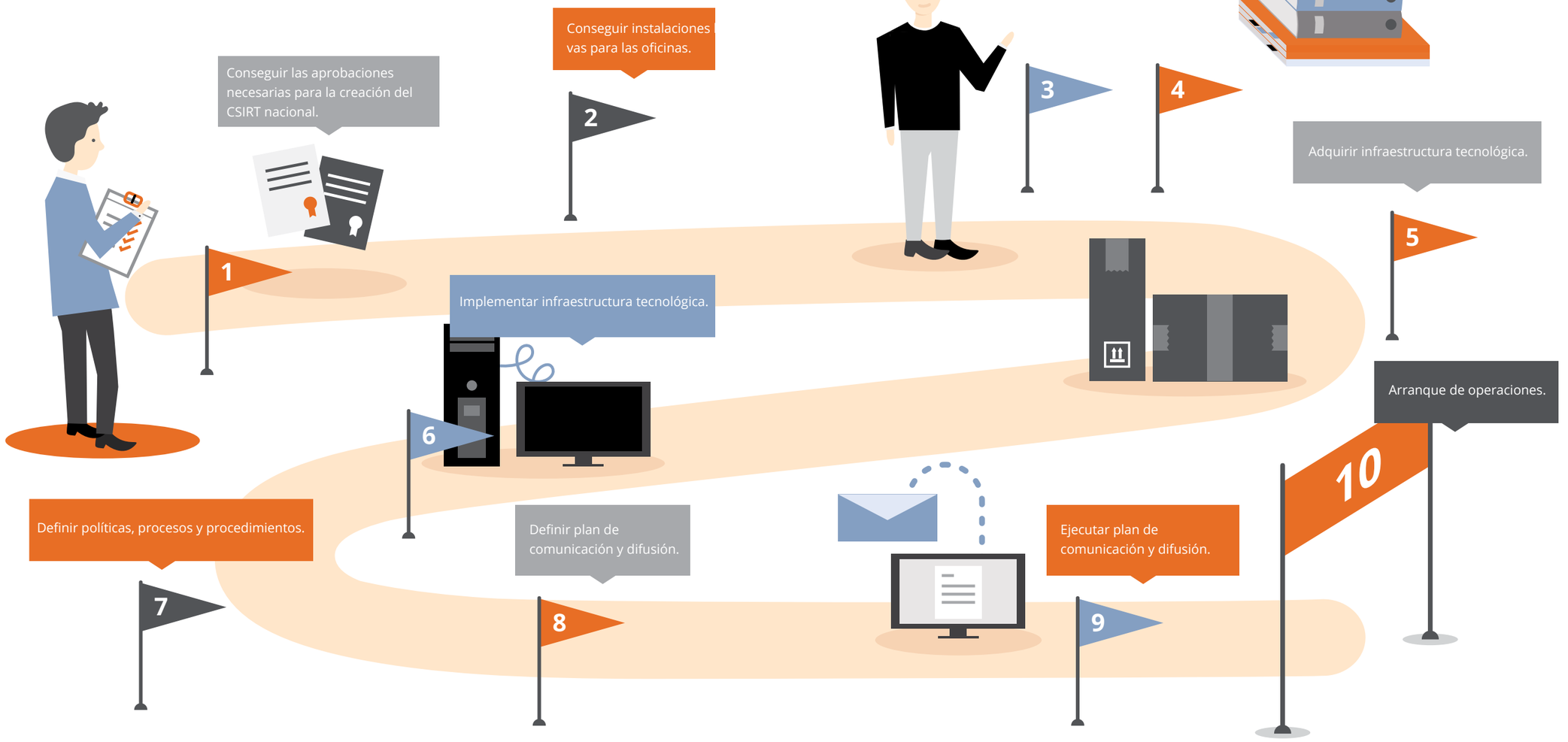
- Esta tabla se basa en las experiencias adquiridas por medio de consultas con algunos CSIRT en la región (ningún CSIRT está estructurado exactamente igual; cada CSIRT es diferente en función de sus necesidades o funciones particulares).
- Algunas posiciones pueden ser asumidas por una misma persona.

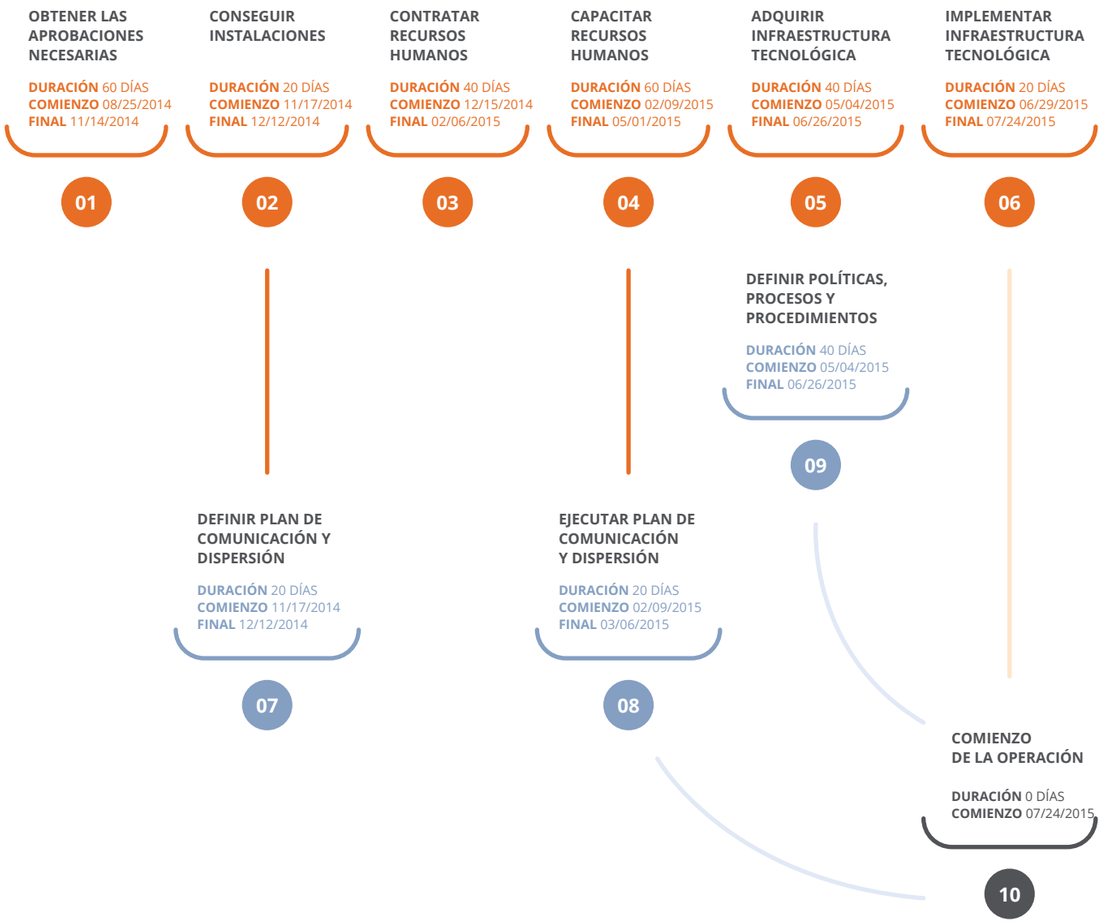
# Cronograma

El período de ejecución de un CSIRT debe seguir un cronograma definido y objetivos específicos.

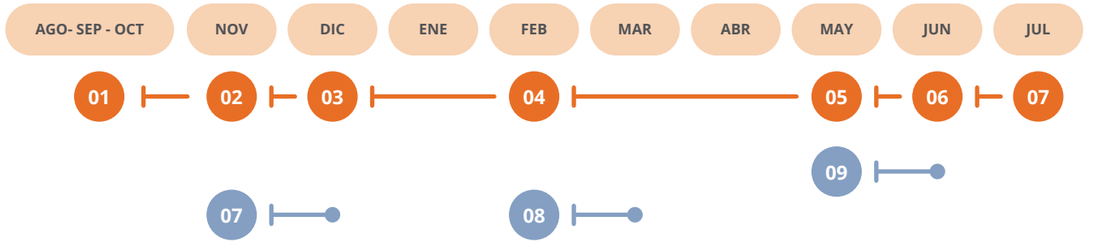
El primer paso para crear un cronograma es definir la lista de actividades necesarias para la implementación del CSIRT. Inicialmente, estas actividades serán de alto nivel, y el grado de detalle aumentará a medida que estas maduran.

El siguiente es un ejemplo de una lista de actividades:






| | NOMBRE | DURACIÓN | COMIENZO | FINAL | PREDECESORES |
|---|---|---|---|---|---|
| 01 | OBTENER LAS APROBACIONES NECESARIAS | 60 DÍAS | 08/25/14 | 11/14/14 | |
| 02 | CONSEGUIR INSTALACIONES | 20 DÍAS | 11/17/14 | 12/12/14 | 01 |
| 03 | CONTRATAR RECURSOS HUMANOS | 40 DÍAS | 12/15/14 | 02/06/15 | 02 |
| 04 | CAPACITAR RECURSOS HUMANOS | 60 DÍAS | 02/09/15 | 05/01/15 v | 03 |
| 05 | ADQUIRIR INFRAESTRUCTURA TECNOLÓGICA | 40 DÍAS | 05/04/15 | 06/26/15 | 04 |
| 06 | IMPLEMENTAR INFRAESTRUCTURA TECNOLÓGICA | 20 DÍAS | 06/29/15 | 07/24/15 | 05 |
| 07 | DEFINIR PLAN DE COMUNICACIÓN Y DISPERSIÓN | 40 DÍAS | 05/05/15 | 06/26/15 | 04 |
| 08 | EJECUTAR PLAN DE COMUNICACIÓN Y DISPERSIÓN | 20 DÍAS | 11/17/14 | 12/12/14 | 01 |
| 09 | DEFINIR POLÍTICAS, PROCESOS Y PROCEDIMIENTOS | 20 DÍAS | 02/09/15 | 03/06/15 | 03 |
| 10 | COMIENZO DE LA OPERACIÓN | 0 DÍAS | 07/24/15 | | 06 - 07 - 09 |




Una vez que se completa una lista de actividades, estas deben ser organizadas secuencialmente, teniendo en cuenta las dependencias que los vinculan. Una de las maneras más convenientes para formular y planear un proyecto, incluyendo las dependencias, es construir un diagrama utilizando el Método de Diagramación de Precedencia (PDM por sus siglas en inglés).

El PDM utiliza nodos y flechas. Cada nodo representa una actividad que está conectada con otra por medio de flechas que representan las dependencias. En PDM reconoce cuatro modos en que las actividades se relacionan:

- **Final a inicio:** El inicio de una actividad sucesora depende del fin de la predecesora.
- **Final a final:** La finalización de una actividad sucesora depende del final de la actividad predecesora.
- **Inicio a inicio:** El inicio de la actividad sucesora depende del inicio de la actividad predecesora.
- **Inicio a final:** La finalización de la actividad sucesora depende del inicio de la actividad predecesora.

Durante esta etapa de planificación, el equipo del proyecto deberá examinar las actividades de paralelización para reducir el tiempo necesario de su implementación.

Un ejemplo de un diagrama de precedencia con las actividades mencionadas anteriormente podría ser el que sigue.

Por último, una vez que está listo el PDM, se debe establecer el cronograma. Esto requiere la estimación de la duración de cada una de las actividades, que dependen de los recursos disponibles para su ejecución. También puede haber factores externos importantes para considerar en la determinación del cronograma, incluidos plazos políticos, procesos de concesión de licencias, fechas de los cursos de formación impartidos, asignación de recursos, etcétera.

Hay varias maneras de estimar la duración de las actividades necesarias para la implementación de un CSIRT. A continuación se muestran tres:

- **Juicio de expertos:** Con información de contexto el equipo del proyecto puede consultar a expertos en la materia, que pueden realizar la estimación basados en su experiencia. Esta técnica es muy simple y efectiva.
- **Estimación por analogía:** En esta técnica se busca información histórica de otros proyectos que hayan tenido actividades similares y se utilizan los valores históricos de las duraciones.
- **Estimación de tres valores:** Se utilizan las técnicas anteriormente mencionadas, pero en este caso se toman tres valores para estimar: uno pesimista, uno optimista y uno más probable. Esta técnica es muy utilizada cuando es complejo encontrar información histórica de características similares.[21]

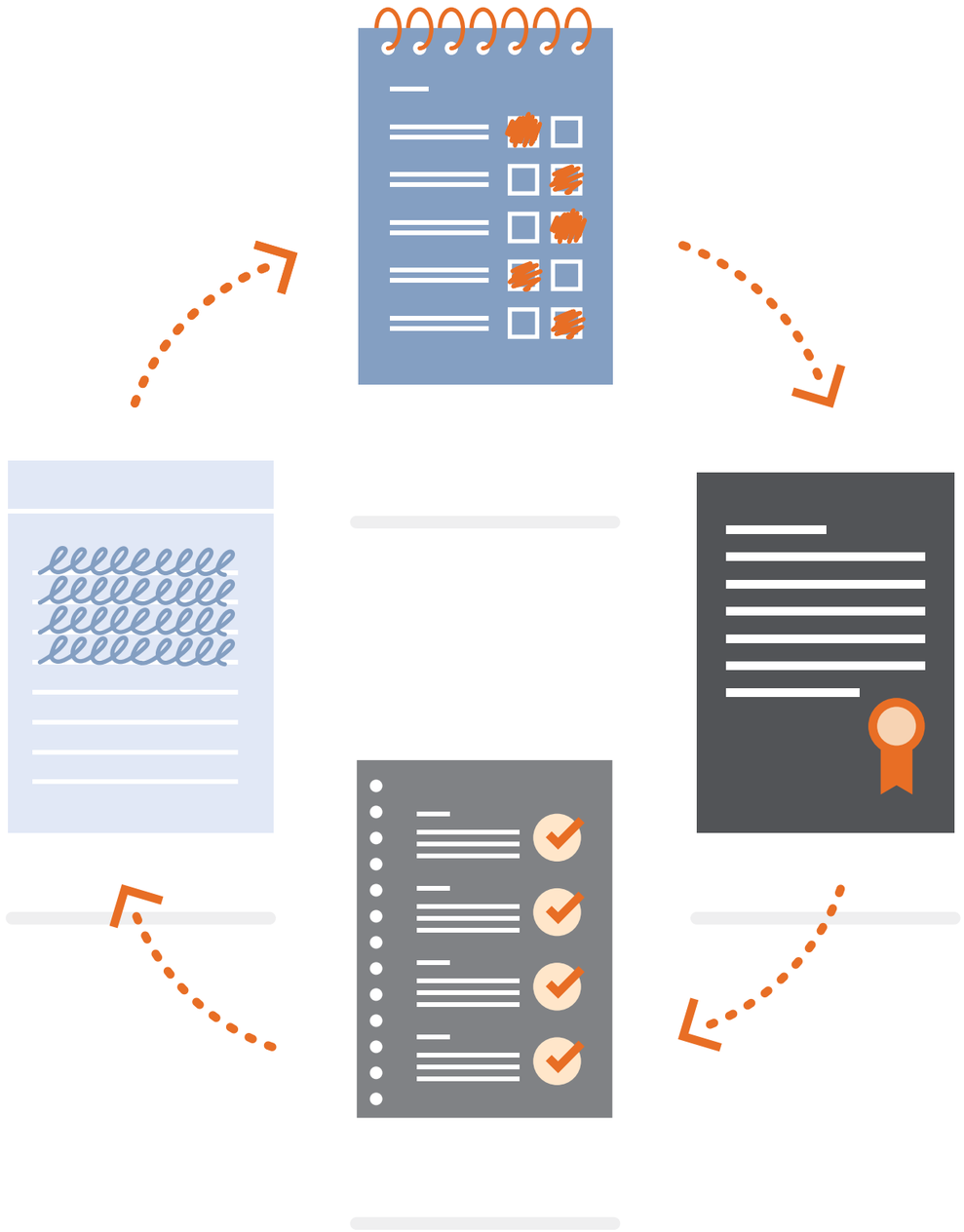
Finalmente se establece el diagrama del cronograma. A continuación se muestra anteriormente un ejemplo del diagrama de Gantt:

# Conclusión de la planificación preliminar

Al término de la etapa de planificación, debe haber una serie de documentos finalizados relacionados con el establecimiento de un CSIRT nacional, incluyendo:

- **Documento de identificación de los interesados.**
- **Plan de gestión de los interesados.**
- **Documento de constitución del CSIRT nacional.**
  - **Misión y visión.**
  - **Marco institucional.**
  - **Marco legal.**
- **Actas de reuniones.**
- **Listas de participantes en las diferentes actividades.**
- **Emails intercambiados con expertos.**
- **Definición de comunidad objetivo.**
- **Lista de servicios.**
- **Estructura organizacional.**
- **Recursos humanos necesarios.**
- **Cronograma de puesta en funcionamiento.**

Estos documentos servirán como referencia y guía para el resto del proyecto; algunos serán documentos formales firmados, mientras que otros solo serán documentos de soporte.

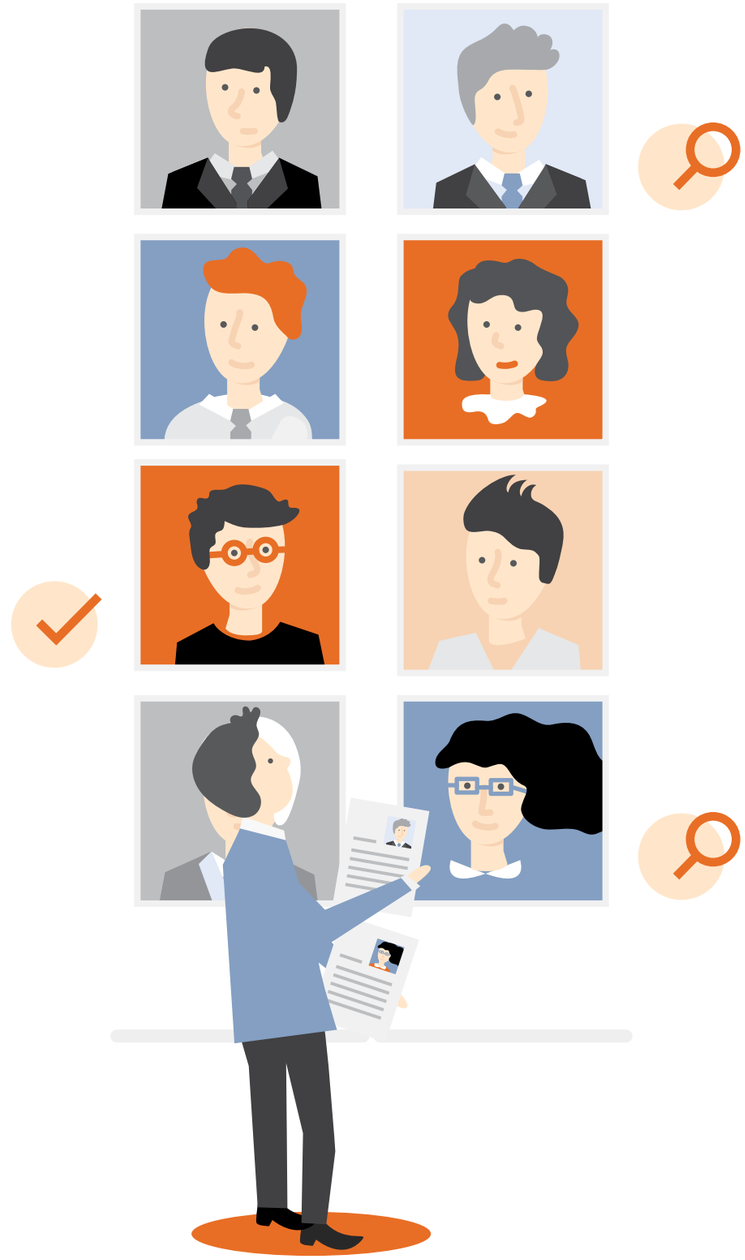


# 2 EJECUCIÓN

# A Selección de recursos humanos

En esta sección se detallan el conocimiento, la experiencia y las habilidades necesarias de los empleados potenciales de un CSIRT. La contratación de candidatos calificados es, sin duda, una de las partes más difíciles del proceso de establecer un CSIRT. Sin embargo, esta sección puede ser utilizada como una referencia en la evaluación de los perfiles de los candidatos durante el proceso de contratación.

Los perfiles se enumeran para los cargos en cada una de las áreas principales dentro del CSIRT: Dirección, I+D, TI y Operaciones.



## Dirección

Para los directores, tener experiencia de liderazgo es tan importante como el conocimiento técnico. Por supuesto, un candidato puede no satisfacer a la perfección el perfil de trabajo; sin embargo, en la tabla se dejan algunos aspectos para su consideración.

### FORMACIÓN

**Requerido**
- Título Universitario en TI.
- Especialización en Seguridad Cibernética.

**Se valorará**
- Postgrado en Gerencia (MBA, MMoT o similar).
- Certificaciones en Seguridad Cibernética (CISSP, CISM, CISA o similar).

### EXPERIENCIA

**Requerido**
- Más de diez años de experiencia en posiciones técnicas en TI o Seguridad Cibernética.
- Más de tres años en posiciones de gerencia de TI.

**Se valorará**
- Experiencia en respuesta a incidentes de seguridad cibernética.
- Experiencia en posiciones similares.

## Operaciones

Para las posiciones de Operaciones se requiere un perfil eficiente, organizado y dinámico, que se adapte naturalmente a un ambiente de alta presión.

### FORMACIÓN

**Requerido**
- Título universitario en TI.
- Especialización en Seguridad Cibernética.

**Se valorará**
- Cursos de especialización y experiencia en respuesta a incidentes de seguridad cibernética.
- Cursos de especialización en informática forense u otra área de seguridad cibernética y aseguramiento de información.
- Certificaciones en seguridad cibernética (CISSP, CISM, CISA o similar).

### EXPERIENCIA

**Requerido**
- Más de cinco años de experiencia en posiciones técnicas en TI o seguridad cibernética.

**Se valorará**
- Experiencia en operaciones y respuesta a incidentes de seguridad cibernética.
- Experiencia en metodologías de gestión ágiles.
- Experiencia en administración de sistemas, soporte y trabajo en organizaciones utilizando ITIL.

## Investigación y Desarrollo

El perfil de I+D se centra en el desarrollo y el análisis de sistemas. Los especialistas en I+D deben ser meticulosos y organizados y tener conocimiento en lenguajes de programación.

### FORMACIÓN

**Requerido**
- Título universitario en TI.
- Conocimiento de desarrollo de sistemas, familiaridad con al menos tres lenguajes de programación (Python, BashShell, PHP, C++, Java, etcétera).

**Se valorará**
- Cursos de especialización en seguridad cibernética y respuesta a incidentes de seguridad cibernética.
- Cursos de especialización en informática forense.
- Certificaciones en seguridad cibernética (CISSP, CISM, CISA).

### EXPERIENCIA

**Requerido**
- Más de cinco años de experiencia en posiciones técnicas en TI, Desarrollo de proyectos y seguridad cibernética.

**Se valorará**
- Experiencia en investigación y desarrollo.
- Experiencia en metodologías de gestión ágiles.
- Experiencia en trabajo con sistemas criptográficos y PKI.

## Tecnología de Información

Todos los técnicos en el CSIRT deberán tener experiencia y conocimiento en TI. Lo que diferencia al especialista encargado de TI es que estará orientado a tareas de administración de sistemas.

### FORMACIÓN

**Requerido**
- Título universitario o estudiante avanzado en TI.

**Se valorará**
- Cursos de especialización en seguridad cibernética y respuesta a incidentes de seguridad cibernética.
- Cursos de gestión basados en ITIL.

### EXPERIENCIA

**Requerido**
- Más de tres años de experiencia en posiciones técnicas en TI o como administrador de sistemas.

**Se valorará**
- Experiencia en organizaciones utilizando ITIL.
- Experiencia en metodologías de gestión ágiles.
- Experiencia en trabajo con sistemas criptográficos (PKI, PGP).

# B Requisitos de formación

En esta sección se describe la formación sugerida para cada uno de los miembros del personal del CSIRT nacional. Debe tenerse en cuenta que los cursos mencionados aquí pueden ser sustituidos o complementados por otros cursos similares que cubran temas comparables. Cabe destacar que en esta lista no se incluyen cursos ofrecidos por los fabricantes, sin embargo, son altamente provechosos para la formación del equipo del CSIRT.

Además, siempre es conveniente revisar opciones académicas como especializaciones de pregrado y de postgrado universitario disponibles, dependiendo del país o la región.

## Seguridad cibernética general

Las organizaciones International Information Systems Security Certification Consortium (ISC)² e Information Systems Audit and Control Association (ISACA) ofrecen algunas de las certificaciones de seguridad cibernética más respetadas y completas disponibles, en particular los títulos otorgados abarcan el Profesional Certificado en la Seguridad de Sistemas de Información (CISSP), el Gerente Certificado en la Información de Seguridad (CISM) y el Auditor de Sistemas de Información Certificada (CISA). Para más detalle se puede consultar su sitio web:

- → ISACA
- → (ISC)²

El Centro de Coordinación CERT (CERT-CC) de la Universidad Carnegie Mellon también tiene excelentes cursos de seguridad cibernética, incluyendo seguridad de la información para el personal técnico, muchos de los cuales están disponibles por medio de su plataforma de aprendizaje en línea.

## Capacitación en respuesta a incidentes en seguridad cibernética

Instituciones con amplia experiencia en temas de respuesta a incidentes de seguridad cibernética son la Universidad Carnegie Mellon (CMU) y el Instituto SANS.

CMU ofrece tanto cursos básicos como avanzados de manejo de incidentes cibernéticos. Los enlaces a estos cursos son los siguientes:

- → Fundamentals of Incident Handling
- → Advanced Incident Handling

El Instituto SANS ofrece la certificación en respuesta a incidentes y una multitud de otros cursos relacionados con la seguridad de la información, incluidos los que cubren técnicas de *hacking*, explotación y manejo de incidentes:

- → Incident response
- → Hacker Herramientas, Techniques, Exploits and Incident Handling

## Cursos de análisis de *malware* y forense

CMU y SANS son líderes mundiales en cursos sobre análisis de malware y forense, así:

- → CMU **Advanced Forensic Response and Analysis**
- → CMU **Malware Analysis Apprenticeship**
- → SANS **Advanced Computer Forensics and Incident Response, FOR 508**
- → SANS **Advanced Network Forensics and Analysis, FOR 572**
- → SANS **Reverse-Engineering Malware: Malware Analysis Herramientas and Techniques, FOR610**

# C Instalaciones e infraestructura TI

Esta sección describe los servicios básicos que el CSIRT debe tener, incluyendo la infraestructura de TI, arquitectura de red y diagramas. Es una de las muchas formas en que un CSIRT podría estructurar su plataforma.

Como regla general, las instalaciones del CSIRT y sus redes de datos y telecomunicaciones serán diseñadas orientadas a la protección no solo de la información confidencial recogida sino también de la protección al personal CSIRT. Esto significa que la información debe ser almacenada y gestionada por el propio CSIRT, en lugar de tener que subcontratar esta actividad o almacenar la información fuera del sitio o fuera del país.

## Instalaciones CSIRT

Debido a la sensibilidad de la información con la que trabaja, un CSIRT y sus empleados deben asegurarse de la misma manera que una organización protege un centro de datos. Esto significa que un CSIRT no puede estar en un ambiente de oficina abierta. Más bien, debe tener su propio espacio de oficina separada por paredes y puertas, para así reducir la posibilidad de que la información sensible sea vista o escuchada. Se debe limitar el acceso a las instalaciones del CSIRT con el fin de evitar el acceso no autorizado a los recursos y a la información. Con el mismo fin, el edificio o el área donde se encuentran las principales instalaciones CSIRT deben contar con vigilancia 24 horas.

Los servidores, los equipos de comunicaciones, los dispositivos de seguridad lógica y los repositorios de datos pueden permanecer en un centro de datos o en las instalaciones del CSIRT, pero en todos los casos, el acceso físico y lógico a los equipos se regirá por un estricto control de acceso que garantice que se respeten las políticas de acceso a la información. Además de asegurar la información electrónica, el CSIRT mantendrá un depósito de seguridad para almacenar información sensible no digital, fichas, discos duros y servidores, entre otros.

**Se debe limitar el acceso a las instalaciones del CSIRT con el fin de evitar el acceso no autorizado a los recursos y a la información.**

El siguiente diagrama muestra un ejemplo de un diseño de un CSIRT. El ejemplo debe servir como una guía para la creación de las instalaciones de un CSIRT; sin embargo, los países pueden construir su modelo sobre la base de sus necesidades y realidades logísticas.

### Consideraciones generales

→ **Equipamientos del espacio físico**

- Aire acondicionado y piso falso (principalmente para el centro de datos).
- Sistemas de detección y extintores en las salas comunes y en el centro de datos.
- Sistemas redundantes (fuente de Sistema de Alimentación Ininterrumpida (UPS), aire acondicionado, etcétera)
- Gabinetes de papelería bajo llave.

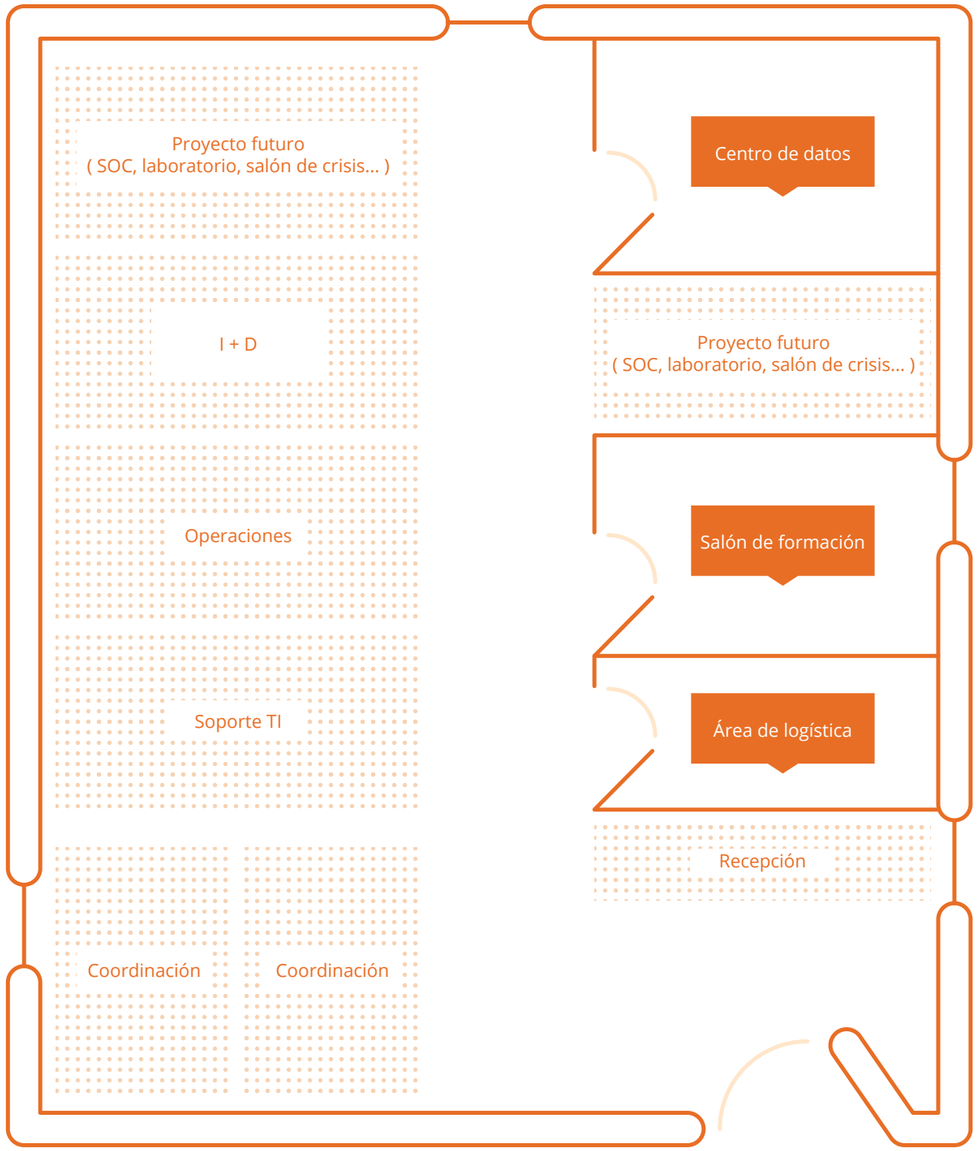
→ **Métodos para restringir el acceso físico a las distintas zonas**

- Acceso controlado a:
  - El edificio (puertas y ventanas).
  - El piso.
  - Zonas comunes (Operaciones, Soporte Informático, I+D, etcétera).
  - Centro de datos.
  - Área de Logística.
  - Proyectos futuros (laboratorio, sala de monitoreo).

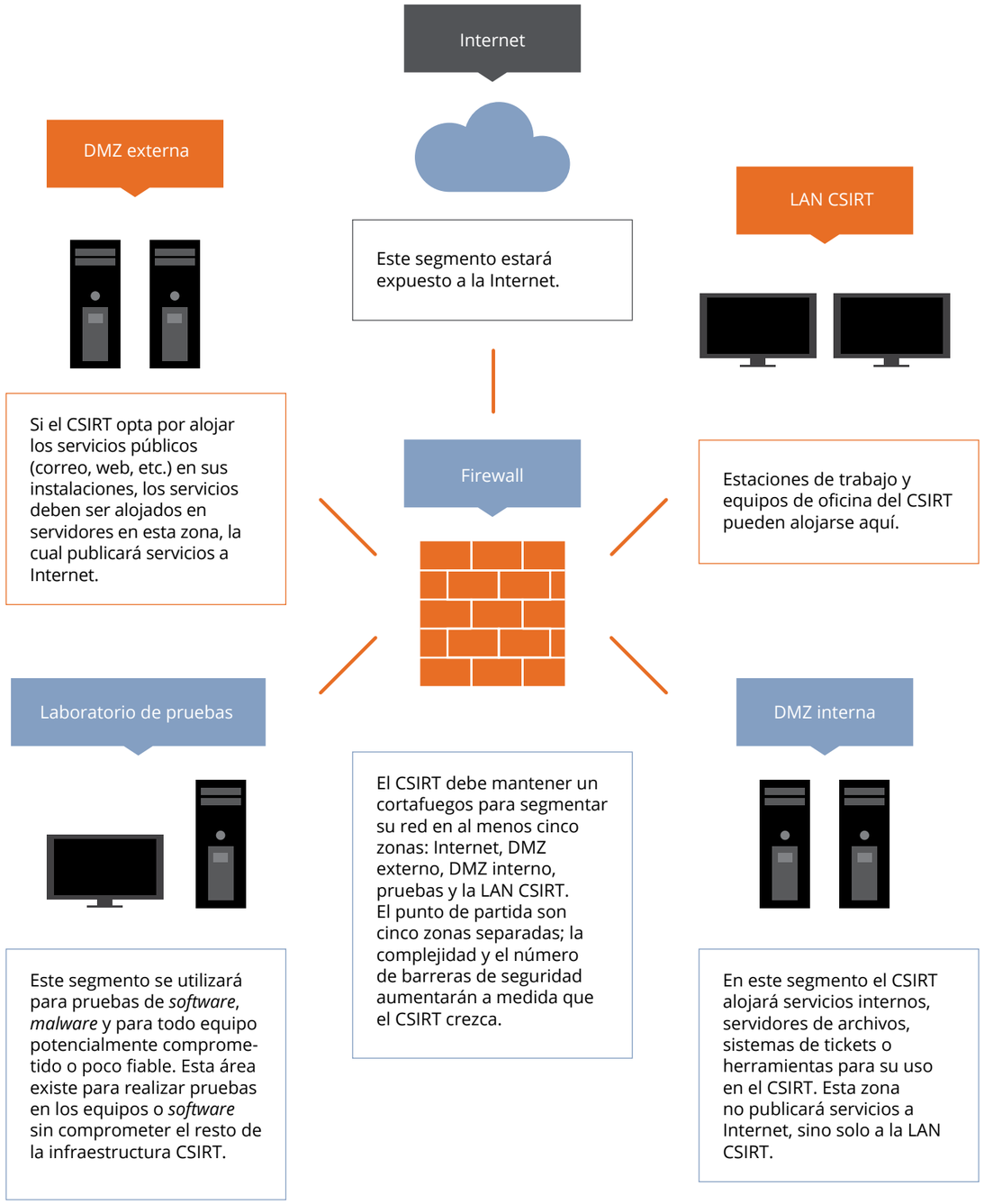
→ **Visitas restringidas (proveedores, etc.), acompañados todo el tiempo en todas las áreas CSIRT.**

→ **Vigilancia por medio de circuito cerrado de televisión.**

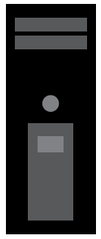
**Plano de planta básico**




# Diseño básico de la red CSIRT



# Equipo básico sugerido



## Computadores y servidores

Sistemas de *software* CSIRT, que incluyen lo siguiente:

**Servidor web institucional**

Este servidor contiene el sitio institucional donde se encuentra toda la información pública, no sensible en temas CSIRT, incluyendo alertas, boletines de noticias, contactos y formularios de notificación de incidentes.

**Servidor de correo institucional**

Este servidor se encarga de las comunicaciones por correo electrónico CSIRT y almacena los buzones de correo electrónico CSIRT.

**Servidor Intranet**

El propósito de este servidor es facilitar el intercambio de información entre el personal de CSIRT. Almacena datos relevantes para el equipo y los procedimientos, las técnicas de respuesta a incidentes, las mejores prácticas, los manuales de operación, la documentación de incidentes y otras informaciones de interés.

**Servidor de archivos**

Este servidor se utiliza para almacenar archivos digitales del equipo, que deben permanecer en línea y ser publicados dentro de las instalaciones del CSIRT.

**Copias de seguridad del servidor**

Este servidor tiene la tarea de realizar copia de seguridad de la información de todos los sistemas del CERT y estaciones de trabajo. Se generan copias de seguridad en bóveda fuera del sitio desde este equipo.

**Servidor DNS**

Este servidor es el responsable de la resolución de nombres de la infraestructura del CSIRT.

**Servidor de monitoreo**

El monitoreo activo de los sistemas se lleva a cabo en este servidor CSIRT, entre ellas: el monitoreo de los portales del gobierno y el de los servicios del CSIRT y sistemas de detección de vulnerabilidad de activos. Se recomienda que las consolas de monitoreo sean visibles para todo el personal del CSIRT.

**Recolección y correlación de eventos**

El papel de este servidor es concentrar los registros de transacciones de los sistemas del CSIRT, de la red de sensores desplegados por el CSIRT. Este servidor realiza la correlación de eventos y de alertas.

**Registro y seguimiento de incidentes**

Este es quizás el más importante de los servidores del CSIRT y está comprometido con el mantenimiento de registros y seguimiento de los incidentes del CSIRT. Registra informes de incidentes recibidos, las comunicaciones que entran y salen del CSIRT, relacionados con la respuesta a incidentes. También sirve como una fuente de conocimiento para el equipo. Cada correo electrónico enviado a la cuenta para reportar incidentes (por ejemplo. incidents@cert.xx), así como los formularios completados en el sitio web del CSIRT generarán automáticamente un ticket en el sistema de gestión. Estos sistemas tendrán la capacidad de adaptarse al procedimiento de gestión de incidentes que se vaya a utilizar, por ejemplo la creación de colas para la asignación y el escalamiento de tickets de incidentes.

## Computadores

El personal del CSIRT debe tener computadoras portátiles que se utilicen exclusivamente para funciones de trabajo.

## Teléfonos

El CSIRT tiene acceso directo a los servicios de telefonía, telefonía fija, telefonía IP y los teléfonos móviles, que le permiten hacer llamadas locales e internacionales según sea necesario para operar.



## Fax

Se recomienda que el CSIRT tenga una máquina de fax de uso exclusivo dentro de sus instalaciones con el fin de evitar que cualquier fax con información sensible sea visto por personal no autorizado.

## Triturador

El CSIRT debe tener una trituradora que le permita destruir información sensible impresa o discos compactos (CD). La destrucción de los materiales debe ser realizada por el personal del CSIRT, o como se indica en la política de destrucción de información.

## Almacenamiento lógico portátil

Durante la respuesta a incidentes, a menudo es necesario el uso de unidades externas o unidades *flash* para almacenar información. El CSIRT debe tener al menos cuatro unidades externas de 2 TB y cinco unidades de memoria *flash* de 32 GB.

# D Políticas y procedimientos operacionales

Las políticas CSIRT son fundamentales para su funcionamiento. Son directrices que deben ser seguidas por su personal en la realización de operaciones y reflejan a su vez las directrices de los patrocinadores del CSIRT, rigen el funcionamiento y las actividades del centro de respuesta y garantizan la confidencialidad, la disponibilidad y la integridad de la información y de los recursos CSIRT, así como la calidad de sus servicios.

Las políticas de un CSIRT, además de servir como guía para sus empleados y la comunidad objetivo, son recursos útiles para los miembros de la comunidad objetivo, ya que detallan cuándo un CSIRT proporciona qué tipo de servicios y cómo mantiene y protege la información que gestiona.

El mayor foro internacional de CSIRT en el mundo, la Organización FIRST, tiene las siguientes políticas obligatorias mínimas para un CSIRT que desee convertirse en un miembro de la comunidad.

## Políticas mínimas obligatorias

### Política de clasificación de información

Esta política define cómo el CSIRT clasifica la información basado en distintos niveles de criticidad.

### Política de protección de datos

Esta política define la forma de proteger la información de acuerdo a su criticidad.

### Política de retención de información

Esta política define el tiempo que el CSIRT debe mantener registros u otra información de que disponga.

### Política de destrucción de información

Esta política define cómo el CSIRT destruye información, registros, medios, dispositivos, etc., para garantizar que la información esté protegida cuando su ciclo de vida o los medios que lo contienen llegan a su fin.

### Política de divulgación de información

Esta política debe especificar cómo y cuándo el CSIRT puede compartir o distribuir la información interna o externamente.

### Política sobre el acceso a la información

Esta política establece quién puede acceder a la información del CSIRT, teniendo en cuenta el personal, miembros de la comunidad objetivo o el personal de la organización matriz del CSIRT (si lo tiene).

### Políticas de uso apropiado de los sistemas del CSIRT

Esta política define el uso aceptable de los sistemas y recursos del CSIRT.

### Definición de incidentes de seguridad y política de eventos

Esta política describe los criterios que determinan la definición de un evento o incidente de seguridad y la clasificación de cada uno según el tipo y la gravedad.

### Política de gestión de incidentes

Esta política debe definir cómo se lleva a cabo la gestión de incidentes, incluyendo el tipo de incidentes a los que el CSIRT responderá, el tiempo de respuesta aceptables, los procedimientos que se van a aplicar, etcétera.

### Política de cooperación

Esta política define las otras entidades con las que cooperará el CSIRT y cómo lo harán, particularmente otros equipos de respuesta a incidentes. <

## Otras políticas

Además de las políticas mínimas requeridas para un CSIRT, puede haber otras con el fin de mejorar la calidad de los servicios y el funcionamiento del centro:

- Política de uso de Internet.
- Política de notificación de incidentes.
- Política de comunicación del CSIRT.
- Política de capacitación y entrenamiento.
- Política de seguridad de computador personal.
- Política de seguridad de la red.
- Política de uso de correo electrónico.
- Política de uso de dispositivos móviles.
- Política de seguridad de equipo de telecomunicaciones.
- Política de copias de seguridad.
- Política de segregación de funciones.
- Política de control de cambio.
- Política de contraseñas.

Los anexos contienen más ejemplos de políticas.

3 CIERRE

## El cierre del proyecto se produce cuando toda la información generada en el proceso de creación del CSIRT, incluida su integridad, es analizada y verificada. Después de que el proceso de cierre esté completo, se habrá establecido formalmente el CSIRT nacional.

Al cerrar el proceso de creación, el Gerente de Proyectos CSIRT tendrá:

- Lista de interesados.
- Documentos de constitución del CSIRT (misión, visión, servicios, etcétera).
- Documentos legales de la creación del CSIRT.
- Instalaciones físicas, contratos de alquiler, etcétera.
- Recursos humanos contratados y capacitados.
- Manual de operaciones con políticas y procedimientos.
- Infraestructura tecnológica y los respectivos contratos de soporte

Además, se redactarán otros documentos durante la fase de establecimiento, incluyendo la definición de alcance, el cronograma y el presupuesto. Se debe convocar al equipo del proyecto a una sesión informativa para analizar las lecciones aprendidas y dónde se podría mejorar el proceso.

Por último, con toda la información generada, es esencial hacer un informe final que contenga:

- Objetivo general del proyecto.
- Actividades realizadas.
- Desempeño del proyecto (alcance, cronograma, presupuesto).
- Lecciones aprendidas.
- Recomendaciones futuras.

Este informe se adjuntará a la documentación del proyecto y le dará su cierre formal.

### Finalización formal de las actividades

Durante la planificación, el equipo del proyecto establece medidas claras para ser llevadas a cabo durante la ejecución del proyecto. Cada uno de ellos tiene un claro indicador de finalización, como “recursos humanos capacitados”. Para registrar la actividad como formalmente completada, el equipo del proyecto debe verificar que todo el personal necesario recibió el entrenamiento y luego recoger la documentación apropiada. Del mismo modo, todos los contratos y acuerdos de servicio deben ser verificados y tener la aprobación legal y la documentación necesaria.

**Por último, el informe final debe ser aprobado por el patrocinador del proyecto con el fin de completar la fase de implementación del CSIRT.**

# ANEXOS

# Muestra de la política de uso aceptable

**OBJETIVO**

El propósito de esta política es establecer usos aceptables e inaceptables de los dispositivos electrónicos y recursos de red que pertenecen a CSIRT-XX. Se ha formulado para cumplir con las normas legales y éticas establecidas y se basa en la confianza, la integridad y la transparencia de las actividades del CSIRT.

El CSIRT-XX opera dispositivos de computación, redes y otros sistemas de información con el fin de llevar a cabo sus mandatos, sus objetivos y sus iniciativas. Todos estos dispositivos deben ser gestionados de manera responsable para mantener la confidencialidad, la integridad y la disponibilidad de los activos de información que CSIRT-XX tiene en su poder o con los que trabaja.

Esta política requiere que los usuarios de los dispositivos y recursos de la red acepten y cumplan con las políticas definidas, a fin de proteger el CSIRT-XX, su personal, sus operaciones y sus socios, de los daños y demandas.

**ALCANCE**

Todos los empleados, contratistas, consultores, pasantes y otros que trabajan directa o indirectamente en CSIRTXX, incluyendo todo el personal afiliado a terceros, deben cumplir con esta política. Esta se aplica a los activos de información que son propiedad de o arrendados por CSIRT-XX, o a dispositivos que se conectan a la red del CSIRT-XX o que están alojados en un sitio que pertenece al CSIRT-XX.

En circunstancias atenuantes, la administración del CSIRT-XX puede aprobar excepciones que serían contrarias a esta política. Cualquier excepción debe ser aprobada formalmente por escrito e incluir una justificación y una evaluación de los posibles riesgos de tal excepción.

**DECLARACIÓN DE LA POLÍTICA**

### Requerimientos generales

Como empleado de CSIRT-XX, usted es responsable de ejercer el buen juicio con respecto al uso apropiado de los recursos CSIRT-XX de conformidad con las políticas y los procedimientos establecidos por el CSIRT-XX. Los recursos CSIRT-XX no pueden ser utilizados con fines ilícitos o que estén en violación de la Política de Ética de CSIRT-XX.

### Cuentas del sistema

Usted es responsable de la seguridad de los datos, las cuentas y los sistemas bajo su control. Mantenga contraseñas seguras y no comparta su información de cuenta o contraseña con nadie, incluyendo otros empleados, familiares o amigos. Facilitarle el acceso a otra persona, ya sea intencionalmente o debido a la falta de garantías de acceso, es una violación de esta política. Usted debe mantener un nivel de contraseña de usuarios y del sistema de acuerdo con las directivas de contraseña.

Usted debe asegurarse, por medios legales o tecnológicos, que la información con la que trabaja se mantiene bajo el control y la gestión de CSIRT-XX en todo momento. El almacenamiento, el acceso o el uso de información confidencial en ambientes o aplicaciones administradas por un tercero o no directamente operados o controlados por CSIRT-XX están prohibidos. Esto incluye los dispositivos que son mantenidos por terceros con los que no hay acuerdo contractual. Además, esto prohíbe específicamente el uso de una cuenta de correo electrónico que no ha sido proporcionada por el CSIRTxx para intercambiar información propiedad de la CSIRTxx.

### Activos informáticos

Usted es responsable de garantizar la protección de los activos que le fueron asignados por CSIRT-XX. Esto incluye el uso de cables de bloqueo del computador y cualquier otro dispositivo de seguridad. Computadores portátiles que se queden por la noche en el CSIRT-XX deben ser colocados en un cajón cerrado con llave o un armario. Cualquier robo o pérdida de equipo debe ser reportada a la administración de CSIRT-XX inmediatamente.

Todas las estaciones de trabajo y dispositivos personales deben asegurarse con un protector de pantalla protegido por contraseña, y usted debe bloquear la pantalla o cerrar la sesión cuando esté desatendida la estación de trabajo o dispositivo. Por otra parte, la función de bloqueo automático se debe activar tal como se establece en el procedimiento de configuración de estación de trabajo. Cualquier dispositivo que se conecte a la red CSIRT-XX debe cumplir con la política de acceso mínimo.

### Uso de comunicaciones electrónicas e Internet

Usted es responsable de la seguridad y el uso adecuado de los recursos de red y de las herramientas bajo su control. Queda terminantemente prohibida la utilización de los recursos que:

- causen un fallo de seguridad o violación de uno o más recursos de red CSIRT-XX;
- causen una interrupción del servicio a uno o más recursos de red CSIRT-XX;
- violen las disposiciones de la ley de derechos de autor;
- violen las políticas de seguridad establecidas de las leyes locales;
- apoyen cualquier actividad ilegal, incluyendo la transmisión o ayuda en la transmisión de material que viole las políticas que protegen la información confidencial o de propiedad; y
- tergiversen, ofusquen, eliminen o sustituyan una identidad de usuario en cualquier comunicación electrónica con el fin de inducir a error al destinatario sobre quién es el remitente.

Por último, usted debe ejercer buen juicio para evitar tergiversar o exceder su autoridad en la representación de las opiniones de los CSIRT-XX al público.

**IMPLEMENTACIÓN**

Un empleado que se encuentre en violación de esta política o de cualquier otra política del CSIRT-XX estará sujeto a medidas disciplinarias, que pueden incluir el despido. Una violación de esta política por un empleado temporal, contratista o proveedor puede resultar en la terminación del contrato o cesión con CSIRT-XX.

# Política de divulgación

**OBJETIVO**

Definir qué información puede ser revelada a quién, cómo y en qué circunstancias, incluyendo las partes interesadas, socios CSIRT, otros órganos del gobierno, o incluso otros miembros del CSIRT-XX. La manera en que se comparta la información se hará de acuerdo a su nivel de clasificación.

**ALCANCE**

Toda la información en poder o generada por el CSIRT-XX.

**DECLARACIÓN DE LA POLÍTICA**

### Información pública

La divulgación de información pública está autorizada, aunque debe ser difundida por medio de los canales establecidos y gestionada por las comunicaciones o la unidad de asuntos públicos de CSIRT-XX, y se hará de acuerdo con los procedimientos de esa unidad.

### Información clasificada

La información clasificada solo podrá ser divulgada cuando sea autorizada por el director del CSIRT-XX o su designado. En todos los casos, se firmará un acuerdo de no divulgación, que establece que cualquier destinatario de información clasificada será debidamente notificado de la clasificación de la información que está recibiendo.

### Información clasificada de uso comunitario

La información que es clasificada pero aprobada para su difusión dentro de la comunidad es un tipo especial de información. Todas las consideraciones anteriormente mencionadas siguen siendo válidas, salvo que la divulgación que realizan ciertos miembros de la comunidad objetivo sea autorizada por el director de CSIRT-XX.

### Información confidencial

El CSIRT-XX y su personal no divulgarán información confidencial. Si, por razones operativas, se hace necesario compartir información confidencial con terceros, usted deberá obtener el consentimiento del propietario de la información, que podrá autorizar la divulgación o no. Si el propietario lo autoriza, se le exigirá al receptor firmar un acuerdo de no divulgación, ya sea proporcionado por el propietario de la información o por el CSIRT.

### Información secreta

En ningún caso el CSIRT-XX revelará información secreta por la ley.

### Información incompleta/no terminada

La información que se encuentra en borrador, y que no contiene información confidencial, puede ser revelada individualmente siguiendo las directrices definidas para este fin.

**DIVULGACIÓN INTERNA**

Dentro del equipo CSIRT-XX no habrá limitaciones en la divulgación ni en el intercambio de información, a menos que se haga una petición expresa por parte del director con respecto a una acción específica. Como parte de los requisitos operativos diarios, el CSIRT-XX revelará cierta información a los miembros de la organización. Cualquier divulgación deberá tener en cuenta los procedimientos establecidos de acuerdo con la clasificación de la información de que se trate; la divulgación de información sensible debe ser autorizada por el director del CSIRT-XX o su designado.

**ASPECTOS LEGALES**

El CSIRT-XX cumplirá con toda la legislación nacional o política de la organización para responder a todas las peticiones de información por parte de terceros. Dichas solicitudes de información deben hacerse por medio del departamento jurídico o el asesor del CSIRT-XX.

**INFORMACIÓN DE PEDIDOS**

### Grupos de respuesta a incidentes

La cooperación y el intercambio de información con otros grupos de respuesta a incidentes son vitales para el funcionamiento y la supervivencia de CSIRT-XX y la comunidad nacional e internacional más amplia de los equipos de respuesta a incidentes de seguridad informática. La mayor cantidad de información posible será compartida con otros grupos de respuesta, de acuerdo con esta política, mediante la evaluación de cada caso de forma individual y con el permiso del director de CSIRT-XX o su designado.

### Prensa

La comunicación y el enlace con la prensa serán coordinados y realizados exclusivamente por el portavoz designado de CSIRT-XX, con la aprobación previa del director de CSIRT-XX o su designado. Cuando sean contactados por un representante de la prensa, todos los miembros del CSIRT-XX trasladarán las solicitudes al portavoz, lo que indica que no están autorizados a divulgar información y no revelarán ninguna información en ninguna circunstancia, independientemente de la clasificación de la información en cuestión.

**COMUNICADO DE PRENSA DE INFORMACIÓN SENSIBLE**

Cuando sea necesario, la información confidencial será divulgada de tal manera que evite el acceso a esta por un tercero no autorizado.

# Formatos de respuesta a incidentes

## 1 Defacement Incident Response Form

DEFACEMENT INCIDENT RESPONSE FORM

**GENERAL INFORMATION**

**FOLIO:** _____

**Name:** | **Position:**

**Office:** | **Contact Phone No:**

**Institutional e-mail:** | **Personal e-mail (optional):**

**Date and Time of Report:** | **Agent of the Case or Incident:**

**Brief description of the facts:**

**GENERAL INFORMATION OF THE COMPROMISED EQUIPMENT**

**Operating System:** | **Hard Drive Capacity:**

**RAM Capacity:** | **Network Interfaces (add IP addresses):**

**Kernel Version:** | **Time Zone of the Compromised System:**

**Additional Information:**



DEFACEMENT INCIDENT RESPONSE FORM

**INFORMATION FOR ANALYSIS**

1. Put the URL of the compromised site:
2. Take a screenshot of the compromised system (if it is still possible to retrieve such evidence) and save it as a jpg file.
3. Save the records of the compromised web server in a TXT file (at least two days before the incident was registered and two days after, if applicable) and compress it with a .zip extension, entering the password "*defacement2014*".
4. If applicable, send the handler and the version of the Database:
   Send the list of updates installed on the compromised server. This updates list can be obtained with the aid of a tool. Save the file where the list is generated.
5. Additional Information (optional):

**7.-** Send the information gathered as attachments via email to the account of your national incident response team along with this form, indicating the email subject as *"defacement incident folio: XXX"* where XXX is the folio assigned to this incident.

## 2 Unit Linux Intrusion Detection Incident Response Form

UNIX LINUX INTRUSION DETECTION INCIDENT RESPONSE FORM

### GENERAL INFORMATION

FOLIO: _____

**Name:** | **Position:**

**Office:** | **Contact Phone No:**

**Institutional e-mail:** | **Personal e-mail (optional):**

**Date and Time of Report:** | **Agent of the Case or Incident:**

**Brief description of the facts:**

### GENERAL INFORMATION OF THE COMPROMISED EQUIPMENT

**Operating System:** | **Hard Drive Capacity:**

**RAM Capacity:** | **Network Interfaces (add IP addresses):**

**Kernel Version:** | **Time Zone of the Compromised System:**

**Additional Information:**



UNIX LINUX INTRUSION DETECTION INCIDENT RESPONSE FORM

### INFORMATION FOR ANALYSIS

Run the following commands and save the results to a TXT file.

| Command | Description |
|---|---|
| **Identification of the operating system** | |
| **uname -a** | Provides: Name, version, date and time of installation |
| **hostname** | Name of equipment |
| **lscpu** | Kernel information |
| **lsb_release –a**<br>**RedHat: cat /etc/redhat-release** | Displays distribution and system version |
| **date** | Current date and time of the system (option –u shows universal time zone) |
| **who -b** | Date and time the system was started |
| **df –h**<br>**hdparm [/dev/DISCO]**<br>**dmes \| grep hd** | Hard drive information |
| **fdisk -l** | List of partitions per disk (root) |
| **free –o –m** | State of RAM and SWAP memory |
| **smbclient –L nom-equipo**<br>**Red Hat: net –l share –S nom-equipo** | See which shared resources are on the equipment |
| **dumpe2fs -h /dev/sda1 \| grep created**<br>**ls -lct /etc/ \| tail -1 \| awk '{print $6. $7, $8}'**<br>**Red Hat: install.log** | Date of operating system installation (root)<br>The install.log file provides information on when the OS was installed |
| **Mount** | Devices mounted on the system |

| | |
|---|---|
| **df**<br>**Red hat: /etc/mtab**<br>**/proc/mounts** | |
| **RAM extraction** | |
| **dd if=/dev/mem of=direc-destino** | Generates a copy of RAM memory |
| **objdump [Binario]** | Obtains information of a binary |
| **fsstat -f linux-ext2 [Rutalmagen.dd]** | General image information |
| **Xxd [Imagen]** | General image information |
| **Creación de Imagen** | |
| **dd** | Clones partitions or hard drives |
| **EnCase** | Forensic tool that helps create images |
| **FTK Imager** | Forensic tool, helps create images |
| **Information of applications and services** | |
| **ps -fe** | System processes (option -fe is used for standard syntaxes) |
| **dpkg -l**<br>**Red Hat: rpm -qa** | Installed applications and updates |
| **service --status-all** | See system services |
| | |
| **Network Information** | |
| **ifconfig -a** | Network Interfaces, IP addresses, netmask and gateway |
| **netstat -nap** | Active connections list on the system |
| **arp -a** | Relation of IP with MAC Address |
| | |
| **Iptables –L**<br>**Red Hat: /etc/sysconfig/iptables**<br>**/etc/sysconfig/ip6tables** | Firewall configuration (root) |





| | |
|---|---|
| **lsof -i** | Files open on the network (root) |
| **findsmb** | NetBIOS configurations |
| **/etc/resolv.conf** | DNS Servers |
| **User Information** | |
| **cat /etc/passwd** | List of users registered in the system |
| **w** | Active users in the system |
| **last** | Last users that used the system |
| **cat /etc/passwd**<br>**cat /etc/group**<br>**cat /etc/shadow** | User files, groups and passwords (to view them you should have administrator privileges) |
| **whoami** | Current system user |

1. Copy the file records listed below (when applicable) to a TXT file:
   - /var/log/auth.log (for Operating System: DEBIAN, UBUNTU, LINUX MINT)
   - /var/log/secure (for Operating System: RED HAT, FEDORA, CENTOS)
   - /var/log/httpd/error.log (for Operating System: RHEL, RED HAT, CENTOS and FEDORA)
   - /var/log/mysqld.log (for Operating System: RED HAT, RHEL, CENTOS, FEDORA)

   For Operating System: DEBIAN and UBUNTU:
   - /etc/log/apache2/acceses.log
   - /var/log/mysql.log
   - /var/log/mysqld.error.log
   - /usr/local/uce/server/logs/audit.log
   - /usr/local/uce/server/logs/error.log
   - /home/nombredeusuario/.mozilla/firefox/archivo_aleatorio.default/places.sqlite

2. Additional Information (optional):

**UNIX LINUX INTRUSION DETECTION INCIDENT RESPONSE FORM**

**4.-** Send the TXT files generated via email to the account of your country's incident response team along with this form, indicating the email subject as *"intrusion detection in Unix Linux incident folio: XXX"* where XXX is the folio assigned to this incident.





## 3 Information Leak Incident Response Form

**INFORMATION LEAK INCIDENT RESPONSE FORM**

### GENERAL INFORMATION

**FOLIO:** _____

**Name:** _____ **Position:** _____

**Office:** _____ **Contact Phone No:** _____

**Institutional e-mail:** _____ **Personal e-mail (optional):** _____

**Date and Time of Report:** _____ **Agent of the Case or Incident:** _____

**Brief description of the facts:** _____

_____

_____

### GENERAL INFORMATION OF THE COMPROMISED DOMAIN (IF APPLICABLE)

**Operating System:** _____ **Hard Drive Capacity:** _____

**RAM Capacity:** _____ **Network Interfaces (add IP addresses):** _____

**Kernel Version:** _____ **Time Zone of the Compromised System:** _____

**Additional Information:** _____

_____

_____

## 4 Phishing Incident Response Form

PHISHING INCIDENT RESPONSE FORM

### GENERAL INFORMATION

**FOLIO:** _____

**Name:** _____ **Position:** _____

**Office:** _____ **Contact Phone No:** _____

**Institutional e-mail:** _____ **Personal e-mail (optional):** _____

**Date and Time of Report:** _____ **Agent of the Case or Incident:** _____

**Brief description of the facts:** _____

_____

_____

### GENERAL INFORMATION OF THE COMPROMISED DOMAIN

**Operating System:** _____ **Hard Drive Capacity:** _____

**RAM Capacity:** _____ **Network Interfaces (add IP addresses):** _____

**Kernel Version:** _____ **Time Zone of the Compromised System:** _____

**Additional Information:** _____

_____

_____



INFORMATION LEAK INCIDENT RESPONSE FORM

### INFORMATION FOR ANALYSIS

1. Put the URL where the compromised information is posted:

   _____

2. Take a screenshot of the website posting the extracted information and save it as a jpg file.

3. Additional incident information (optional):

4.- Send the information via email to the account of your country's computer security incident response team along with this form, indicating the email subject as *"information leak incident folio: XXX"* where XXX is the folio assigned to this incident. (who provides the folio number)

**PHISHING INCIDENT RESPONSE FORM**

**INFORMATION FOR ANALYSIS**

1. Put the URL of the apocryphal site:

   _____

   If the fake site is hosted on one of your servers, compress the files in the directory where the phishing site was mounted (phishing kit) on a file with .zip extension entering the password "*phishing2014*".
2. If you have access to the server that was breached to put the fake site, save your web server logs (at least two days before the incident was registered and two days after, if applicable) to a TXT file and compress them with a .zip extension and enter the password "*phishing2014*".

3. Write the handler and the database version, if applicable:

   _____

4. If the phishing arrived via a fake email, store the email headers and forward the phishing email (if applicable) to the email account of your national incident response team.

5. Additional Information (optional):

6.- Send the information gathered as attachments via email to the account of your national CERT along with this form, indicating the email subject as *"phishing incident folio: XXX"* where XXX is the folio assigned to this incident.

**2**



# Referencias


**1.** Centro Criptológico Nacional: Guía de Creación de un CERT/CSIRT (CCN-STIC-810): España, 2011.

**2.** CERT Program at the Software Engineering Institute: FIRST Site Visit Requirements and Assessment: Estados Unidos, Carnegie Mellon University, 2013.

**3.** CERT Program at the Software Engineering Institute CMU: Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability: Estados Unidos, Carnegie Mellon, 2011.

**4.** CERT/CC: CMU Creating and Managing CSIRTs: Estados Unidos, Carnegie Mellon, 2004.

**5.** Charles W. L. HILL y Gareth R. JONES: Administración estratégica. Un enfoque integrado. Santa Fé de Bogotá: McGraw – Hill Interamericana S.A., 1996.

**6.** ENISA: Good Practice Guide for Incident Management: Unión Europea, ENISA, 2010.

**7.** Baseline Capabilities of National/Governmental CERT: Unión Europea, ENISA, 2012.

**8.** Georgia Killcrece et al: Organizational Models for Computer Security Incident Response Teams (CSIRT). Estados Unidos, Carnegie Mellon, 2003.

**9.** Jack Fleitman: Negocios exitosos: México, Interamericana McGraw Hill, 2000.

**10.** Moira J. West-Brown, et al: Handbook for Computer Security Incident Response Team. Estados Unidos, Carnegie Mellon, 2003.

**11.** Orión Aramayo: Manual de planificación estratégica. Chile, Universidad de Chile, 2009.

**12.** Rubén Aquino Luna et al: Manual de gestión de incidentes de seguridad informática. AMPARO y LACNIC.

## Notas finales


**1.** Guía de Buenas Prácticas en la Gestión de Incidentes (2010). http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management.

**2.** Guía de Creación de un CERT/CSIRT (CCN-STIC-810) del Centro Criptológico Nacional de España.

**3.** Baseline Capabilities of National/Governmental CERTs: Unión Europea, ENISA, 2012.

**4.** Guía de Creación de un CERT/CSIRT (CCN-STIC-810) del Centro Criptológico Nacional de España.

**5.** CERT Program at the Software Engineering Institute CMU: Best Practices for National Cyber Security.

**6.** John M. Bryson, en su artículo "Stakeholder Identification and Analysis Techniques".

**7.** Handbook for Computer Security Incident Response Team: Carnegie Mellon University.

**8.** Charles W. L. Hill y Gareth R. Jones, Administración estratégica: Un enfoque integrado. Santa Fe de Bogotá: McGraw – Hill Interamericana S.A.

**9.** Handbook for Computer Security Incident Response Team: Estados Unidos, Carnegie Mellon, 2003.

**10.** Negocios exitosos: México, Interamericana McGraw Hill, 2000

**11.** Orión Aramayo, Manual de Planificación Estratégica, Universidad de Chile.

**12.** Handbook for Computer Security Incident Response Team: Estados Unidos, Carnegie Mellon, 2003.

**13.** "Home", Centro Criptológico Nacional de España, visitada el 21 de diciembre de 2015, https://www.ccn.cni.es/.

**14.** Handbook for Computer Security Incident Response Team: Estados Unidos, Carnegie Mellon, 2003.

**15.** Organizational Models for Computer Security Incident Response Teams (CSIRT): Estados Unidos, Carnegie Mellon, 2003.

**16.** Manual de gestión de incidentes de seguridad informática: AMPARO y LACNIC.

**17.** Manual de gestión de incidentes de seguridad informática. AMPARO y LACNIC.

**18.** http://www.enisa.europa.eu/activities/cert/support/guide2/internal-management/structure

**19.** CMU Creating and Managing CSIRT: EE.UU., Carnegie Mellon, 2004.

**20.** Es común que los "servicios de soporte" se apoyen en los departamentos financieros, de comunicación y legales de la institución que alberga el CSIRT.

**21.** Instituto de gestión de proyectos PMBOK.

**Secretario General**
Luis Almagro Lemes

**Secretario General Adjunto**
Nestor Mendez

BUENAS PRÁCTICAS
PARA EL ESTABLECIMIENTO DE UN CSIRT NACIONAL

**Secretario Ejecutivo del Comité Interamericano Contra el Terrorismo**
Alfred Schandlbauer

**Desarrollado por**
Ignacio Lagomarsino
Santiago Paz

**Coordinación de Proyecto**
Diego Subero
Belisario Contreras

**Editores**
Pablo Martinez
Kerry-Ann Barrett
Robert Fain
Barbara Marchiori
Geraldine Vivanco

**Contribuidores**
Brian Dito
Yezyd Donoso
Luis Fuentes
Gonzalo Garcia-Belenguer
José María Gómez de la Torre
Catalina Lillo
Raul Millan
Emmanuelle Pelletier
Francisco Javier Villa

Departamento de Seguridad Nacional de los Estados Unidos
Policía Federal de México


Organización de los
Estados Americanos

Más derechos para más gente