Foro sobre los equipos de seguridad e intervención en caso de incidente (FIRST.Org)

Primavera de 2016 | 16

Marco de servicios del equipo de intervención en caso de incidentes de seguridad (SIRT)

Versión 1.0

Marco de servicios del equipo de intervención en caso de incidentes de seguridad (SIRT)

Introducción

En el presente documento se enumeran y definen los servicios que una organización con equipo de intervención en caso de incidentes de seguridad (SIRT) puede aplicar para satisfacer las necesidades de sus mandantes, así como los mecanismos para solventar las dificultades vinculadas a este propósito. El objetivo de esta lista es presentar los servicios tradicionales que prestan los SIRT así como los servicios de reciente aparición que están ofreciendo los equipos y organizaciones existentes a medida que evolucionan. El presente documento es por tanto una lista de los servicios que deberían figurar en todo marco de servicios SIRT.

Cada uno de estos servicios se divide en funciones primarias y subfunciones que dan soporte a las prestaciones de SIRT de ese servicio y contribuyen a llevar a cabo su cometido general. Aunque se presentan aquí como únicas, muchas de las funciones y subfunciones se utilizan para realizar varios servicios y/o funciones y pueden ser interdependientes. En el presente documento se pone de manifiesto la existencia de estas relaciones, pero no se aborda su definición.

En el futuro los servicios se agruparán según sus similitudes dentro de una esfera de servicios. La primera parte del presente documento se centra en tres tipos de equipos de intervención en caso de incidentes: CSIRT nacionales, CSIRT sectoriales (infraestructuras fundamentales) y CSIRT empresariales (organizativo). En una próxima versión del marco de servicios se incluirán otros dos tipos: equipos de intervención en caso de incidentes de seguridad de productos (PSIRT), e intervención en caso de incidentes regionales/multipartitos. En futuros documentos conexos se mostrarán ejemplares para cada tipo, y para las esferas de servicio/servicios/funciones más habituales en la creación de un programa base. A fin de preparar los módulos de formación se publicará también otro documento en el que se describan las tareas, subtareas y acciones de cada subfunción. A fin de trabajar de forma consensuada a escala mundial se están coordinando grados de madurez con muchas otras partes.

Finalidad

En el marco de servicios CSIRT se define un conjunto de servicios y funciones que aplican los CSIRT para dar servicio a sus mandantes. El objeto de este marco es facilitar la formación y la educación, las actividades de desarrollo de la capacidad mundial y la interoperabilidad de los CSIRT utilizando

una terminología y un planteamiento aceptados por la comunidad internacional acerca del funcionamiento de los CSIRT.

Historia

En muchos casos se ha recurrido a la lista de servicios CERT/CC CSIRT para describir de manera coherente y comparable los CSIRT y sus correspondientes servicios. Recientemente se evaluaron las listas de servicios CSIRT existentes y se concluyó que la lista CERT/CC, aunque se adaptaba y utilizaba ampliamente, había quedado obsoleta y carecía de los componentes fundamentales que representan la misión de los actuales CSIRT. El Foro FIRST, interesado en el desarrollo y la consolidación de los CSIRT en todo el mundo, señaló que este era un factor fundamental en la elaboración de un programa completo de formación CSIRT. Teniendo en cuenta el alcance geográfico y funcional de los miembros del FIRST, se decidió que su comunidad sería una fuente adecuada para describir y representar definitivamente los servicios prestados por los CSIRT. También se decidió que se necesitaba un planteamiento similar para los servicios CSIRT, y que éste se incorporaría a una versión futura del presente marco de servicios.

Definiciones

A continuación se definen ciertos términos utilizados en el presente documento. Las esferas de servicios, los servicios y las funciones definen *lo que* se hace a diferentes niveles de detalle, y las tareas y acciones definen *el cómo* se hace, también a diferentes niveles de detalle. Las tareas y acciones se publican en un documento adjunto que puede actualizarse, y se actualizará, con mayor frecuencia:

- **Esfera de servicios –** grupo de servicios relativos a un aspecto común. Ayudan a organizar los servicios en una clasificación general con miras a facilitar su comprensión. (Esta área seguirá desarrollándose en la versión 2.0).
- **Servicio** – Conjunto de acciones coherentes y reconocibles encaminadas a un resultado determinado para los mandantes de un equipo de intervención en caso de incidentes, o en su nombre. Lista de funciones utilizadas para realizar el servicio.
- **Función** – Medio para cumplir el propósito o la tarea de un servicio determinado. Lista de tareas que pueden realizarse por dicha función.
- **Tareas –** Lista de acciones que deben realizarse para realizar la tarea.

- **Acciones –** Lista del modo de actuar en diferentes niveles de detalle/madurez.

- **Capacidad** – Actividad cuantificable que se realiza con arreglo a los roles y responsabilidades de una organización. A los efectos del marco de servicios SIRT, las capacidades pueden definirse como servicios más amplios o como las funciones, subfunciones, tareas o acciones necesarias.

- **Volumen de capacidad** – Número de veces que una organización puede ejecutar una determinada capacidad antes de agotar los recursos de algún modo.

- Madurez – Grado de eficacia con el que una organización ejecuta una capacidad particular con arreglo a su cometido y potestades. Constituye el nivel de competencias adquiridas en acciones o tareas, o en un conjunto de funciones o servicios.

Tipos de equipos de intervención en caso de incidentes

- CSIRT (equipo de intervención en caso de incidentes de seguridad informática) nacional – Entidad constituida por una autoridad nacional para coordinar incidentes de ciberseguridad a nivel nacional. Por lo general entre sus mandantes se encuentran todos los organismos y departamentos gubernamentales, las fuerzas del orden público y la sociedad civil. También suele ser la autoridad para interactuar con los CSIRT nacionales de otros países, así como con actores regionales e internacionales.

- CSIRT sectorial / infraestructura fundamental – Encargado de supervisar, gestionar e intervenir en caso de incidentes de ciberseguridad relativos a un sector determinado (por ejemplo, energía, telecomunicaciones o finanzas).

- CSIRT empresarial (organizativo) – Suele ser un equipo encargado de supervisar, gestionar e intervenir en caso de incidentes de ciberseguridad que afectan a las infraestructuras y servicios TIC internos de una organización determinada.

- CSIRT regional/multipartito – Equipo o matriz de equipos encargados de supervisar, gestionar e intervenir en caso de incidentes de ciberseguridad relativos a una región determinada o a un número de organizaciones.

- Equipo de intervención en caso de incidentes de seguridad de productos (PSIRT) – Equipo dentro de una entidad comercial (normalmente un operador) que gestiona la recepción, investigación y la notificación interna o pública, de información de seguridad sobre vulnerabilidades relativas a productos o servicios comercializados por esa organización.

Service 1 Gestión de incidentes

Función 1.1 **Gestión de incidentes:** servicios relativos a la gestión de un ciberevento destinados a incorporar a los mandantes que lanzan la alerta y las actividades de coordinación relacionadas con la respuesta, la mitigación y la recuperación en caso de incidente. La gestión de incidentes depende de las actividades de análisis que se definen en la sección "Análisis".

Subfunción 1.1.1 **Recopilación de información**: servicios relativos a la obtención, catalogación y almacenamiento de información sobre eventos e incidentes:

- **Recopilación de informes sobre incidentes:** recopilación de informes sobre incidentes y eventos maliciosos o sospechosos de mandantes y terceras partes (como otros equipos de seguridad o fuentes de inteligencia comercial), manuales, automatizados o susceptibles de ser leídos por una máquina.
- **Recopilación de datos digitales:** recopilación y catalogación de datos digitales que pueden ser útiles, aunque no esté garantizado que así sea, para comprender la actividad de incidentes (por ejemplo, imágenes de discos, ficheros o registros/flujos de red).
- **Otros tipos de datos (no digitales):** recopilación y catalogación de datos no digitales (hojas de registro físicas, diagramas de arquitectura, modelos de negocio, datos de evaluación in-situ, políticas, marcos de riesgos de la organización, etc.).
- **Recopilación de artefactos:** actividad y procesos técnicos utilizados para obtener, catalogar, almacenar y rastrear artefactos que se consideran restos de actividades de adversarios.
- **Recopilación de pruebas:** recopilación de información y de datos para su posible uso en actividades de las fuerzas del orden. A menudo se incorpora la captación de metadatos relativos a la fuente, el método de recopilación y la información de propietario y custodia.

Subfunción 1.1.2 **Respuesta**: servicios para reducir las consecuencias de un incidente y para trabajar en la recuperación de las funciones de la actividad del mandante.

- **Contención:** parada inmediata de los daños y limitación del alcance de la actividad maliciosa mediante acciones tácticas a corto plazo (por ejemplo, bloqueo o filtrado de tráfico); también puede implicar la recuperación del control de los sistemas.
- **Mitigación:** evitación de daños adicionales mediante erradicación, aplicación de una alternativa o aplicación de estrategias de contención más exhaustivas y detalladas.
- **Reparación:** en el dominio, infraestructura o red afectados, aplicación de los cambios necesarios para solventar este tipo de actividad e impedir que vuelva a producirse. Por ejemplo, fortalecimiento de la posición defensiva organizativa y disponibilidad operativa mediante cambios de política y mediante formación y educación adicional.
- **Recuperación:** recuperación de la integridad de los sistemas afectados y vuelta al estado operativo no degradado de los sistemas, datos y redes afectados.

Subfunción 1.1.3 **Coordinación**: reparto de información y actividades de deliberación dentro y fuera del CSIRT. Esto se produce principalmente cuando el CSIRT depende de información y recursos ajenos a su control directo para tomar las acciones necesarias en la mitigación de un incidente. Ofreciendo una coordinación bilateral o multilateral, el CSIRT participa en el intercambio de información para habilitar aquellos recursos con los que actuar, o para ayudar a otros en la detección, protección y resolución de actividades en curso de adversarios.

Subfunción 1.1.4 **Rastreo de incidentes**: documentación de información sobre acciones tomadas para resolver un incidente, por ejemplo información crítica recopilada, análisis realizados, pasos tomados en la resolución y mitigación, y cierre y resolución.

Función 1.2 **Vulnerabilidad, configuración y gestión de activos:** servicios relativos al entendimiento y la resolución de vulnerabilidades, problemas de configuración e inventario de activos.

Subfunción 1.2.1 **Estudio para el descubrimiento de vulnerabilidades**: identificación de nuevas vulnerabilidades a través de investigación y experimentación (es decir, pruebas fuzz e ingeniería inversa).

Subfunción 1.2.2 **Realización de informes sobre vulnerabilidad**: actividad y procesos técnicos utilizados para obtener, catalogar, almacenar y rastrear informes de vulnerabilidad.

Subfunción 1.2.3 **Coordinación de vulnerabilidad**: notificación a las organizaciones apropiadas sobre una vulnerabilidad que afectará a las reparaciones y limitará el posible resultado de la explotación.

Subfunción 1.2.4 **Resolución de la causa principal de la vulnerabilidad**: aplicación de las acciones correctivas oficiales necesarias para corregir una vulnerabilidad identificada. En general la aplicación la lleva a cabo el operador del producto.

Service 2 Análisis

Función 2.1 **Análisis de incidente:** servicios relativos a la identificación y caracterización de información sobre eventos o incidentes, por ejemplo alcance, partes afectadas, sistemas implicados, plazos (descubrimiento, existencia, elaboración de informes) o estado (en curso frente a completado).

[Nota: Mediante otras tareas de análisis más específicas, como el análisis de información forense, de artefactos, configuración errónea, vulnerabilidad o red, se realiza un análisis más detallado del incidente].

Subfunción 2.1.1 **Validación de incidente**: verificación definitiva de que un incidente señalado ha ocurrido realmente y ha afectado a los sistemas implicados.

Propósito: ofrecer pruebas técnicas de que un evento es un incidente de seguridad, o un error de red o de hardware, y determinar las posibles consecuencias en la seguridad y los daños en la confidencialidad, disponibilidad e integridad de los activos de información.

***Resultado**: determinar si un evento señalado es realmente un incidente que debe tratarse, o si puede registrarse el informe en los sistemas pertinentes y cerrar el caso sin hacer nada más. Descubrir los detalles de los eventos que han hecho creer al mandante que se ha producido un incidente de seguridad y determinar si se trataba de un objetivo malicioso o de otra razón (como un error de configuración o de hardware).*

Subfunción 2.1.2 **Análisis de consecuencias**: determinar y caracterizar las consecuencias en la función de la actividad a la que dan soporte los sistemas implicados.

Propósito: determinar el tamaño y el alcance del incidente para tener en cuenta las partes afectadas de los servicios, infraestructura, datos, departamento u organización. Es posible realizar un enfoque general de resolución basándose en este análisis.

***Resultado**: determinar el daño (potencial) que un incidente ha provocado o podría provocar. Determinar no sólo los aspectos técnicos, sino también la cobertura mediática, la pérdida de confianza o credibilidad y los daños a la reputación.*

Subfunción 2.1.3 **Lecciones aprendidas**: examen posterior para determinar mejoras en procesos, políticas, procedimientos, recursos y herramientas con miras a atenuar y prevenir futuros peligros.

Propósito: determinar qué ha fallado, aplicar medidas preventivas y dar a conocer a la comunidad de seguridad lo aprendido mediante publicaciones y presentaciones.

***Resultado**: conjunto de recomendaciones para modificar los sistemas, procesos y procedimientos de información en los departamentos relevantes de la organización afectada.*

Función 2.2 **Análisis de artefacto:** servicios encaminados a comprender las capacidades y el objetivo de los artefactos (por ejemplo, software maligno, explotaciones maliciosas, correo basura y fichero de configuración) y su entrega, detección y neutralización.

***Propósito:** gracias al proceso de tratamiento de incidentes es posible encontrar artefactos digitales en los sistemas afectados o en los sitios de distribución de software maligno. Los artefactos pueden ser restos de un ataque de intruso, por ejemplo secuencias de comandos, ficheros, imágenes, ficheros de configuración, herramientas, resultados de herramientas, registros de inicio, etc. El análisis de artefacto se realiza para conocer cómo un intruso ha podido utilizar el artefacto para entrar en los sistemas y redes de la organización, o para determinar qué ha hecho el intruso una vez dentro del sistema. Con el análisis de artefacto se intenta determinar cómo opera el artefacto por sí sólo, o junto con otros artefactos. Esto se puede hacer a través de varios tipos de actividades: análisis de superficie, ingeniería inversa, análisis de tiempo de ejecución y análisis comparativo. Cada actividad ofrece más información sobre el artefacto. Entre los métodos de análisis figura la identificación del tipo y las características del artefacto, la comparación de artefactos conocidos, la observación de la ejecución del artefacto en un entorno de ejecución y el desembalaje y la interpretación de artefactos binarios. Mediante un análisis de los artefactos se intenta reconstruir y determinar lo que hizo el intruso para evaluar los daños, diseñar soluciones contra el artefacto y proporcionar información a los mandantes y a otras partes interesadas en los resultados.*

***Resultado:** comprender la naturaleza del artefacto digital recuperado y su relación con otros artefactos, ataques y vulnerabilidades explotadas. Buscar soluciones contra el (los) artefacto(s) analizado(s) comprendiendo la táctica, técnica y procedimientos que han utilizado los intrusos para poner en peligro los sistemas y las redes, y llevar a cabo actividades maliciosas.*

Subfunción 2.2.1 **Análisis de superficie**: determinar y caracterizar la información básica y los metadatos sobre los artefactos (por ejemplo, tipo de fichero, resultado de cadenas, troceados criptográficos, tamaño de fichero, nombre de fichero); así como revisar cualquier información de fuente pública o privada sobre el artefacto.

Propósito: *como primer paso en la recopilación de información básica, mediante el análisis de superficie se compara la información recopilada del artefacto con información de otros artefactos públicos y privados y/o repositorios de firma. Se recopila y analiza toda la información conocida (es decir, daño potencial, funcionalidad y mitigación). En función del objetivo del análisis en curso puede ser necesario realizar más análisis.*

Resultado*: determinar características y/o firma de artefacto digital y cualquier información ya conocida sobre el artefacto, incluida malignidad, consecuencias y mitigación.[1] (Esta información puede utilizarse para determinar los siguientes pasos).*

Subfunción 2.2.2 **Ingeniería inversa**: análisis estático detallado de un artefacto para determinar toda su funcionalidad, independientemente del entorno en el que se ejecute.

Propósito: *ofrecer un análisis más detallado de los artefactos de software maligno con miras a incorporar acciones ocultas de identificación e instrucciones de activación. La ingeniería inversa permite al encargado del análisis descubrir cualquier ocultación o recopilación pasada (para códigos binarios), y el programa, comando o código que compone el software maligno, desvelando un código fuente cualquiera o desensamblando el código binario en un lenguaje de ensamblaje e interpretándolo posteriormente. O desvelando todas las acciones, funciones y exposiciones de lenguaje de la máquina que el software maligno puede ejecutar. La ingeniería inversa es un análisis más detallado que se realiza cuando el análisis de superficie y de tiempo de ejecución no proporciona toda la información necesaria.*

Resultado*: descubrir toda la funcionalidad de un artefacto digital para comprender cómo funciona, cómo se activa, las debilidades conexas del sistema susceptibles de ser explotadas, todas sus consecuencias y posibles daños, y crear soluciones contra el artefacto y, si fuera necesario, crear una nueva firma para compararla con otras muestras.*

Subfunción 2.2.3 **Análisis de tiempo de ejecución**: comprender las capacidades de un artefacto observando la ejecución de la muestra en un entorno real o emulado; por ejemplo, en un espacio acotado (sandbox), un entorno virtual o en emuladores de hardware o software.

Propósito: *comprender el funcionamiento del artefacto. Al utilizar un entorno simulado se detectan los cambios en el anfitrión, el tráfico de red y el resultado de la ejecución. La premisa básica es intentar ver el artefacto en funcionamiento en un entorno lo más real posible.*

Resultado*: obtener información adicional sobre la operación del artefacto digital observando su comportamiento durante su ejecución con miras a determinar cambios en el sistema anfitrión afectado, otras interacciones de sistema y el tráfico de red resultante, para comprender mejor las consecuencias y los daños en el sistema, crear una(s) nueva(s) firma(s) de artefacto y determinar los pasos de mitigación. (Nota: no puede observarse toda la funcionalidad a partir del análisis de tiempo de ejecución ya que no es posible activar todas las secciones de código de artefacto. El tiempo de ejecución sólo permite ver lo que hace el software maligno en la situación de prueba, y no lo que es capaz de hacer).*

Subfunción 2.2.4 **Análisis comparativo:** análisis centrado en determinar objetivos o funcionalidades comunes, incluido el análisis por familias de los artefactos catalogados.

Propósito: *descubrir la relación de un artefacto con otros. Es posible encontrar similitudes en códigos, modus operandi, metas, objetivos y autores. Estas similitudes pueden utilizarse para descubrir el alcance de un ataque (es decir, ¿hay un objetivo más ambicioso?, ¿se ha utilizado anteriormente un código similar?, etc.). Entre las técnicas de análisis comparativos pueden encontrarse comparaciones de emparejamientos exactos y comparaciones de códigos similares. El análisis comparativo ofrece una visión más amplia del modo en que se utilizó y modificó con el tiempo el artefacto, o versiones similares del mismo, y ayuda a comprender la evaluación del software maligno o de otros tipos de artefactos maliciosos.*

Resultado*: descubrir otros puntos en común, o relaciones, con otros artefactos para determinar tendencias o similitudes que pueden aportar información adicional con la que comprender la funcionalidad, las consecuencias y la mitigación del artefacto digital.*

Función 2.3 **Análisis de medios**: servicios para analizar datos relevantes de sistemas, redes, almacenamiento digital y medios extraíbles para comprender mejor cómo prevenir, detectar y/o mitigar incidentes similares o conexos. Estos servicios pueden aportar información para exámenes legales, forenses o de conformidad, o para otros exámenes históricos de información.

Propósito: *recopilar y analizar pruebas de medios, como discos duros, dispositivos móviles, almacenamiento extraíble, almacenamiento en la nube u otros formatos como papel o vídeo. Si los resultados del análisis deben presentarse cumpliendo requisitos legales para su presentación, la información deberá recopilarse de modo fiable, desde un punto de vista forense, para preservar la integridad y la cadena de custodia de la prueba. Las pruebas pueden ser artefactos como: restos de software maligno; cambios en el estado de los ficheros, registros y otros componentes de sistema; captura del tráfico de red u otros ficheros de registro; información en memoria, etc. El objetivo del análisis de medios es buscar pruebas de lo ocurrido y, si se desea, otorgar un atributo a esa actividad; es diferente del análisis de artefacto, con el que se intenta comprender un artefacto y sus relaciones. Ahora bien, las técnicas de análisis de artefacto pueden utilizarse como parte de los métodos y técnicas de análisis de medios. También pueden utilizarse estos servicios fuera de un ciberincidente, como parte de un problema de recursos humanos o de otra investigación jurídica u organizativa.*

Resultado: *presentar resultados con los que 1) realizar un inventario de los activos de información (es decir, propiedad intelectual u otra información encontrada que exige una discreción absoluta); 2) proporcionar una línea cronológica de eventos de los posibles borrados, adiciones y alteraciones realizados en cualquier activo de medio implicado en el incidente, así como la persona o programa que realizó esas actividades, si es posible, y el modo en que las pruebas concuerdan e ilustran el alcance y las consecuencias del incidente.*

Función 2.4 **Análisis de explotación/vulnerabilidad:** servicios prestados para comprender mejor las vulnerabilidades que influyen en un ciberincidente.

Subfunción 2.4.1 **Análisis de explotación/Vulnerabilidad (software maligno) técnica**: comprender los puntos débiles ocasionadas para producir un incidente y las técnicas utilizadas por el adversario para aprovechar esos puntos débiles.

Propósito: informar al mandante de cualquier vulnerabilidad conocida (puntos de entrada comunes para los atacantes) para que mantenga los sistemas actualizados y monitorizados frente a explotaciones, y reduzca al mínimo cualquier consecuencia negativa.

Resultado*: comprender perfectamente una vulnerabilidad y la forma en que los delincuentes podrán utilizarla para infiltrarse en los sistemas y explotarlos.*

Subfunción 2.4.2 **Análisis de causa principal**: comprender el error de "diseño" o "aplicación" que permitió el ataque.

Propósito: determinar la causa principal y el punto de puesta en peligro, y ayudar a erradicar completamente el problema.

***Resultado**: comprender perfectamente las circunstancias que permiten la existencia de una vulnerabilidad y las circunstancias en que un atacante puede explotar esa vulnerabilidad.*

Subfunción 2.4.3 **Análisis de resolución**: comprender los pasos necesarios para solucionar el error subyacente que permitió el ataque, y evitar este tipo de ataques en el futuro.

Propósito: determinar el problema que permitió la puesta en peligro, reparar la vulnerabilidad, cambiar un procedimiento o diseño, que una tercera parte examine la resolución, y determinar cualquier nueva vulnerabilidad adoptada durante los pasos de resolución.

***Resultado**: establecer un plan para mejorar procesos, infraestructuras y diseños con miras a cerrar un vector de ataque determinado y a evitar dicho ataque en el futuro.*

Subfunción 2.4.4 **Análisis de mitigación**: análisis para determinar los medios con los que atenuar (prevenir) los riesgos generados por un ataque o una vulnerabilidad sin por ello subsanar necesariamente el error subyacente que lo introdujo.

Service 3 Protección de la información

Función 3.1 **Evaluación de cumplimiento/riesgo:** servicios relativos a la evaluación de riesgos o a las actividades de evaluación de cumplimiento. Puede referirse a la evaluación *per se* o a la prestación de ayuda para estudiar los resultados de una evaluación. Suele hacerse en apoyo de un requisito de cumplimiento (por ejemplo, ISO 27XXX, COBIT).

Propósito: identificar mejor las oportunidades y las amenazas y mejorar los controles, la gestión de incidentes, la prevención de pérdidas, la seguridad de la información y otras funciones relevantes.

Resultado: **proceso coherente de evaluación y gestión de riesgos de información aplicado a datos y activos fundamentales, información para la evaluación de riesgos, selección de opciones fundamentales de tratamiento de riesgos a incorporar en la gestión de incidentes y el análisis forense, cuando sea apropiado.**

Subfunción 3.1.1 **Inventario de datos/activos críticos**: identificación de datos y activos fundamentales, imprescindibles para cumplir la misión de la organización. Puede que la organización no esté necesariamente en posesión de estos datos y activos (por ejemplo, pertenecen a un proveedor de la nube o son un conjunto de datos externos). La identificación de datos y activos consiste, entre otras cosas, en determinar su ubicación, su propietario, su grado de confidencialidad, la función de su misión y su estado/nivel actual.

Propósito: determinar de forma regular los datos y activos en los que la gestión de incidentes pueda ser un requisito para que la organización cumpla su misión, junto con las líneas de actividad relevantes.

Resultado: *un inventario, base de datos o lista de los activos y datos fundamentales, actualizado regularmente, para que la organización lo utilice en la evaluación de riesgos.*

Subfunción 3.1.2 **Determinar normas de evaluación**: obtener normas enumeradas/identificadas y políticas de riesgos organizativos para que los responsables evalúen el estado/nivel de seguridad. Sugerir criterios de evaluación o referencia a los gestores de riesgos empresariales y a los directores de seguridad de sistemas de información (CISO). Algunos ejemplos de normas son: Basilea II, COBIT, ITIL o el proceso de certificación y acreditación.

Propósito: ayudar a elegir una metodología aprobada de evaluación de riesgos de información para utilizarla en la organización, y proporcionar información con miras a obtener una gestión y evaluación de riesgos más amplia de la organización.

Resultado: *una metodología seleccionada de evaluación de riesgos de información para utilizarla en toda la organización; apoyo e implicación de la opción elegida a nivel ejecutivo; políticas organizativas para regular el uso de la metodología de evaluación de riesgos seleccionada, cuando sea adecuado; resultados, medidas, plantillas acordados; procesos y procedimientos acordados para la evaluación de riesgos de información; mecanismos acordados para integrar los resultados de la evaluación de riesgos de información en la toma de decisiones y la gestión de riesgos de la organización.*

Subfunción 3.1.3 **Evaluación ejecutiva**: ayudar a la realización de exámenes y participar en evaluaciones para que se cumplan los requisitos de riesgos y seguridad.

Propósito: utilizando la metodología aprobada, ultimar de la forma más detallada posible la evaluación de riesgos de información de los datos o activos fundamentales seleccionados.

Resultado: *una evaluación completa de riesgos de información de los datos o activos fundamentales seleccionados.*

Subfunción 3.1.4 **Resultados y recomendaciones**: elaborar y presentar resultados, informes y/o recomendaciones (por ejemplo, elaboración de informes utilizando las tareas para publicar información).

Propósito: ayudar a documentar todos los resultados de una evaluación completa de riesgos, y enumerar medidas a adoptar y recomendaciones a tener en cuenta, fruto de esta evaluación.

Resultado: *un informe autorizado y ratificado con información pormenorizada sobre los datos o activos críticos, el proceso de evaluación de riesgos utilizado, los datos utilizados en la evaluación, resultados, recomendaciones, medidas, planes y plazos de distribución.*

Subfunción 3.1.5 **Rastreo**: ayudar a los CISO y/o gestores de riesgos a comprobar el estado de las evaluaciones y la subsiguiente aplicación de las recomendaciones.

Propósito: garantizar que todos los planes, medidas y recomendaciones se cumplen y acatan en los plazos documentados.

Resultado: *examen regular de planes y plazos, lista de medidas acatadas, revisión de plazos si no se finalizan a tiempo las acciones, informe sobre los avances respecto a planes y plazos.*

Subfunción 3.1.6 **Realización de prueba**s: comprobar activamente que se respetan los niveles de riesgos. Para ello pueden realizarse, entre otras cosas, pruebas de penetración, escaneados y evaluaciones de vulnerabilidad, pruebas de aplicación, auditorías y verificaciones, etc.

Propósito: comprobar que los tratamientos de riesgos seleccionados y aplicados son aptos para el propósito definido, se han aplicado correctamente y proporcionan la mitigación de riesgo esperada.

Resultado: *un plan de prueba documentado con los resultados esperados; pruebas y resultados documentados; comparación con resultados esperados, y medidas y plazos para corregir cualquier desviación respecto del objetivo esperado.*

Función 3.2 **Gestión de parches:** servicios para ayudar al mandante con las capacidades necesarias para gestionar la identificación de inventario, los sistemas a parchear y el despliegue y verificación de la instalación de parche.

Propósito: ayudar a identificar, adquirir, instalar y verificar parches para productos y sistemas, y evaluar la utilidad y las consecuencias de los parches desde una perspectiva de gestión de incidentes.

Resultado: *tomar conciencia y comprender los parches requeridos, los parches que deben aplicar los proveedores de servicios y la repercusión de los parches en el riesgo de información y en la gestión de incidentes.*

Función 3.3 **Gestión de políticas operativas**: servicios con los que formular, mantener, institucionalizar y afianzar el concepto organizativo de operaciones y otras políticas.

Propósito: asesorar con garantías a mandantes o líneas de actividad para la recuperación y continuidad de la actividad en caso de catástrofe, ofreciendo consejos imparciales y basados en hechos, teniendo en cuenta las oportunidades o problemas planteados, el entorno en el que puede aplicarse el consejo y cualquier limitación en los recursos.

Resultado: *decisiones sobre la actividad con recuperación y continuidad de la misma en caso de catástrofe; gestión de incidentes como asesor de confianza; implicación de los miembros del equipo de gestión de incidentes en las decisiones de la actividad, cuando y donde sea posible.*

Función 3.4 **Deliberación sobre análisis de riesgo/recuperación y continuidad de actividad en caso de desastre:** servicios prestados al mandante relativos a actividades de resiliencia organizativa a partir de riesgos identificados. Entre ellos figuran diversas actividades de gestión de riesgo: desde realizar la propia evaluación hasta ayudar en el análisis de evaluación y mitigación de los problemas descubiertos en la evaluación.

Propósito: asesorar con garantías a mandantes o líneas de actividad en la recuperación y continuidad de la actividad en caso de catástrofe, ofreciendo consejos imparciales y basados en hechos, y teniendo en cuenta las oportunidades o problemas planteados, el entorno en el que puede aplicarse el consejo y cualquier limitación en los recursos.

Resultado: *decisiones sobre la actividad con gestión de incidentes y seguridad de la información; gestión de incidentes como asesor de confianza; implicación de los miembros del equipo de gestión de incidentes en las decisiones de la actividad, cuando y donde sea posible.*

Función 3.5 **Deliberación de seguridad**: servicios para asesorar a un mandante o línea de actividad sobre la ejecución y aplicación de las operaciones o funciones de seguridad pertinentes.

Service 4 Toma de conciencia del entorno

Propósito: sensibilizar a una organización, a través de un conjunto de actividades, sobre su entorno operativo. La toma de conciencia del entorno implica determinar los elementos críticos que pueden afectar a la misión de una organización, monitorizarlos y utilizar estos conocimientos para fundamentar la toma de decisiones y otras medidas.

Resultado: *sensibilizar en la medida necesaria sobre los eventos y actividades en la organización, y en su entorno, que pueden impedir que ésta actúe de forma puntual y segura.*

Función 4.1 **Operaciones con medidas/sensores:** servicios que se centran en la concepción, despliegue y operación de metodologías de análisis y sistemas con miras a determinar actividades para investigación.

Propósito: crear los procesos y la infraestructura de recopilación de información necesarios para sensibilizar a la organización sobre el entorno.

Resultado: *una infraestructura de recopilación de información operativa (es decir, sensores) con la que obtener información encaminada a sensibilizar sobre el entorno.*

Subfunción 4.1.1 **Elaboración de requisitos**: comprender las necesidades del mandante y obtener las autorizaciones bajo las que puede operar el CSIRT.

Propósito: con el proceso de elaboración de requisitos se definen las necesidades de la organización relativas a la toma de conciencia del entorno y, a continuación, se vinculan con la información necesaria para cumplir dichos objetivos.

Resultado: *desde un punto de vista de la información, comprender el nivel de concienciación que necesita la organización y su mandante. Además, garantizar que la organización dispone de todas las aprobaciones jurídicas y políticas necesarias para recopilar la información.*

Subfunción 4.1.2 **Identificación de datos necesarios**: determinar los datos necesarios para cumplir los requisitos.

Propósito: los sensores pueden ser muchas cosas, desde sistemas automáticos hasta humanos. Estas fuentes de información (datos) se utilizan para sensibilizar sobre el entorno a una organización. Con el proceso de "Identificación de datos necesarios" se vinculan los requisitos de toma de conciencia del entorno con las posibles fuentes de información (es decir, los sensores).

Resultado: *la identificación de los datos necesarios para ayudar a cumplir los requisitos de toma de conciencia del entorno de la organización. Es posible que ya existan algunas fuentes de datos, pero otras habrá que diseñarlas y/o adquirirlas.*

Subfunción 4.1.3 **Métodos de adquisición de datos**: determinar los métodos, herramientas, técnicas y tecnologías utilizados para recopilar los datos necesarios.

Propósito: con este proceso se determinan los métodos de recopilación, procesamiento y almacenamiento de información (datos) recopilada.

Resultado: *determinar detalladamente cómo se recopilará, almacenará, procesará y clasificará la información.*

Subfunción 4.1.4 **Gestor de sensores**: mantenimiento y mejora continua del rendimiento de sensores relativo a los requisitos definidos.

Propósito: mantener y monitorizar sensores para que funcionen de forma correcta y precisa.

Resultado: *aplicación de un programa de mantenimiento de ciclo de vida y gestión de sensores.*

Subfunción 4.1.5 **Gestión de resultados**: selección y divulgación de la información y las medidas obtenidas con sensores. Por lo general se muestran en una interfaz para que varios niveles dentro de una organización puedan consultarlos.

Función 4.2 **Fusión/Correlación:** servicios con los que se realizan análisis y se incorporan múltiples fuentes de datos. Utilizan información suministrada por una fuente cualquiera y la integran en una visión general de la situación (toma de conciencia del entorno).

Propósito: descubrir nuevas relaciones entre incidentes, indicadores y actores que permitan mejorar la mitigación o la respuesta en caso de incidente de seguridad.

Resultado*: habilitar un proceso coherente para que la organización pueda servirse de la nueva información sobre amenazas, e integrarla en las bases de datos de la organización junto con la información disponible. El resultado final de este proceso será una información que el CSIRT utilizará para tomar decisiones de forma más eficiente y precisa.*

Subfunción 4.2.1 **Determinar algoritmos de fusión**: determinar los métodos y técnicas (algoritmos) o tecnologías utilizadas para analizar (fusionar) la información.

Propósito: como parte del tratamiento de incidentes es importante que el CSIRT mantenga una buena visión operativa de la información recibida desde varias fuentes. La fusión permite gestionar la información de forma que el CSIRT tenga en cuenta rápidamente información nueva en cuanto llegue, la circunscriba completamente a un contexto y la aproveche durante el proceso de tratamiento de incidentes.

***Resultado**: elaborar un proceso interno con el que obtener información nueva, evaluarla en el contexto de la información existente y aprovechar satisfactoriamente la información resultante, disponible para el CSIRT, en el contexto de un incidente.*

Subfunción 4.2.2 **Análisis de fusión**: análisis (fusión) de los recursos de datos a partir de los datos del sistema de gestión de conocimientos, con miras a descubrir puntos en común y relaciones entre ellos.

Propósito: para tratar incidentes, el CSIRT necesitará comprender en todo momento la amenaza que supone un incidente particular para la organización. Para ello deberá conocer las últimas novedades sobre el incidente y cómo evolucionan las tácticas, técnicas y procedimientos utilizados por el adversario. Además, tendrá que recopilar continuamente información y realizar evaluaciones a partir de la información existente. La subfunción 4.2.2 utilizará los algoritmos de fusión seleccionados en la subfunción 4.2.1 para analizar la información de amenazas obtenida a partir de fuentes externas.

***Resultado**: entender cómo puede aprovecharse la nueva información contra los incidentes existentes y preparar a la organización ante cualquier cambio realizado por un adversario en los TTP, o ayudarla a que actualice continuamente sus técnicas de mitigación y respuesta con miras a tratar mejor incidentes conexos.*

Función 4.3 **Elaboración y conservación de información sobre seguridad:** servicios ofrecidos a mandantes internos o externos para elaborar y mantener fuentes de información sobre seguridad de terceros. La información sobre seguridad puede definirse como la información sobre seguridad y amenazas que proporciona inteligencia operativa o sobre amenazas. Entre los servicios puede figurar el análisis, la elaboración, la distribución y la gestión de información sobre seguridad, incluidos los indicadores de amenaza, la lógica de detección de amenaza (como firmas y normas contra software maligno) y las tácticas, técnicas y procedimientos del adversario. Estos servicios dependen de las actividades de intercambio de información definidas en la sección 5.6 "Divulgación/Comunicaciones".

Propósito: la información de entidades externas es decisiva para obtener un nivel suficiente de toma de conciencia del entorno. Para su operación, el CSIRT necesita mucha información relevante y de gran calidad, pero los costes y la carga de trabajo necesarios para ello obligan a concentrar los esfuerzos en algunas fuentes seleccionadas.

Resultado: *obtener múltiples fuentes de datos de gran calidad que cubran todas las esferas operativas relevantes de un CSIRT -principalmente a través de procesos completamente automáticos- mediante un sistema de gestión de datos (función 4.4). Otro resultado son los procesos para detectar anomalías o cambios de tendencia en los flujos de información obtenidos de las fuentes externas.*

Subfunción 4.3.1 **Identificación de fuente e inventario:** continua identificación, mantenimiento e integración de fuentes de información en procesos de análisis y gestión de conocimientos.

Propósito: obtener información relevante y de gran calidad a partir de fuentes externas para responder al incidente de forma eficaz, y aumentar proactivamente la toma de conciencia del entorno (y, en general, la posición de la organización en materia de seguridad). Con las fuentes externas se completan los datos recopilados internamente: informes de incidentes (función 1.1), informes de vulnerabilidad (función 1.2) e información de sensores manejados por el CSIRT (función 4.1).

Resultado: *la adquisición de información de seguridad relevante y de gran calidad, a partir de fuentes internas, externas, gratuitas y/o comerciales. Toda la información recopilada se almacena en el sistema de gestión de datos (función 4.4).*

Subfunción 4.3.2 **Recopilación y catálogo del contenido de fuentes**: la adquisición de material proveniente de fuentes de información de amenazas. Estas fuentes pueden ser internas, externas, gratuitas y/o de pago.

Propósito: clasificar la calidad de la información recopilada. Señalar cambios en las características (incluida la cantidad) de los datos obtenidos a partir de fuentes externas para detectar anomalías y/o nuevas tendencias.

Resultado: *documentación con clasificaciones de calidad de las fuentes. Proceso automático o semiautomático relativo a los cambios más importantes en las características principales de la información obtenida a partir de fuentes externas.*

Función 4.4 **Gestión de datos y conocimientos:** servicios ofrecidos a los mandantes para ayudarles a obtener, elaborar, compartir y utilizar de forma eficaz conocimientos organizativos que incorporen etiquetado de datos (por ejemplo, STIX, TAXII, IODEF o TLP), bases de datos de indicadores y catálogos de software maligno/vulnerabilidades.

Propósito: los mandantes exigen conocimientos y datos de ciberseguridad oportunos y de calidad suficiente para cubrir sus necesidades. Los datos de ciberseguridad consisten en información que los sistemas procesarán para dar soporte a la automatización de la seguridad. Los conocimientos de ciberseguridad son información destinada a las personas que operan/analizan la ciberseguridad. Hay también otros servicios y funciones CSIRT que necesitan la entrada de datos y conocimientos de ciberseguridad. La mejor forma de gestionar este tipo de información es como un recurso CSIRT general, ya que la mayoría de la información se reutiliza en varios servicios y funciones.

Resultado*: ofrecer oportunamente a los mandantes conocimientos y datos de ciberseguridad de la calidad requerida. Otros servicios y funciones CSIRT pueden obtener fácilmente los datos y conocimientos que necesitan de una sola fuente dentro del CSIRT.*

- **Gestión de representación de datos:** normalización del modo en que se representan e intercambian los datos (por ejemplo, STIX, TAXII, IODEF, RID, etc.).
- **Gestión de almacenamiento de datos:** diseño, aplicación y mantenimiento de los sistemas de gestión de almacenamiento.
- **Digestión de datos:** procesos y sistemas utilizados para recibir, validar y almacenar información.
- **Extracción de datos:** procesos, políticas y métodos técnicos para extraer la información.

- **Evaluación de herramientas:** evaluación e integración de las herramientas utilizadas para la gestión, el análisis y el intercambio de datos.

Función 4.5 **Métrica organizativa**: servicios que se centran en identificar, establecer, recopilar y analizar el grado de éxito de los objetivos de rendimiento organizativo, y en medir la eficacia organizativa.

Propósito: una de las dificultades fundamentales que tienen hoy en día los equipos de intervención en caso de incidentes de seguridad informática (CSIRT), y las organizaciones de gestión de incidentes, es determinar en qué medida consiguen cumplir su objetivo, a saber, gestionar los incidentes de ciberseguridad. A medida que sus operaciones se consolidan, los equipos necesitan saber si realmente lo están haciendo bien. Para ello buscan formas con las que evaluar sus operaciones, no sólo para descubrir los puntos fuertes y débiles de sus procesos, tecnologías y métodos, sino para compararse también con otros equipos similares. Esto lo hacen a través de medidas y pruebas cuantificables que les muestran si son eficaces en la prevención, detección, análisis y respuesta ante ciberincidentes y ciberevents. Esta función se centra en determinar qué preguntas (información) necesitan respuesta para que la gestión, los equipos CSIRT y las partes interesadas, entre otros, puedan evaluar sus operaciones y mostrar su valor; y en establecer mecanismos que, a partir de mediciones, obtengan las medidas requeridas y, a continuación, recopilen, analicen y presenten resultados.

Resultado: *ofrecer pruebas empíricas y hacer que se tome suficiente conciencia como para poder determinar el grado en que una organización de gestión de incidentes está cumpliendo y desarrollando su misión; y descubrir los aspectos susceptibles de mejora. Aprovechar esta información para facilitar la toma de decisiones y mejorar el rendimiento y la responsabilización.*

Service 5 Divulgación/Comunicaciones

Función 5.1 **Asesoría en materia de políticas de ciberseguridad:** servicios con los que se da soporte a la elaboración y adopción de políticas de ciberseguridad que favorezcan el entorno del CSIRT, de su mandante y de otras partes interesadas, ofreciéndoles asesoría profesional sobre el asunto en cuestión para que los responsables puedan fundamentar sus decisiones.

Subfunción 5.1.1 Interna

- **Consulta jurídica y de políticas:** informar sobre las implicaciones jurídicas y de políticas, relativas a los mandatos y autoridades organizativos y de mandantes.
- **Elaboración de políticas**: elaborar políticas relativas a autoridades y a operaciones de organizaciones o de mandantes.

Subfunción 5.1.2 Externa

- **Proporcionar información sobre políticas:** proporcionar asesoramiento sobre asuntos relativos a políticas técnicas y de seguridad que pueden afectar a la organización y a sus mandantes o a otros socios.
- **Influir en las políticas:** proporcionar información fiable o conocimientos sobre el asunto en cuestión para dirigir la revisión de políticas, reglamentos o leyes. Puede consistir, entre otras cosas, en testificar ante entidades legislativas, científicas u otras; redactar informes de posición, libros blancos o artículos; escribir en blogs o medios sociales; reunirse con partes interesadas, etc.
- **Desarrollo de normas y prácticas idóneas:** contribuir en las iniciativas de las organizaciones de prácticas idóneas o normas industriales, mundiales, regionales y nacionales (IETF, ISO, FIRST, etc.) para que se normalicen los procesos y las prácticas idóneas con miras a aumentar al máximo la compatibilidad, interoperabilidad, seguridad, reproductibilidad o calidad.

Función 5.2 **Gestión de relaciones**: servicios que se centran en establecer y mantener las relaciones de la organización.

Subfunción 5.2.1 Gestión de relaciones homólogas: Establecimiento y mantenimiento de relaciones con organizaciones que puedan ayudar al CSIRT a cumplir su misión. Esto puede implicar asegurar la interoperabilidad o fomentar la colaboración entre organizaciones.

Subfunción 5.2.2 **Gestión de relaciones entre mandantes**: elaboración y aplicación de prácticas, estrategias y tecnologías utilizadas para determinar, descubrir, comprender, gestionar, rastrear y evaluar a mandantes y partes interesadas.

Subfunción 5.2.3 **Gestión de comunicaciones**: gestión de listas utilizadas para divulgar anuncios, alertas, avisos, datos y otras publicaciones o información.

Subfunción 5.2.4 **Gestión de comunicaciones seguras**: gestión de mecanismos de comunicación seguros utilizados en las comunicaciones por correo electrónico, web, mensajería instantánea o voz.

Subfunción 5.2.5 **Conferencias / Talleres**: ofrecer oportunidades al CSIRT y a su mandante para que se reúnan y conversen sobre las amenazas y desafíos a los que se enfrentan, fortalezcan sus relaciones de confianza, intercambien sus datos de contacto y se expliquen prácticas idóneas y lecciones aprendidas.

Subfunción 5.2.6 **Relaciones/Implicación de partes interesadas**: coordinación con las organizaciones verticales y del sector, y gestión de puntos de contacto oficiales con las partes interesadas internas y externas. Implicar al nivel ejecutivo de la organización para dar a conocer la misión de ésta y explicar la importancia que tiene tomar conciencia sobre la seguridad.

Función 5.3 **Concienciar sobre la seguridad:** servicios efectuados en la organización del mandante para dar a conocer a todos sus empleados las amenazas a las que se enfrentan y las medidas que pueden tomar para reducir el riesgo que éstas suponen.

Función 5.4 **Marcas/Comercialización**: servicios para que las partes interesadas y los mandantes conozcan al CSIRT, sus capacidades y la forma en la que deberían comunicarle sus necesidades.

Función 5.5 **Publicaciones y compartición de la información**: servicios que se centran en la comunicación, incluidas notificaciones realizadas por la organización a sus mandantes para ayudarles en sus operaciones. Algunos ejemplos son la notificación de formaciones, eventos y procedimientos y políticas organizativos.

Subfunción 5.5.1 **Anuncios de servicio público**: divulgación de información relativa a la seguridad para que se conozcan y apliquen mejor las prácticas de seguridad públicas, sectoriales, organizativas o del mandante.

Subfunción 5.5.2 Publicación de información:

- **Recopilación de requisitos:** determinar la información que debe divulgarse, a quién, de qué modo y en qué plazo (scoping). Nota: la publicación puede estar destinada a una audiencia limitada, o puede ser una publicación más detallada para los socios.
- **Elaboración**: definir el formato y el objetivo de los productos de información para cumplir los requisitos.
- **Creación de documentos:** precisión en la recopilación de información para que la audiencia prevista la comprenda de inmediato (por ejemplo, presentación de los resultados de actividades de gestión de software maligno, vulnerabilidad, incidentes y análisis forense).
- **Revisión:** comprobar que las publicaciones son claras, precisas, ortográfica y gramaticalmente correctas, actuales y conforme a las normas relativas a la divulgación de la información; y obtener la aprobación final.
- **Distribución:** entrega de información a la audiencia prevista por los canales adecuados y necesarios.

Service 6 Capacitación

Propósito: la creación de planteamientos y procesos bien articulados de respuesta y gestión de incidentes debe abordar siempre la capacitación. Es algo básico para el rendimiento y la eficacia generales de una organización. Las organizaciones necesitan saber qué capacidades afectan realmente a su CSIRT y al rendimiento general de la actividad, y adaptar sus programas de formación en consecuencia. En un estudio de McKinsey, cerca de un 60% de los encuestados señalaron que una de las tres prioridades principales de sus organizaciones era la capacitación organizativa. Sin embargo, a la hora de abordar lo más necesario, menos del 30% centraban sus programas de formación en una capacitación que añadiese valor y ayudase a alcanzar un rendimiento óptimo.

Se puede definir la capacidad como todo lo que hace correctamente una organización y que genera resultados de actividad importantes. Las organizaciones necesitan tener capacidades muy importantes para su actividad general y el rendimiento de equipo, y comprender los resultados de centrarse en las que han elegido. La cultura influye en qué capacidades prioriza y desarrolla una organización. La gestión de alto nivel suele estar implicada en diseñar las capacidades de la organización, pero el éxito viene cuando se armonizan las capacidades de la organización con las necesidades y requisitos del equipo o de las unidades de actividad.

***Resultado**: comprender, documentar y ejecutar un plan, y ser capaz de utilizar y medir los resultados y las relaciones de las diferentes oportunidades de creación de capacidad, tanto para cada miembro de equipo como al nivel general de la organización. Definir y poner en práctica un sistema que se convierta en parte de la planificación general del personal.*

Función 6.1 **Formación y educación:** el volumen de capacidad implica que existe un cierto nivel de capacidad con un cierto grado de madurez. Así pues, la capacidad es la piedra angular de los servicios CSIRT. La capacitación consiste en proporcionar formación y educación a un mandante CSIRT (que puede ser personal de organización, pero sin ofrecer información sobre asuntos funcionales como la formación de recursos humanos para el equipo) sobre temas relativos a la ciberseguridad, protección de la información y respuesta en caso de incidente.

> **Propósito:** un programa de formación y educación suele ser el primer paso para definir y poner en marcha una entidad de capacitación. Esto puede hacerse mediante diferentes actividades, como formación y educación, aprendizaje de requisitos documentados, aptitudes y habilidades requeridas, entrega de material de educación y formación estructurado, tutorías, desarrollo profesional y de habilidades, y oferta de ejercicios y actividades de taller. Cada una de estas actividades contribuirá a la capacidad del equipo y de la organización.
>
> ***Resultado**: comprender todo el programa de formación y educación, y cómo puede ayudar a la capacitación del equipo CSIRT. Poder comprender y documentar los tipos de resultados de equipo y organización, y los IFR, para conocer el progreso realizado.*

Subfunción 6.1.1 **Recopilación de requisitos de habilidades, aptitudes y conocimientos**: recopilar las necesidades de habilidades, aptitudes y conocimientos (HAC), y la competencia del mandante, para determinar qué formación y educación debe ofrecerse.

Propósito: evaluar, determinar y documentar correctamente las necesidades del equipo CSIRT relativas a HAC para que sus miembros estén preparados y capacitados.

Resultado: *determinar un proceso y las características necesarias de HAC para que el equipo CSIRT pueda cumplir las necesidades de la actividad, y comparar con otras para encontrar las mejores. Esto ayudará a determinar el nivel en el que está operando el equipo, y si (y dónde) hay opciones de mejora.*

Subfunción 6.1.2 **Elaboración de material educativo y de formación**: elaborar o adquirir contenido educativo y de formación, como presentaciones, clases, demostraciones, simulaciones, etc.

Propósito: el material educativo y de formación elaborado lo utiliza el equipo CSIRT para mantener informado al usuario, para que el equipo pueda reaccionar a los rápidos cambios en el panorama y las amenazas, y para facilitar la comunicación entre el CSIRT y sus mandantes.

Resultado*: material educativo y de formación CSIRT de calidad; respuesta a las necesidades generadas ante los rápidos cambios en el entorno CSIRT, y uso de diferentes técnicas y plataformas de presentación eficaces.*

Subfunción 6.1.3 **Entrega de contenido**: transferencia de conocimientos y contenidos a "estudiantes". Puede realizarse a través de varios métodos: formación por computador/en línea, dirigida por un profesor, virtual, mediante conferencias, presentaciones, talleres, etc.

Propósito: un proceso formal de entrega de contenidos ayudará al equipo a determinar con claridad la mejor forma para que los miembros del CSIRT reciban la formación que necesitan.

Resultado: *un marco de entrega de contenidos que utilice todos los métodos disponibles para presentar y adquirir procesos y habilidades técnicas y básicas, utilizando todos los*

enfoques alternativos, incluidos talleres prácticos, educación a distancia con ayuda de computador y educación personal, etc.

Subfunción 6.1.4 **Tutorías**: puede aprenderse del personal experimentado dentro de una relación establecida a través de visitas al sitio, rotación (intercambio), seguimiento y argumentación debatida de decisiones y medidas específicas.

Propósito: un programa de tutorías suele ser el primer paso para definir y poner en marcha una entidad de capacitación. Puede ser de utilidad proporcionar mecanismos formales e informales para que el tutor y el alumno conversen sobre educación, desarrollo de habilidades, opiniones, experiencias laborales y de vida, etc. fuera de la relación y estructura oficial del equipo.

Resultado: *un equipo CSIRT con mayor capacidad de retención, lealtad, confianza y habilidad general para tomar decisiones fiables.*

Subfunción 6.1.5 **Desarrollo profesional**: ayudar al personal a planificar y emprender satisfactoria y adecuadamente su carrera profesional. Puede hacerse mediante conferencias, formaciones avanzadas, actividades de formación entre los propios miembros, etc.

Propósito: el equipo CSIRT recurre al desarrollo profesional para promover un proceso continuo de afianzamiento de nuevos conocimientos, habilidades y aptitudes relativas a la profesión de seguridad, responsabilidades laborales singulares y el entorno general de equipo.

Resultado*: fomentar el desarrollo profesional para que el equipo adquiera confianza y cuente con los conocimientos, habilidades y aptitudes necesarios transferibles directamente a la práctica, y para que esté al día sobre los roles y necesidades del trabajo.*

Subfunción 6.1.6 **Desarrollo de habilidades**: ofrecer formación al personal de la organización sobre herramientas, procesos y procedimientos relativos a las funciones operativas del día a día.

Propósito: una vez conocidas las habilidades apropiadas, el equipo CSIRT deberá realizar varias medidas, lo que determinará si está preparado.

Resultado: *personal formado y estructurado con los conocimientos necesarios de procesos y habilidades técnicas y básicas. Unos miembros del CSIRT en condiciones de solventar las dificultades operativas diarias, y de dar soporte al equipo y a sus clientes.*

Subfunción 6.1.7 **Realizar ejercicios**: realizar pruebas a los "estudiantes" del mandante para comprobar si pueden aplicar lo aprendido y realizar funciones de trabajo o de tarea. Puede hacerse mediante entornos virtuales, simulaciones, pruebas de campo, talleres, entornos de imitación o combinando estas opciones.

Propósito: mediante simulacros/ejercicios el equipo CSIRT adquirirá confianza en la utilidad del plan CSIR de la organización y en su habilidad para aplicarlo.

Resultado*: un equipo lo más preparado posible que garantice los procesos fundamentales HAC y la ejecución satisfactoria de todo el trabajo. Esto también ayudará a determinar el nivel en el que está operando el equipo, y si (y dónde) hay opciones de mejora.*

Función 6.2 **Organización de ejercicios:** servicios ofrecidos por la organización a los mandantes para dar soporte al diseño, ejecución y evaluación de ciberejercicios encaminados a formar y/o evaluar las capacidades de los mandantes por separado y en conjunto. Este tipo de ejercicios puede utilizarse para:

- **Probar políticas y procedimientos:** el equipo evalúa si hay suficientes políticas y procedimientos en marcha para responder al evento. Suele consistir en un ejercicio de papel/taller.
- **Probar la preparación operativa:** el equipo evalúa si se dispone de la gente adecuada para responder al evento y si los procedimientos se están ejecutando correctamente. Suele consistir en ejercicios de procedimientos.

Propósito: los ejercicios se realizan para mejorar la eficacia y la eficiencia de los servicios y funciones de ciberseguridad. Con esta función y las subfunciones conexas se abordan las necesidades de la organización y de los mandantes. De forma más específica, y a través de la simulación de eventos/incidentes de ciberseguridad, los ejercicios pueden utilizarse para uno o varios objetivos:

- Demostración: poner de manifiesto servicios y funciones de ciberseguridad, y vulnerabilidades, amenazas y riesgos, para que se tome conciencia al respecto.
- Formación: formar al personal sobre nuevas herramientas, técnicas y procedimientos.
- Ejercicio: ofrecer al personal la oportunidad de utilizar herramientas, técnicas y procedimientos sobre los que ha recibido información. Es necesario hacer ejercicios para no perder las habilidades y para mejorar y mantener la eficiencia.
- Evaluación: analizar y comprender el nivel de eficacia y eficiencia de los servicios y funciones de ciberseguridad.

- Certificación: determinar si puede alcanzarse un nivel de eficiencia y/o eficacia determinado para los servicios y funciones de ciberseguridad.

***Resultado**: mejorar directamente la eficiencia y la eficacia de los servicios y funciones de ciberseguridad, y extraer conclusiones para seguir mejorando. Entre los objetivos determinados de un ejercicio figura la demostración de la ciberseguridad a las partes interesadas, la formación del personal y la evaluación y/o certificación de la eficiencia y la eficacia de los servicios y funciones. También pueden extraerse conclusiones para mejorar ejercicios en el futuro.*

Subfunción 6.2.1 **Requisitos**: comprender la intención del ejercicio, en particular los objetivos de todos los participantes, para incorporarla a la elaboración del mismo.

Propósito: el objetivo de participar en ejercicios es mejorar la eficacia y la eficiencia de los servicios y funciones de ciberseguridad. La forma de participación puede ser una de las siguientes:

- Observación: el personal observa la realización de un ejercicio pero no forma parte de la audiencia prevista ni debe resolver los eventos del ejercicio, ni será evaluado por sus resultados. Observar, sin participar directamente, puede ayudar a mejorar en cierta medida la eficiencia y la eficacia de los servicios y funciones CSIRT. También puede ayudar a organizar futuros ejercicios.
- Ejercicio como audiencia: el personal participa en un ejercicio a modo de audiencia prevista, debe resolver los eventos del mismo y puede recibir una evaluación al respecto.

En función de las modalidades del ejercicio, el personal viajará al lugar del mismo o participará a distancia desde su oficina o desde el lugar que le convenga. Además, el ejercicio puede proporcionar un entorno determinado, o el personal puede participar desde su propio entorno de ejercicio o desde el lugar habitual de trabajo.

***Resultado**: mejora en la eficiencia y eficacia de los servicios y funciones de ciberseguridad, y aprendizaje de lecciones para poder seguir mejorando. Entre los objetivos determinados de un ejercicio figura la demostración de la ciberseguridad a las partes interesadas, la formación del personal y la evaluación y/o certificación de la eficiencia y la eficacia de los servicios y funciones. También pueden extraerse conclusiones para mejorar ejercicios en el futuro.*

Subfunción 6.2.2 **Desarrollo de entorno y casos prácticos**: elaboración de casos prácticos para atender los objetivos del mandante.

Propósito: el objetivo de organizar ejercicios es ofrecer una oportunidad a la audiencia prevista para que mejore la eficiencia y la eficacia de sus servicios y funciones gestionando los incidentes/eventos de ciberseguridad.

***Resultado**: mejora de la eficiencia y la eficacia de los servicios y funciones de la audiencia prevista, y aprendizaje de lecciones para seguir mejorando. Aprendizaje de lecciones para poder mejorar los ejercicios en el futuro.*

Subfunción 6.2.3 **Participación en un ejercicio**: una organización puede tener diferentes niveles de participación en un ejercicio en función de su nivel de madurez.

- **Evaluación:** evaluar los resultados de un ejercicio, solicitar comentarios al respecto y determinar opciones de mejora observando el ejercicio.
- **Observación:** observar un ejercicio realizado por un tercero.
- **Coordinación:** coordinar un ejercicio.
- **Participación:** participar en un ciberejercicio. El participante decide el nivel de participación y se beneficia del resultado del ejercicio (por ejemplo, su participación la evalúa un tercero).

Subfunción 6.2.4 **Determinar las lecciones aprendidas**: elaborar un informe postejercicio en el que figuren las lecciones aprendidas o los resultados/prácticas idóneas del ejercicio.

Función 6.3 **Sistemas y herramientas de apoyo al mandante:** servicios que se centran en la recomendación, elaboración, suministro y adquisición de herramientas y servicios de ciberseguridad para un mandante. Todos estos sistemas y herramientas guardan relación con CSIRT/seguridad y no con la tecnología de la información en general; algunos de estos sistemas son los portales de mensajería/alerta.

***Resultado**: el CSIRT dispone de procesos y sistemas para determinar los requisitos y capacidades del mandante y adquirir, suministrar y elaborar plataformas para estos requisitos.*

Función 6.4 **Servicios de apoyo a partes interesadas:** servicios centrados en las capacidades técnicas ofrecidas por el CSIRT para ayudar en la capacitación, el volumen de capacidad y el grado de madurez de los servicios CSIRT ofrecidos a las partes interesadas. Se trata de una consolidación de los niveles de servicio.

Propósito: en el proceso de creación y mejora de las capacidades de un mandante CSIRT se presta especial atención a ofrecer asistencia en el diseño, adquisición, gestión, operación y mantenimiento de su infraestructura.

Resultado: *elaborar un sistema de evaluación de las necesidades de infraestructura, definición de requisitos, diseño de estructura, adquisición, verificación de cumplimiento, mantenimiento y actualizaciones, formación operativa y auditorías internas y externas.*

Subfunción 6.4.1 **Diseño e ingeniería de infraestructura**: asistir en el diseño e ingeniería de infraestructura para ayudar a que se cumplan los requisitos del mandante.

Propósito: facilitar un amplio entendimiento de la metodología de diseño, ofrecer conocimientos sobre las normas y criterios relevantes, y subrayar las prácticas idóneas en el diseño e ingeniería de la infraestructura a partir de la evaluación de todas las necesidades y del análisis de los requisitos del mandante.

Resultado: *experiencia práctica en el desarrollo y comparación de enfoques y alternativas de diseño de infraestructuras, a partir de prácticas idóneas internacionales y la incorporación de normas y criterios relevantes.*

Subfunción 6.4.2 **Adquisición de infraestructura**: asistir en la adquisición de infraestructura, tanto promoviendo la madurez del marco de riesgos como los requisitos y normas de seguridad mínima para un lenguaje de contrato (por ejemplo, solicitando el cumplimiento de una norma particular como una certificación de producto).

Propósito: conocer mejor la elaboración del mandato para la adquisición de infraestructura a la vista de los requisitos institucionales, técnicos y operativos.

Resultado: *comprender el proceso de adquisición de infraestructura, al tiempo que se respetan las normas y criterios relevantes y se tienen en cuenta las diferentes medidas técnicas y procedimientos de contratación que deben seguirse.*

Subfunción 6.4.3 **Evaluación de herramientas de infraestructura**: evaluación de herramientas en nombre del mandante.

Propósito: proporcionar apoyo en la evaluación de la funcionalidad y la conformidad de varias herramientas, incluido el equipo hardware, el software y las aplicaciones personalizadas.

Resultado: *análisis del rendimiento de herramientas y su conformidad con normas, criterios y el mandato previsto.*

Subfunción 6.4.4 **Obtención de recursos de infraestructura**: asistir en la adquisición de los recursos de infraestructura necesarios (es decir, proveedores de hardware, de servicios, etc.)

Propósito: subrayar los factores fundamentales para obtener satisfactoriamente recursos de infraestructura y elaborar mecanismos para establecer relaciones sostenibles y eficaces con proveedores de soluciones, a partir de una clara responsabilidad y responsabilización.

Resultado: *adquirir indicadores fundamentales de rendimiento (IFR) de recursos de infraestructura, con acuerdos apropiados de nivel de servicios (SLA), que puedan proporcionar recursos de infraestructura eficientes y efectivos.*

Service 7 Investigación/Desarrollo

Función 7.1 **Elaboración de metodologías de descubrimiento/análisis/resolución/análisis de causa principal de vulnerabilidades:** servicios que ayudan a definir y determinar nuevas capacidades y a mejorar metodologías para realizar servicios relativos a la vulnerabilidad o para coordinar otras organizaciones o prácticas comerciales que pueden demostrar lo mismo.

Propósito: algunas organizaciones utilizarán únicamente información de vulnerabilidad obtenida de fuentes exteriores, mientras que otras necesitarán o preferirán disponer de capacidades propias para descubrir y analizar vulnerabilidades. Con esta función se pretende mostrar el grado en que una organización puede planificar estas funciones de investigación de vulnerabilidad.

Resultado: *determinar, cuando sea necesario, las metodologías que una organización puede utilizar para comprender mejor las vulnerabilidades.*

Función 7.2 **Elaboración de procesos de recopilación/fusionado/correlación de información sobre seguridad**: servicios con los que se definen y determinan nuevas capacidades y se mejoran metodologías para realizar análisis de información y compartir servicios conexos relativos a información operativa y de amenazas.

Propósito: para tener éxito, todas las funciones de información sobre seguridad deben recopilar información y compartir la información relevante con terceras partes. Esta recopilación suele depender de si las relaciones personales entre las partes involucradas son de la suficiente confianza como para compartir información que exige una discreción absoluta. El analista deberá poder establecer este tipo de relación, determinar la información adecuada que necesita divulgarse, determinar los protocolos más apropiados para efectuar investigaciones conjuntas,

intercambio automático de información y gestión de relaciones, y evaluar la eficacia de la fuente de información.

***Resultado**: la organización dispone de procesos y procedimientos para recopilar, analizar, sintetizar y evaluar la importancia de la información de fuentes externas con la que se describen las amenazas sobre los activos de seguridad de la información. La organización tiene capacidad interna para obtener nuevas fuentes de información y asociados para compartirla.*

Función 7.3 **Elaboración de herramientas**: servicios con los que se elaboran y determinan nuevas capacidades, y con los que se divulgan enfoques sobre nuevas herramientas para automatizar la ejecución de procesos CSIRT conexos.

***Resultado**: herramientas elaboradas por el CSIRT para ayudarle a automatizar sus tareas CSIRT y que sean modulares, fiables, generen resultados predecibles y no pongan en peligro la seguridad del CSIRT que las utiliza. Liberar los recursos del analista para tareas no rutinarias.*

Recursos de apoyo

FIRST - https://www.first.org

CERT/CC - http://www.cert.org

STIX/TAXII - https://stix.mitre.org

TLP - https://www.us-cert.gov/tlp

IETF - https://www.ietf.org

ISO/IEC 27035 -
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

Glosario

Prueba de aplicación – Investigación realizada para proporcionar a las partes interesadas información sobre la calidad del producto o servicio que se está probando.

Basilea II – Segundo Acuerdo de Basilea, que consiste en recomendaciones sobre el reglamento y las leyes bancarias emitidas por el Comité de Supervisión Bancaria de Basilea.

Capacidad – Actividad cuantificable que se efectúa en el marco de los roles y responsabilidades de una organización. Para cumplir los propósitos del marco de servicios CSIRT, las capacidades pueden definirse como servicios más amplios o como funciones, subfunciones o tareas imprescindibles.

Volumen de capacidad – Número de veces que una organización puede ejecutar una capacidad particular antes de agotar los recursos de algún modo.

CERT/CC – Equipo de intervención en caso de emergencia informática/Centro de coordinación.

CISO – Jefe de Seguridad de la Información.

Nube – Entorno de computación distribuida que permite operar el software de aplicación utilizando dispositivos habilitados para Internet.

COBIT – Objetivos de control de la información y la tecnología conexa.

Troceado criptográfrico – Función de troceado considerada como casi imposible de invertir, es decir, de recrear los datos de entrada a partir únicamente de su valor de troceado.

CSIRT – Equipo de intervención en caso de incidentes de seguridad informática.

Conjunto de datos externos – Recopilación de datos por una tercera parte.

FIRST – Foro de los equipos de intervención en caso de incidentes de seguridad.

Función – Medio para cumplir el propósito o la tarea de un servicio determinado.

Pruebas fuzz – Técnica de prueba de software, a menudo automática o semiautomática, que consiste en proporcionar datos no válidos, inesperados o aleatorios a la entrada de un programa informático.

Emulador de hardware / software – Hardware o software que permite a un sistema informático (llamado anfitrión) comportarse como otro sistema informático (llamado huésped). Normalmente se utiliza para que el sistema anfitrión ejecute un software o utilice dispositivos periféricos diseñados para el sistema huésped.

IEC – Comisión Electrotécnica Internacional.

IETF – Grupo Especial sobre Ingeniería de Internet.

IODEF – Formato para el intercambio de descripciones de objetos de incidentes, una representación de datos con la que se obtiene un marco para compartir la información que los equipos de intervención en caso de incidentes de seguridad informática (CSIRT) intercambian a menudo sobre incidentes de seguridad informática.

ISO – Organización Internacional de Normalización.

Normas de la serie ISO/IEC 27000 (ISO27k) – Normas de seguridad de la información que proporcionan recomendaciones de prácticas idóneas sobre la gestión de la seguridad de la información, riesgos y controles en el contexto de un sistema completo de gestión de la seguridad de la información (ISMS) similar en diseño a los sistemas de gestión de garantía de calidad (serie ISO 9000) y protección medioambiental (serie ISO 140000).

ITIL – Biblioteca de Infraestructura de Tecnología de la Información, un conjunto de prácticas de gestión de servicios TIC (ITSM) que se centra en alinear los servicios TIC con las necesidades de la actividad.

Madurez – Grado de eficacia con el que una organización ejecuta una capacidad particular en la misión y las autoridades de la organización.

Fuente abierta – Modelo de desarrollo que promueve un acceso universal a través de una licencia abierta a un modelo o diseño de producto, y su redistribución universal, incluidas las subsiguientes mejoras realizadas por cualquier persona.

Pruebas de penetración – Ataque a un sistema informático para encontrar carencias en la seguridad, accediendo al mismo, a su funcionalidad y a datos.

Ingeniería inversa – Proceso de extracción de información o información de diseño a partir de cualquier cosa hecha por el hombre, y su reproducción o reproducción de cualquier cosa a partir de la información extraída.

RID – Defensa entre redes en tiempo real, un método de comunicación entre redes para facilitar la divulgación de datos de gestión de incidentes e integrar al mismo tiempo los mecanismos ya existentes de detección, rastreo, identificación de fuente y mitigación para obtener una solución completa de gestión en caso de incidentes.

Sandbox – Mecanismo de seguridad para separar programas en ejecución.

Servicio – Acción de ayudar o realizar un trabajo en nombre de un mandante, o para él.

STIX – Expresión de información de amenazas estructurada, una iniciativa colaborativa comunitaria para definir y elaborar un lenguaje estandarizado con el que representar la información estructurada de ciberamenazas.

Resultado de cadenas – Secuencia resultante de caracteres, como constante literal o como alguna forma de variable.

TAXII – Intercambio fiable y automático de información de indicadores, un conjunto de servicios e intercambios de mensajes que, una vez aplicados, permiten compartir información de ciberamenazas con la que poder actuar dentro de los límites de la organización y el producto/servicio.

TLP – Protocolo ligero de tráfico. Se utiliza para garantizar que la información que exige una discreción absoluta se comparte con la audiencia adecuada.

Entorno virtual – Emulación de un sistema informático particular.

Exploración y evaluación de vulnerabilidades – Técnica de seguridad utilizada para determinar las carencias en la seguridad de un sistema informático.

Anexo – Estructura de servicio

Tal como se ha mencionado en las secciones anteriores, la estructura de servicio adoptada en este marco engloba la identificación de tres capas (áreas de servicio, servicio y funciones) que definen el "qué", y dos capas más (tareas y acciones) que definen el "cómo".
Simplificando, la estructura general es la siguiente: