Capacidad de respuesta ante incidentes

Los incidentes de seguridad requieren una respuesta rápida y eficiente para minimizar el impacto que puedan ocasionar. Para ello, se debe contar con un conjunto de medios (humanos, materiales, organizativos, etc.) que permitan a la organización gestionarlos de forma adecuada.

Este conjunto de medios, debidamente articulados es lo que conforma la **Capacidad de Respuesta ante Incidentes** (***Incident Response Capability*** **o IRC**) de la organización y será fundamental para sentar las bases de una buena gestión de incidentes de seguridad. Por tanto, orquestar una capacidad de respuesta ante incidentes efectiva, debe ser un **objetivo primordial para la Dirección de la organización** dentro de su estrategia de seguridad.

La capacidad de respuesta ante incidentes deberá liderarse por un grupo de trabajo específico. Aunque no existe una nomenclatura oficial para este grupo y cada organización puede adoptar un nombre diferente, adoptaremos para este libro uno de los más usados, **ERI** o **Equipo de Respuesta ante Incidentes** (**IRT** ***Incident Response Team***).

Capacidad de respuesta ante incidentes

En el sector también se encontrarán otras nomenclaturas como:

- **CIRT** (***Computer Incident Response Team,*** Equipo de Respuesta a Incidentes Informáticos).
- **CIRC** (***Computer Incident Response Capability***, Capacidad de Respuesta a Incidentes Informáticos).
- **SERT** (***Security Emergency Response Team***, Equipo de Respuesta a Emergencias de Seguridad).
- **CERT** (***Computer Emergency Response Team***, Equipo de Respuesta a Emergencias Informáticas) o **CSIRT** (***Computer Security Incident Response Team***, Equipo de Respuesta a Incidentes de Seguridad Informática. De estos dos términos hablaremos en detalle más adelante para realizar una serie de aclaraciones.

Capacidad de respuesta ante incidentes

De acuerdo con el **ENS**, **la seguridad se concibe como una actividad integral**, en la que no caben actuaciones puntuales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas, pero deficientemente ensambladas. Es por lo que **las organizaciones deben decidir cuáles son los servicios que deberá proveer el equipo de respuesta a incidentes**, **qué estructura y modelo tendrán** (comúnmente formarán parte del Departamento de Seguridad de la compañía) **y cómo interactuarán con otros equipos**, tanto dentro como fuera de la organización. Los medios que conformen la capacidad de respuesta ante incidentes deberán estar debidamente coordinados para dar una respuesta ágil, eficaz, y proporcionada.

Capacidad de respuesta ante incidentes

En definitiva, *las organizaciones tienen que establecer una capacidad de respuesta que les permita gestionar los incidentes de una forma acorde a sus políticas y requisitos de seguridad* de forma que:

- Se responda de forma que **se minimice la probabilidad de ocurrencia de un incidente** y, si este se materializa, **se mitigue su impacto** asociado en la organización.
- Se aborde la gestión de los incidentes de seguridad a través de una **metodología aprobada y apoyada por la Dirección** y conocida por toda la organización.
- Se mejore la seguridad corporativa en su conjunto a través del **aprendizaje** obtenido en el proceso de gestión de incidentes.

Capacidad de respuesta ante incidentes

EQUIPO DE RESPUESTA ANTE INCIDENTES (ERI)

El equipo de respuesta ante incidentes o **ERI es el conjunto de analistas especializado que**, junto con los medios de los que dispone, **dará respuesta a cualquier notificación sobre un incidente bajo su ámbito de actuación.** En todo momento deberá estar disponible para analizar cualquier amenaza identificada, determinará su impacto y actuará de la forma más apropiada -siempre de acuerdo a los procedimientos establecidos, para limitar los daños, y restablecer la normalidad a la mayor brevedad.

Respecto a los **modelos** que puede adoptar un **ERI**, se puede hablar de:

1. **ERI centralizado.** Un único equipo de gestión de incidentes conforma la capacidad de respuesta en la organización; este ***modelo*** es ***eficaz para organizaciones pequeñas*** (por ejemplo, PYMES) o bien para organizaciones de tamaño mayor, pero con poca dispersión geográfica.
2. **ERI distribuidos.** La organización tiene varios ERI responsables de diferentes ámbitos. Este **modelo** es **eficaz para organizaciones grandes y para organizaciones con importantes recursos informáticos en ubicaciones distantes**.

Capacidad de respuesta ante incidentes

En este modelo se pueden encontrar por ejemplo ERI por áreas (por ejemplo, un ERI encargado de los incidentes de ciberseguridad perimetral, otro ERI responsable de los incidentes de ciberseguridad industrial OT Operational Technology), otro ERI encargado de los incidentes relacionados con el puesto de trabajo, etc.), ERI por distribución geográfica (por ejemplo, un ERI por país o zonas, o por ciudades, etc.). A pesar de estar distribuidos, los equipos deberían formar parte de un único equipo global para que el proceso de respuesta a incidentes sea coherente en toda la organización y la información fluya entre todos los equipos, ya que puede darse el caso de varios ERI involucrados en la gestión de un mismo incidente. De esta forma, la compartición de información entre los equipos también mejoraría los métodos de gestión de los incidentes, así como la capacidad ciber defensiva de la organización puesto que la inteligencia que recabe un ERI puede ser diseminada al resto de equipos aumentando así sus capacidades preventivas y reactivas.

Se puede valorar un modelo híbrido, mezcla de los anteriores, en el que un ERI coordinador proporciona apoyo a los equipos de gestión de incidentes de la organización.

Capacidad de respuesta ante incidentes

El **equipo humano que conforme el ERI** debe tener unas características muy particulares como **un conocimiento técnico muy especializado, ser multidisciplinar, poder trabajar bajo presión, estar en continuo aprendizaje, etc.** así que las organizaciones deben evaluar minuciosamente la plantilla del personal del equipo que formará parte del ERI de forma que contemplen un equipo íntegramente formado por empleados de la compañía, con apoyo limitado y puntual de los proveedores, o bien que se opte por la externalización parcial o completa del equipo de respuesta ante incidentes.

Este tipo de modelos tienes sus ventajas y sus inconvenientes. Por ejemplo, entre los **pros de un equipo completamente externalizado** (generalmente será provisto por una empresa especializada en ciberseguridad), al estar dedicado habitualmente a un conjunto de clientes variado, **tendrá mucha experiencia en diferentes tecnologías**, entornos y **estará en continua actividad gestionando todo tipo de incidentes,** con lo que tendrá una capacidad de reacción muy bien entrenada. Además, t**endrá una visión global de las tendencias de los ataques** que pueden estar sufriendo otros clientes y aportar ese conocimiento a la organización. Otra ventaja podría ser el

ahorro de costes de personal especializado. Dependiendo de los recursos de la organización, tener un equipo interno especializado, con formación continuada en ciberseguridad, puede suponer un coste económico importante.

Por el contrario, un equipo externalizado **no conocerá tanto la infraestructura y el negocio de la compañía como un empleado** de esta, y en el caso de que se requiera presencialidad para dar respuesta al incidente, se aumentará el tiempo de respuesta por el desplazamiento si el equipo externalizado no está prestando el servicio *in situ*.

Una solución intermedia sería un **ERI parcialmente externalizado**, en el que la organización delega ciertos aspectos de la gestión de incidentes a uno o más proveedores externos. Un modelo interesante podría ser disponer de **un pequeño equipo de empleados de la organización especialistas en ciberseguridad que hagan de interfaz con los proveedores externos contratados**. Este modelo permite a la organización flexibilidad y funcionalidad.

En síntesis, los principales **factores** que las organizaciones deberían considerar para optar **por un modelo u otro** serían los siguientes:

Capacidad de respuesta ante incidentes

- Tamaño, estructura y dispersión geográfica de la compañía.
- Necesidad de disponer de una capacidad de respuesta 24/7.
- Conocimiento técnico y especializado de los empleados.
- Disponibilidad de los empleados.
- Coste económico.

Aunque el principal cometido del ERI es la gestión de incidentes de seguridad, ***suelen ser los responsables también de la operación de los sistemas de detección de intrusos, del despliegue y operación de sistemas de vigilancia en la red, de sistemas antimalware/antirootkits, Data Loss Prevention (DLP), sistemas de contrainteligencia como honeypots, etc.*** es decir, todo lo relacionado con la monitorización y gestión de las alertas de seguridad. Cada vez más, también estos equipos ofrecen a sus clientes servicios preventivos como **la formación**, la **distribución de avisos de seguridad** a otros grupos de la organización sobre distintas temáticas (vulnerabilidades publicadas, nuevas amenazas, campañas de fraude a través de correo electrónico, leaks de información, entre otros), **servicios para la**

mejora de la calidad de la gestión de la seguridad, sistemas de alerta temprana, etc.

El ERI **también podría llevar a cabo auditorias de vulnerabilidades** sobre los sistemas y redes bajo su ámbito con el objetivo de obtener fallos de seguridad no identificados y poder subsanarlos. En la práctica, lo habitual es encontrarnos con ERI enmarcados dentro de un Departamento o equipo de Seguridad, en el que hay perfiles especializados por ejemplo para la parte de auditoría, para prevención del fraude, etc. y cuya comunicación con el ERI es constante y muy fluida, trabajando de forma colaborativa en todo momento.

El éxito de un ERI está vinculado a la cooperación de los individuos en toda la organización por lo que es imprescindible que la misma disponga de una estructura apropiada que dote al equipo de respuesta ante incidentes de capacidad de maniobra, contundencia y de los medios necesarios para el desempeño de su trabajo.

Es importante remarcar que la creación de un equipo de respuesta no implica implantar solo tecnología o designar un grupo de personas, sino adoptar una serie

de procesos en toda la organización, no sólo en el Departamento de TI, gestionados de acuerdo a unas normas que persiguen cumplir unos objetivos concretos.

Como se ha comentado un modelo común de organización que se puede encontrar es el de un ERI integrado en la propia compañía a la que presta el servicio, habitualmente integrado dentro del Departamento de Seguridad.

También es posible encontrar equipos de respuesta ante incidentes con un modelo de organización con entidad propia (CERT, CSIRT) o formando parte de centros de operaciones de seguridad (SOC). En el siguiente apartado se aclararán algunos conceptos relacionados con estos términos.

Capacidad de respuesta ante incidentes

SOC, CSIRT, CERT

Los términos **CERT, CSIRT SOC** son habituales en el ámbito de la respuesta a incidentes de seguridad. Aunque puedan describir equipos que hacen funciones similares, es necesario aclarar ciertos matices.

Tanto el término **CERT** (Equipo de Respuesta ante Emergencias Informáticas) como el término **CSIRT** (Equipo de Respuesta ante Incidentes de Seguridad Informática) **suelen usarse para describir equipos centrados en la respuesta a incidentes de seguridad**. No obstante, hay que aclarar que el término **CERT es una marca registrada por la Universidad *Carnegie Mellon* de Pensilvania**, Estados Unidos.

En el año 1988 se tuvo constancia de la creación del primer ejemplar de *malware* auto replicable, el gusano Morris, que afectó a casi el 10% sistemas conectados a ARPANET, el antecesor de la actual Internet. Este incidente de seguridad manifestó la necesidad de coordinar el trabajo del personal de TI de una manera ágil y eficaz. A raíz de este caso la DARPA (*Defense Advanced Research Proyects Agency*) patrocinó la creación del primer Equipo de Respuesta ante Incidentes, el CERT *Coordination Center* (CERT/CC) ubicado en la anteriormente citada, *Universidad Carnegie Mellon*.

Capacidad de respuesta ante incidentes

Poco después, empezó a hablarse de CSIRT para completar el concepto de CERT, y ofrecer como valor añadido los servicios preventivos y de gestión de seguridad, asumiendo el resto de las actividades clave de la gestión de la seguridad.

Tal y como se describe en **la Guía de Seguridad (CCN-STIC-810). "Guía de Creación de un CERT/CSIRT"** del CCN, tradicionalmente la definición de CERT engloba un equipo o capacidad de un organismo de ofrecer servicios y soporte a un colectivo determinado ámbito de actuación para prevenir, gestionar y responder a los incidentes de seguridad de la información que puedan surgir.

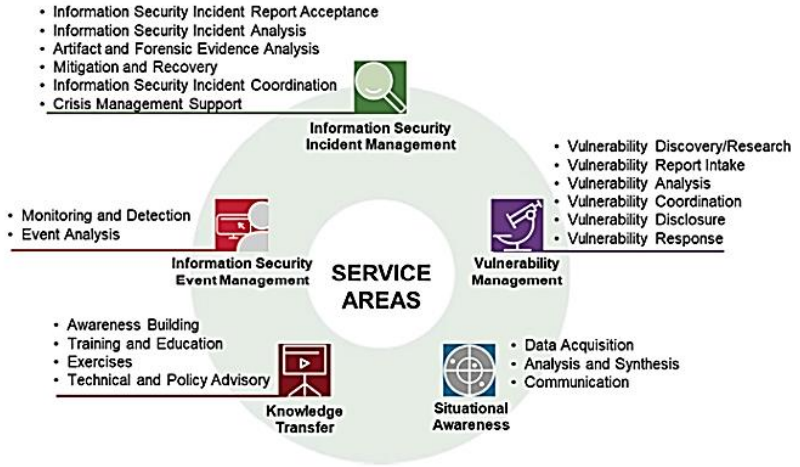
Capacidad de respuesta ante incidentes

"Esta definición genérica viene materializándose en un equipo multidisciplinar de expertos que trabaja según unos procesos definidos previamente y que disponen de unos medios determinados para implantar y gestionar, de un modo centralizado, todas y cada una de las medidas necesarias para mitigar el riesgo de ataques contra los sistemas de la Comunidad a la que presta el servicio y responder de forma rápida y efectiva en caso de producirse."

Sin embargo, los servicios que engloban este tipo de equipos han ido evolucionando con el tiempo y sus funciones se han visto ampliadas incluyendo otras adicionales como tareas preventivas o de recuperación tras un incidente o la gestión de vulnerabilidades. Algunos equipos incluso operan sus propios sistemas y comunicaciones, como se ha mencionado con anterioridad.

Este modelo viene alineado con el concepto que venimos repitiendo en el libro de modelo integral de gestión la seguridad entendiendo la misma como un proceso centralizado, colaborativo, y teniendo en cuenta todos los elementos técnicos, humanos, materiales y organizativos y en donde sobresalen los servicios proactivos y de alerta temprana.

Capacidad de respuesta ante incidentes



CSIRT Services Framework Areas and Services. Fuente: FIRST

Capacidad de respuesta ante incidentes

En el panorama internacional el foro de CERT/CSIRT más importante es **FIRST** (*Forum of Incident Response and Security Teams*) En Europa, el principal foro es TF-CSIRT-Trusted Introducer

En el ámbito estatal, los foros de referencia son **CSIRT.es** y la **Red Nacional de SOC** (Centro de Operaciones del Ciberespacio).

El foro CSIRT.es se trata de una plataforma independiente sin ánimo de lucro compuesta por CERT/CSIRT cuyo ámbito de actuación o comunidad de usuarios en la que opera, se encuentra en España. Su misión se describe como:

"El Foro CSIRT.es pretende crear una plataforma independiente de coordinación y colaboración de confianza entre los CSIRT de ámbito nacional que permita optimizar la cooperación entre los mismos para actuar frente a problemas de seguridad informática en las redes españolas. A su vez, fomentar la divulgación de información de interés y la mejora de la visibilidad de los CSIRT miembros del Foro en la comunidad española e internacional".

Capacidad de respuesta ante incidentes

Entre los miembros de CSIRT.es se encuentran los principales centros públicos de referencia a nivel estatal (CCN-CERT, INCIBE, MCCE), centros de ámbito regional (CSIRT-CV -Centro de Ciberseguridad de la Comunitat Valenciana- que fue el primer CERT autonómico que se creó en España, Andalucia-CERT, Basque Cybersecurity Centre, CSIRT CARM -Región de Murcia-, CSIRT.gal -Galicia-, etc.), representantes de la comunidad educativa (IRIS-CERT, esCERT-UPC - Universidad Politécnica de Cataluña, primer CERT creado en España, CSUC-CSIRT -Consorci de Serveis Universitaris de Catalunya-), también FFCCSE (Ertzaintza SCDTI, Mossos d'Esquadra, Policia Nacional y Guardia Civil con 2 departamentos representados), y también empresas privadas y clientes finales (CaixaBank, S2 Grupo, Entelgy Innotec Security, CSA, etc.).

Respecto a la RNS o Red Nacional de SOC (Centro de Operaciones del Ciberespacio), es un foro que celebra su primer encuentro en octubre de 2021 a iniciativa del Centro Criptológico Nacional, con el fin de mejorar las capacidades de protección y defensa del ciberespacio español. Para coordinar esta Red Nacional de SOC el RD 43/2021, que desarrolla la directiva se seguridad en redes de la UE, establece en su artículo 11

Capacidad de respuesta ante incidentes

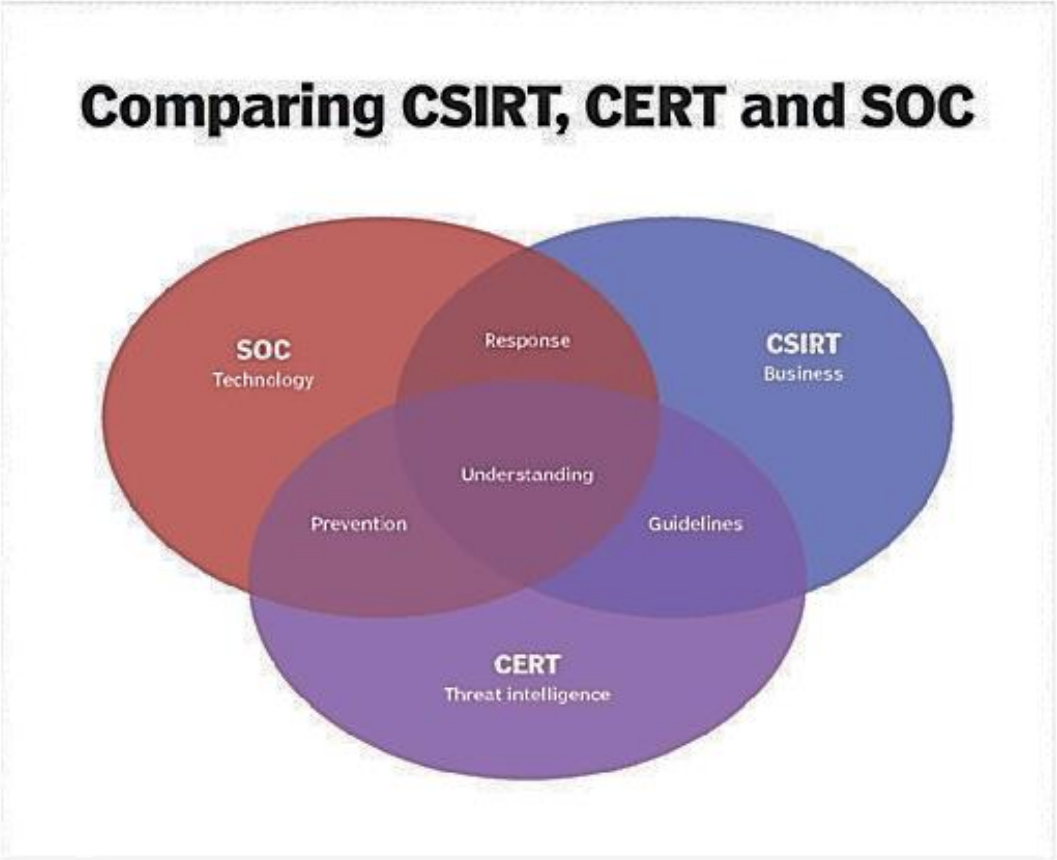
la creación de una Plataforma Nacional de Notificación y Seguimiento de Ciber incidentes sobre la base de los tres Equipos de Respuesta ante Emergencias Informáticas (CERT) de Referencia: CCN-CERT, INCIBE-CERT y el ESP-DEFCERT del Mando Conjunto del Ciberespacio.

Para formar parte de este tipo de foros es necesario llevar a cabo un proceso de acreditación para asegurar y preservar la confianza entre los miembros.

Un SOC es más amplio en su alcance y puede incluir la función de respuesta al incidente, tanto parcial como total, así como otras tareas como podrían ser:

- **Supervisar y operar monitorización** el despliegue de los sistemas de monitorización de eventos de seguridad y recolección de información.
- **Administrar** tareas como la **gestión de identidades**
- **Administrar dispositivos perimetrales de seguridad** como firewalls (reglas de filtrado, gestión de cambios, etc.).
- **Realizar análisis forenses**.
- Etc.

Capacidad de respuesta ante incidentes



Un ejemplo de servicios que podría prestar un CSIRT lo podemos consultar en el catálogo que ofrece CSIRT-CV que además de llevar a cabo la respuesta a incidentes de seguridad también ofrece servicios a determinados colectivos dentro de la

Capacidad de respuesta ante incidentes

Comunitat Valenciana. Entre los servicios que ofrece se pueden encontrar reactivos (alertas y advertencias. gestión y respuesta a incidentes, detección de intrusiones, monitorización de portales web), preventivos (avisos, auditorias, test de intrusión, divulgación de información, cuadro de mando), o de valor añadido como la formación, concienciación, asesoría técnica y legal o la seguridad semántica.

A la hora de dimensionar este tipo de equipos se deberán considerar parámetros como los siguientes:

- Tamaño del ámbito al que presta el servicio. A mayor número de miembros se generarán más notificaciones de incidentes a gestionar, así como peticiones de otro tipo de servicios.
- Grado de autoridad sobre los miembros del ámbito al que presta el servicio y el modelo de relación jerárquica entre ambos.
- Servicios ofrecidos y nivel de servicio. Si se ofrece un soporte de 24x7x365 se requerirán muchos más recursos. También hay que considerar los acuerdos de niveles de servicio o tiempos de respuesta mínimos.
- Promoción y comunicación de los servicios.

Capacidad de respuesta ante incidentes

- Plan estratégico del equipo. Es recomendable planificar de forma adecuada la evolución del equipo prestando especial atención a aspecto como la financiación, la incorporación de nuevos servicios, o la puesta en marcha de nuevas iniciativas.

En conclusión, los CSIRT y los CERT se centran específicamente en la respuesta a incidentes, aunque han ido evolucionando a lo largo del tiempo incluyendo entre los servicios que prestan también los relativos a seguridad proactiva, preventiva y de recuperación tras el incidente. **Los dos términos se usan a menudo como sinónimos.** El alcance de un SOC tradicionalmente ha sido considerado más amplio que la respuesta a incidentes y se extiende a otras áreas de seguridad; sin embargo**, hoy en día los términos CERT, CSIRT y SOC son casi homónimos.**

Equipo humano

En la práctica, un equipo de respuesta ante incidentes está constituido por un grupo de analistas especializados que, según unos procedimientos definidos, y siguiendo la política de seguridad de la organización, hacen uso de los medios de los que dispongan para proporcionar servicios de gestión y respuesta de incidentes (además

de otros no específicamente relacionados con incidentes tal y como ya se ha comentado en su ámbito de actuación.

Como se verá a lo largo del libro, la gestión de un incidente conlleva identificadas dos esferas de actuación: por un lado, la operativa y de respuesta técnica al incidente y por otro la organizativa y estratégica, en la medida en que su impacto afecta a diferentes ámbitos de la organización. Por tanto, para afrontar las amenazas es imprescindible tener un gran conocimiento organizativo, normativo y técnico, y estar continuamente al día en cuestiones de seguridad. Es por ello que lo recomendable es disponer de un equipo de trabajo multidisciplinar y con gran experiencia demostrable.

Aunque el número de miembros del equipo dependerá del ámbito de actuación y otros factores (mencionados en el punto anterior) es importante contar con figuras como:

- **Responsable global del equipo**, que dependiendo del tipo de centro que tengamos podemos llamar director del CERT CSIRT, Coordinador del ERI, O SOC Manager

Capacidad de respuesta ante incidentes

(cualquier nombre que represente la figura de un responsable global del equipo). Debería tener una formación y amplia experiencia en el ámbito de la ciberseguridad, sobre todo en procesos de gestión de crisis y recuperación de negocio.

- **Especialistas** de carácter técnico, analistas de seguridad. Serán los que ejecuten las tareas de los servicios técnicos que se presten.
  Dependiendo de los servicios que se oferten podrían encontrarse expertos en gestión y respuesta de incidentes de seguridad, especialistas en hacking ético y gestión de vulnerabilidades, analistas forenses, analistas de malware, especialistas en ciber inteligencia, etc.
  Este tipo de perfiles debe poseer conocimientos extensos en seguridad, así como una experiencia en cada ámbito particular que complemente dichos conocimientos.
- **Expertos en leyes y normativas** que presten apoyo en la gestión de incidentes o presten servicios si los hubiera de esta índole.

Capacidad de respuesta ante incidentes

En el caso de que el propio CERT sea responsable de la operación, administración y mantenimiento de sus sistemas TIC, se necesitará un responsable de Ingeniería o similar.

Adicionalmente se pueden sumar al equipo administradores de sistemas y redes, operadores de seguridad, o cualquier otro personal implicado en la gestión y operación de equipos de seguridad.

Dependiendo del tipo de incidente a gestionar o el servicio prestado es posible que el equipo deba contar con expertos de una determinada área de conocimiento. Por ejemplo, expertos en cloud, en sistemas de virtualización, en tecnología IoT, en pasarelas de pago, en desarrollo de software, en comunicación o relaciones públicas, etc. Por ello, es conveniente que tanto si se dispone de personal interno que cubra estas necesidades como si se tiene que contar con apoyo externo se tengan definidos listados de colaboradores y procedimientos adecuados que faciliten su incorporación al equipo de respuesta a incidentes en el momento en el que se les requiera. En el siguiente punto del libro se tratarán estos aspectos en profundidad identificando que otros actores deben tenerse en cuenta en la gestión de incidentes de seguridad.

Capacidad de respuesta ante incidentes

En muchos centros suele prevalecer por operatividad y economía un modelo jerarquizado (Modelo de Tiers); por ejemplo, en los SOC se puede encontrar que el equipo de analistas técnicos está compuesto por un primer nivel de operación que filtra inicialmente las alertas recibidas sobre posibles incidentes. Este nivel 1 (Tier 1) suele trabajar con procedimientos operativos o playbooks que le indican qué pasos seguir según el tipo de notificación o alerta recibida. Estos perfiles necesitan tener un grado de conocimiento técnico básico suficiente para entender la situación notificada, trabajando por procedimientos la mayor parte del tiempo, permanecen en una situación de monitorización continua de las alertas que van recibiendo y haciendo un análisis previo inicial ante posibles incidentes. Para ello suelen hacer uso de herramientas de gestión de eventos de seguridad, como el SIEM (Security Information and Event Management), del que hablaremos más adelante.

Luego se encontraría un segundo nivel (Tier 2) que apoyaría al nivel 1 en el análisis de las amenazas y seria el encargado de llevar a cabo investigaciones más avanzadas en caso de que se declare un incidente de seguridad. Suelen ser los responsables de estudiar nuevas amenazas, definir patrones de detección, establecer reglas de

correlación que ayuden a identificar nuevos ataques o cualquier otro tipo de tarea operativa centrada en la mejora de la monitorización, detección y análisis de amenazas.

Por último, se disponen de especialistas de tercer nivel (Tier 3) que serían los que tienen más experiencia del equipo y gestionarían los incidentes de seguridad más complejos dando apoyo a los niveles inferiores o se encargarían de tareas más específicas como el análisis o reversing de una pieza de malware, tareas de threat hunting, un análisis forense o pericial, apoyo en una actuación en una tecnología determinada, etc. Este tipo de perfiles tienen un gran conocimiento técnico y grandes habilidades tanto de análisis como de comunicación. Deben saber trabajar en entornos complejos y mantener la calma para asesorar de forma adecuada en situaciones de emergencia que un incidente de seguridad pueda provocar.

Un resumen de algunas habilidades que deben tener cada uno de los perfiles mencionados se recogen en la tabla a continuación:

Capacidad de respuesta ante incidentes

Roles	Habilidades requeridas
SOC MANAGER	Gran capacidad de liderazgo, habilidades de comunicación y organización.
TIER 3	Gran experiencia en materias específicas como el *Threat Hunting*, análisis forense, técnicas de *hacking* avanzado, etc. Existen varios roles. Son perfiles metódicos y con gran capacidad de análisis.
TIER 2	Son los analistas que responden inicialmente al incidente de seguridad y por tanto deben tener una gran capacidad de trabajar bajo presión, ser capaces de mantener la calma ante situaciones de estrés, y tener una gran curiosidad por el entendimiento de las situaciones.
TIER 1	Analistas expertos en el triage de las alertas y notificaciones recibidas, por tanto, deben tener al menos un conocimiento genérico de todos los tipos de incidentes al que se pueden enfrentar. Deben saber identificar situaciones de riesgo y ser metódicos a la hora de seguir los procedimientos operativos o *playbooks* definidos.

Por supuesto este es solo un ejemplo de lo que se suele encontrar en la conformación de un equipo de respuesta ante incidentes, CERT/CSIRT O SOC, pero cada organización tiene la libertad de diseñarlo bajo los criterios que mejor se adecúen a sus expectativas.

Las personas que conforman estos equipos deben contar con una formación y experiencia previa especifica dependiendo de su rol. Deberán estar en continuo aprendizaje y **formación permanente**, puesto que será necesario que adquieran toda la información posible sobre el funcionamiento a todos los niveles (técnico, organizativo, funcional) de la organización y estar actualizados en los principales aspectos en cuanto a operaciones en el ciberespacio. Además de la requerida

formación permanente, estos equipos deben estar en continuo entrenamiento y, es por ello por lo que se recomienda que participen de forma periódica en ciber ejercicios o simulacros.

OTROS ACTORES INVOLUCRADOS

Es fundamental identificar qué grupos dentro de la organización podrían ser necesarios en la colaboración de la gestión de un incidente.

Para que la gestión de incidentes sea eficiente, el ERI debe tener el apoyo de una serie de grupos o departamentos internos a la compañía, e igualmente debe

Capacidad de respuesta ante incidentes

establecer relaciones -puntuales o habituales, con agentes externos que pudieran ser de interés. Algunos de estos actores son los que se detallan a continuación:

- **Equipo directivo de la organización**. La Dirección o Gerencia deberá establecer las prioridades y requisitos del servicio de respuesta ante incidentes. Como con cualquier área, deberá definir aspectos como la dotación económica o de personal para el ERI, así como la política a alto nivel del equipo. Sin el apoyo de la Dirección es poco probable que un ERI tenga éxito.
  Habitualmente el ERI reportará periódicamente al equipo directivo su trabajo, especialmente si hay algún incidente de especial relevancia.
  Aunque el ERI tenga full authority (plena autoridad) o shared authority (autoridad compartida para ejecutar cualquier tarea que considere en la gestión de los incidentes de seguridad, en última instancia la dirección corporativa deberá asumir ciertas decisiones y responsabilidades sobre acciones a ejecutar en la gestión de determinados incidentes.
- **Departamento de Seguridad** El ERI normalmente estará integrado en este departamento, que, además dispondrá de otros servicios clave para la seguridad

de la compañía como por ejemplo la gestión de la seguridad de los elementos de red o de sistemas, gestión de seguridad física, cumplimiento y normativa, etc.
Por tanto, el ERI deberá contar con la ayuda de todo este departamento a la hora de hacer la gestión de un incidente, principalmente en la fase de análisis o contención del incidente (por ejemplo, crear nuevas reglas en un Firewall, desplegar nuevas firmas en un antivirus, deshabilitar ciertos usuarios en un determinado sistema, bloquear correos electrónicos con determinadas características, etc.)
Algunos incidentes podrían ocurrir a través de violaciones de la seguridad física o implican ataques lógicos y físicos coordinados. O quizá el ERI necesite acceso a determinadas instalaciones de acceso
restringido durante la investigación del incidente.

- **Departamento/s TI.** Los departamentos tecnológicos (Sistemas. Comunicaciones y Redes. Desarrollo, Aplicaciones. Puesto de Trabajo, expertos en Cloud, etc.) son esenciales dentro de la gestión de un incidente en los que se requiera su colaboración.

Capacidad de respuesta ante incidentes

El conocimiento especializado del personal de estos departamentos sobre la propia infraestructura de la organización, su tecnología, sus aplicaciones, etc. juegan un papel crucial a la hora de dotar al ERI de la información necesaria para tomar las decisiones más adecuadas (por ejemplo determinar cuáles son los activos más críticos, cual es el impacto de interrumpir un determinado servicio, como se puede llevar a cabo un bloqueo de usuarios en una determinada tecnología, apoyo en la fase de recolección de evidencias si la hubiere, probar una PoC sobre un determinado sistema, etc.).

- **Departamento Legal.** El ERI debe tener un amplio soporte legal en cualquier fase de la gestión del incidente que se requiera. Este equipo supervisará los procedimientos de respuesta a incidentes para garantizar el cumplimiento de la ley asesorando al ERI en aspectos tales como monitorización y análisis de datos, almacenamiento de evidencias, cadena de custodia, posibles peritajes o denuncias, etc.
- **Relaciones públicas y con los medios de comunicación**. Dependiendo de la naturaleza del incidente puede existir la necesidad u obligatoriedad de hacer comunicaciones a terceros relativas a la situación del incidente.

Capacidad de respuesta ante incidentes

Los equipos encargados de comunicaciones con la prensa o el equipo de relaciones públicas son los que, en coordinación con el ERI y la Dirección Corporativa suelen canalizar este tipo de comunicaciones ya que disponen de los medios y experiencia adecuados para tal fin.

Toda comunicación al exterior debe estar consensuada por los equipos implicados en la gestión del incidente, aprobada por Dirección y supervisada en algunos escenarios por el Departamento Legal.

- **Recursos Humanos.** Tanto si un empleado es víctima de un incidente o se sospecha que sea el origen de este (los denominados insiders o atacantes internos), el departamento de Recursos Humanos a menudo se involucra en ayudar a asesorar a dichos empleados o llevar a cabo procedimientos disciplinarios contra ellos.
- **Equipo responsable del Plan de Continuidad de Negocio de la compañía**. Las organizaciones deben contar con un Plan de Continuidad del Negocio (o por sus siglas en inglés BCP, Business Continuity Plan) que detalle como una organización debe recuperar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo deseado después de una interrupción no deseada. Este tipo de interrupciones podrían ser provocadas por un incidente de seguridad y es por ello

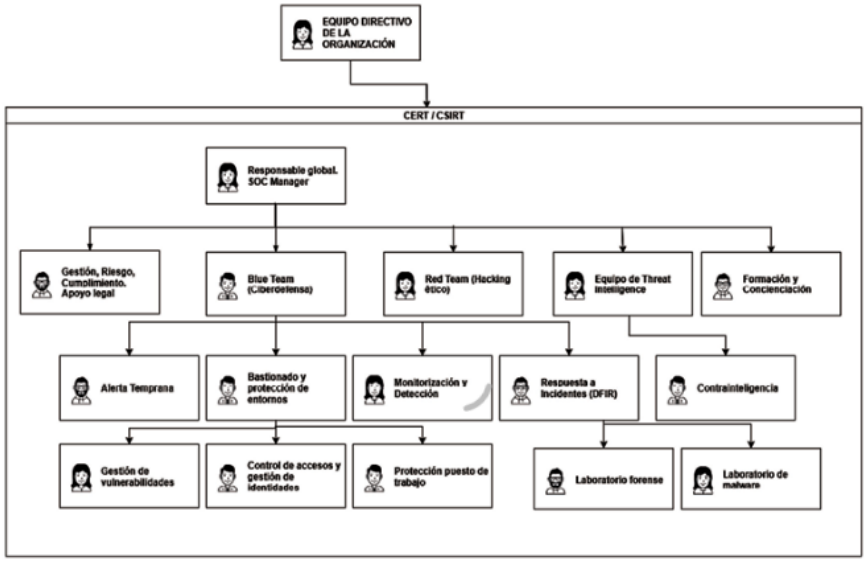
Capacidad de respuesta ante incidentes

que el equipo responsable del BCP debe estar al tanto de cualquier incidente y su impacto para que evalúen el riesgo y la continuidad de las operaciones del negocio. Además, debido a que este departamento suele tener una amplia experiencia en minimizar la interrupción operativa durante circunstancias críticas, pueden ser de valiosa ayuda en la planificación de respuesta a ciertos tipos de incidentes como una denegación de servicio (DoS o Denial of Service), el compromiso de un activo crítico para la actividad empresarial como por ejemplo un servidor de correo, el cifrado de todos los activos de la compañía a través de un ransomware, etc.

En definitiva, las políticas y procedimientos de respuesta ante incidentes deben estar alineados con los planes de continuidad de negocio de la organización.

Un ejemplo orientativo, sin establecer muchos niveles de profundidad en la definición de roles y sin entrar en detalles, de cómo podría ser la estructura de un CERT/CSIRT podría ser el siguiente:

Capacidad de respuesta ante incidentes



El CERT podría depender directamente de la dirección de la compañía (o de la dirección del Departamento de Seguridad) y estaría liderado por un responsable o SOC Manager, del cual dependerían diferentes unidades: la unidad de Gestión, Riesgo y Cumplimiento, el equipo de ciberdefensa o Blue-Team, el equipo de ciberataque o Red-Team, el equipo de inteligencia de las amenazas o Threat Intelligence y el equipo de Formación y Concienciación

Capacidad de respuesta ante incidentes

Es importante también que el Departamento de Seguridad de la compañía, especialmente el ERI, también tenga vínculos con determinados **actores externos** que pueden ser de gran ayuda en la gestión de ciertos incidentes estableciendo un canal de comunicación bidireccional:

- **Fuerzas y Cuerpos de Seguridad del Estado**. La comunicación entre ambos grupos debe servir para facilitar a las FFCCSE información relativa a delitos que pudieran darse en el ámbito de la. En España es posible denunciar un delito telemático tanto ante la Guardia Civil, a través del Departamento de Delitos Telemáticos, como ante la Policía Nacional, a través de la Brigada Central de Investigación Tecnológica (B.C.IT). además de en otros sitios, como en sede judicial, policías autonómicas...
- **CERT/CSIRT de referencia**. Un CERT o un CSIRT de referencia es un equipo de respuesta a incidentes externo a la organización en cuyo ámbito de actuación pueda encontrarse la misma. Los CERT/CSIRT de referencia pueden prestar apoyo operativo total o parcial en la gestión de determinados incidentes, así como pueden dotar a la organización de información relevante sobre nuevas

Capacidad de respuesta ante incidentes

amenazas, vulnerabilidades, o compromiso de datos que puedan afectar a la organización.

En España, el Sector Público, los ciudadanos y empresas, las infraestructuras críticas y operadores estratégicos, las redes académicas y de investigación, así como las redes de defensa, tienen a su disposición una serie de CSIRT de referencia:

- **CCN-CERT,** con un ámbito competencial en el Sector Público general, autonómico y local, y sistemas que manejan información clasificada.
- **INCIBE-CERT,** con un ámbito competencial en la ciudadanía, el sector privado y las instituciones afiliadas a Red IRIS (red académica española), en coordinación con el CCN-CERT en lo que se refiere a organismos públicos.
- **Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)** con un ámbito competencial en las infraestructuras críticas, operadores críticos y servicios esenciales.
- **ESP-DEF-CERT del Mando Conjunto del Ciberespacio**, con ámbito competencial en las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes

y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional.

Algunas Comunidades Autónomas cuentan con su propio CERT de referencia como es el caso del CSIRT-CV en la Comunitat Valenciana, la Agencia de Ciberseguridad de Cataluña, Andalucía-CERT, el Basque Cybersecurity Centre, CSIRT.gal, etc. La mayoría de los servicios que prestan estos CERT son para el sector público (Administración autonómica o Entidades Locales) o ciudadanos (principalmente en materia de asesoría y concienciación en ciberseguridad).

- **Fabricantes y proveedores de productos y sistemas utilizados en la organización.** El ERI deberá establecer contacto con estos grupos para obtener de primera mano información relativa a la seguridad de la tecnología, sistemas, productos o servicios que provean información sobre vulnerabilidades, parches de seguridad, bastionado de entornos, etc.). Habitualmente esta relación se mantiene a través del propio contrato de soporte entre la compañía y el proveedor.

  Es relevante también el papel del proveedor en la respuesta a incidentes que pudieran afectar a sus productos, sistemas o servicios ya que son los que más

conocen sus tecnologías y particularidades y pueden proporcionar el apoyo especializado en caso de ser necesario. Un ejemplo importante es el papel que pueda tener el ISP (Internet Service Providers) contratado a la hora de ayudar a mitigar un ataque de Denegación de Servicio.

En este grupo también entrarían todos los servicios externalizados que pudiera tener la organización ya que al igual que un incidente en la organización puede afectarles, un incidente en un proveedor puede poner en jaque la seguridad de las organizaciones que utilicen sus productos o servicios. De hecho, en la actualidad uno de los ataques más habituales -por el gran potencial que tiene- es el ataque a la cadena de suministro (en inglés, Supply Chain Attack), también llamado “ataque a terceros" ya que consiste en comprometer a proveedores de servicios externos como instrumento para infiltrarse desde allí en una o varias organizaciones objetivo. Un ejemplo conocido de un incidente ocasionado por este tipo de ataques fue el que tuvo lugar en 2017 provocado por la infección a gran escala del malware NotPetya, en el que el vector de infección fue la actualización de la suite MeDoc, un software de contabilidad de uso recurrente en países como Ucrania o Rusia.” Otro ejemplo más reciente fue el que afectó

en 2020 a la compañía Solar Winds, en la que se implementó una actualización con malware Sunburst para su conocida aplicación de monitorización de redes, Orion.

UNIDAD DE CIBERINTELIGENCIA

La OTAN define el término inteligencia como el producto resultante del procesamiento de información relativa a naciones extranjeras, fuerzas o elementos hostiles o potencialmente hostiles o áreas de operaciones reales o potenciales, y también aplica el término a la actividad cuyo resultado es justamente este producto, esta inteligencia. Simplificando, podríamos hablar de inteligencia como el producto resultante de un análisis de información cuyo objeto es facilitar la toma de decisiones.

Son varios los conceptos que se pueden expresar con el término inteligencia. *Sherman Kent*, el considerado padre de la inteligencia estratégica, **identificó el término con tres conceptos:**

Capacidad de respuesta ante incidentes

- **El *producto* derivado de la transformación de la información y el conocimiento en inteligencia**. La inteligencia como producto es el resultado que se obtiene al someter los datos y la información a un proceso intelectual que los convierte en informes adecuados para satisfacer las necesidades de los políticos, militares, empresarios, policías, etc. así como para proteger a aquellos mediante las tareas de contrainteligencia.

  Trasladando este concepto al plano cibernético consideraríamos ciber inteligencia o inteligencia de amenazas (Threat Intelligence) a la adquisición y el análisis de información para identificar y predecir capacidades cibernéticas, intenciones, indicios que puedan significar riesgos y derivar en amenazas y actividades [3] que faciliten medidas para mejorar la toma de decisiones.
- **La *organización* que realiza esta tarea**. La inteligencia como organización se refiere a los organismos y unidades que realizan las anteriores actividades de transformar la información en inteligencia y la protegen.
- **El *proceso* mediante el que se lleva a cabo**. La inteligencia como proceso comprende los procedimientos y medios que se utilizan para definir las necesidades de los decisores, establecer la búsqueda de información, su

obtención, valoración, análisis, integración e interpretación hasta convertirla en inteligencia, y su difusión a los usuarios.

Existen diferentes **disciplinas de intelligence gathering o adquisición de información**; las más habituales son:

- **HUMINT (Human Intelligence),** proporcionada directamente por personas.
- **GEOINT (Geospatial Intelligence).** generada a partir de los datos proporcionados por satélites, mapas, etc.
- **MASINT (Measurement and Signature Intelligence),** obtenida a partir del análisis de datos de medidas y señales.
- **OSINT (Open Source Intelligence)** es un concepto muy utilizado en ciberseguridad, además de en otras muchas disciplinas relacionadas con la adquisición de información. El concepto se refiere a la **recolección de información de cualquier objetivo utilizando fuentes de acceso público o semipúblico** (redes sociales, blogs, foros, conferencias, metadatos, etc.).

Capacidad de respuesta ante incidentes

- **SIGINT (Signals Intelligence),** generada a partir de la interceptación de señales.
- **TECHINT (Technical Intelligence),** obtenida a partir del análisis de armas o equipamiento de un tercero.

Tras haber obtenido, a través de cualquiera de estas disciplinas los datos requeridos, se procede al análisis de los mismos. En los últimos cincuenta años la adquisición SIGINT se ha convertido en la principal fuente de generación de inteligencia ya que las tecnologías son un componente fundamental para el procesamiento de nuestra información.

En el caso de la ciber inteligencia, ésta puede nutrirse de cualquiera de las disciplinas de adquisición de datos indicadas previamente; en general, la adquisición será una combinación del trabajo de fuentes humanas (HUMINT), la interceptación de comunicaciones (SIGINT), el análisis de artefactos o piezas de malware utilizados por un atacante (TECHINT), y el análisis de fuentes abiertas (OSINT) que nos pueden proporcionar datos útiles sobre riesgos potenciales para nuestra organización.

Capacidad de respuesta ante incidentes

La inteligencia y la ciber inteligencia -**según la necesidad de información** que satisface-puede ser:

- **Inteligencia básica.** Es la que se produce para satisfacer los requerimientos de inteligencia permanentes y generales de la organización de que se trate. Se elabora atendiendo a los objetivos estratégicos de la organización.
- **Inteligencia actual.** Es la que tiene como fin satisfacer los requerimientos de inteligencia puntuales y concretos de una organización. Presenta el estado de una situación o de un acontecimiento en un momento dado y puede señalar opciones de evolución en un corto plazo, así como indicios de riesgos inmediatos.

  Los productos de la inteligencia actual suelen adoptar la forma de informes específicos para atender una demanda concreta y actual de información; o la de informes breves y periódicos, sobre cuestiones sobre las que los decisores desean mantener un conocimiento permanente. Un caso particular de la inteligencia actual es el de inteligencia critica, que es la que se elabora para satisfacer los requerimientos informativos que se producen durante la gestión

de una crisis. Los productos más habituales durante la gestión de crisis son alertas e informes de situación sobre la evolución de los acontecimientos.

De acuerdo con la finalidad de la inteligencia, podemos hablar de tres tipos de inteligencia:

- **Inteligencia estratégica**. Se halla ***muy vinculada a la prevención y a la prospectiva, advirtiendo de amenazas a los intereses de la seguridad ciberseguridad y de las oportunidades***. En el plano cibernético, un ejemplo de inteligencia estratégica seria por ejemplo la información detallada sobre el tipo de atacantes que puede tener interés en la organización para definir así un perfil de riesgo y diseñar una estrategia de defensa; ¿Qué grupos APT operan en el país donde está ubicada la organización? ¿Qué grupos de adversarios tienen interés en el sector en el que se engloban los servicios que proporciona la compañía?, etc.
- **Inteligencia táctica.** Es la que **se elabora para contribuir a la planificación y el diseño de las acciones concretas que permitan alcanzar un objetivo de alcance limitado**, subordinado a los grandes objetivos de la inteligencia estratégica. Este

tipo de inteligencia se centra en el futuro inmediato. Un ejemplo de este tipo de inteligencia en el plano cibernético serían los Indicadores de Compromiso (IOC) sobre incidentes de los que se tiene constancia.

- **Inteligencia operativa.** Es la que **se elabora para permitir la organización y ejecución de acciones para el cumplimiento de una misión**, entendiendo por esta la que le es encomendada a un oficial de inteligencia, solo o dirigiendo un grupo, para lograr un propósito determinado. Este tipo de inteligencia protege a la organización previniendo contra peligros concretos. Aunque puede parecer similar a lo que hace la Ciber inteligencia estratégica, esta analiza el riesgo a una escala mucho mayor amenazas a nivel mundial). Por el contrario, la operativa se concentra en el entorno inmediato de la organización.“

Muchos **CSIRT/SOC/CERT** cuentan con apoyo de unidades de Ciber inteligencia, bien sean internas de la organización o externas, que proporcionan información de interés para la establecer la estrategia de ciberdefensa de la organización Entre los **servicios que puede ofrecer una Unidad de Ciber inteligenci**a se encuentran

Capacidad de respuesta ante incidentes

- **Difusión de Ciber inteligencia a través de feeds, informes, alertas, etc.,** bien sea ciber inteligencia básica, actual, estratégica, operativa, táctica, etc. con lo que es posible que se generen desde informes periódicos hasta informes bajo demanda atendiendo al apoyo en algún tipo de situación de crisis.
- **Modelado de ciber amenazas.** El objetivo es obtener las diferentes TTP que puede utilizar un adversario para poder definir una estrategia de defensa. Estudio de familias de malware, grupos APT que puedan tener entre sus objetivos la organización.
- **Vigilancia Digital.** Una de las funciones de este servicio es el de identificar amenazas digitales que puedan afectar a la ciberseguridad de la organización o a su imagen corporativa.
  - *Prevención de fraude* identificando estafas que puedan afectar a la organización incluso haciendo algún tipo de abuso de marca (uso no autorizado de marca, imagen corporativa, etc.). • Control del registro de dominios no legítimos que pudiesen estar vinculados a la organización Cybersquatting).

Capacidad de respuesta ante incidentes

- *Leaks de información.* Localización de información de la compañía como por ejemplo bases de datos de usuarios, documentación interna, etc. publicada en sitios públicos o de la Deep Web/ Dark Web.
- *Monitorización de markets de aplicaciones móviles en busca de aplicaciones falsas vinculadas a la organización*.
- *Seguimiento de grupos hacktivistas* que pudieran tener como objetivo la compañía.
- *Estudio reputacional de la marca de la organización o de los perfiles VIP:* qué se dice sobre, en qué forma se dice, si es información falsa, etc.

- **Huella digital.** Control de la información no autorizada que tiene Internet de la organización o de sus empleados.