AGRADECIMIENTOS

A Toni Villalón por su guía durante la elaboración de este libro y, sobre todo, por ayudarme a crecer personal y profesionalmente a lo largo de todos estos años. Gracias por ser un líder y no un jefe, eres una inspiración.

A Pepe Rosell y Miguel Juan por la confianza depositada en mí, y por todas las oportunidades brindadas, ¡y las que están por venir!

A Jose Vila, Adrián Capdevila y a Antonio Sanz, compañeros de trincheras y por supuesto amigos, por su paciencia, dedicación y todos los conocimientos compartidos.

A mi marido, mi compañero de vida, por su inestimable apoyo en todos los proyectos que emprendo.

A mis padres, por cada segundo vivido.

A los *errantes*, por ser siempre un refugio de ilusión, donde el *hacking* aún sigue vivo.

A todos los compañeros de S2 Grupo, por todo lo que vivimos a diario, por la ilusión compartida.

A todos los clientes que me han permitido ayudarles, y a todos los compañeros del sector con los que he tenido la suerte de compartir algún proyecto, reunión, congreso, conversación, etc., porque de todos he podido aprender algo.

ACERCA DE LA AUTORA

Maite Moreno es Analista de Inteligencia y Ciberseguridad en la compañía S2 Grupo, donde ha desarrollado casi toda su carrera profesional con más de una década dedicada a la gestión de incidentes de ciberseguridad, inteligencia de amenazas y coordinación de equipos en SOC/CSIRT/CERT de ámbito público y privado.

Además de esta labor, ha colaborado con el Foro Nacional de Ciberseguridad (Departamento de Seguridad Nacional) en el grupo de trabajo "*Formación, capacitación y talento en ciberseguridad*", forma parte de los foros nacionales CSIRT.es y la Red Nacional de SOCs y es miembro de los foros internacionales FIRST y TF-CSIRT.

La autora está ligada al mundo universitario, donde ha impartido seminarios en diversos másteres de la Universidad Politécnica de Valencia y la Universidad de Alicante. En la actualidad, forma parte del profesorado del máster en ciberseguridad "*Red Team, Blue Team*" que oferta la Universidad Autónoma de Madrid y codirige ENIGMA, el programa de becas de ciberseguridad de S2 Grupo, un programa formativo de alto rendimiento dirigido a universitarios y estudiantes de Ciclos Superiores de Formación Profesional.

Maite dispone de varias publicaciones y colaboraciones que principalmente pueden ser consultadas en los blogs de S2 Grupo, "Security Art Work"[1] y el blog de Lab52[2] –la división de *Threat Intelligence* de S2 Grupo–, y ha participado como ponente en congresos especializados en ciberseguridad como las Jornadas STIC que organiza el CCN-CERT (Centro Criptológico Nacional), C1b3rwall que organiza la Policía Nacional o Securmática, organizado por la revista SIC.

1 https://www.securityartwork.es/

2 https://lab52.io/blog/

PRÓLOGO

Nunca he prologado un libro. Por eso, cuando Maite me propuso prologar este, le contesté que no sabría muy bien por donde empezar. Pero la respuesta era obvia: por el prólogo, ¿no? Así que manos a la obra. ¿Qué decir de un libro sobre gestión de incidentes, o qué decir sobre la gestión de incidentes en sí misma? Podríamos hablar de las metodologías de gestión, de la importancia de las lecciones aprendidas o del apasionante formato de STIX. Pero todo esto ya lo hace muy bien Maite en este libro, así que, ¿qué puede aportar un simple prólogo en estos ámbitos? Absolutamente nada. Por eso en estas líneas no voy a hablar de ninguno de estos temas, sino de los incidentes y de lo que implican personalmente para quienes los gestionamos.

En primer lugar, obvia decir que un incidente no es algo agradable ni una situación que deseemos para nadie. Un incidente es algo (no entraremos en la definición formal que ya se encarga Maite de presentar en este libro) estresante, que causa mucho daño a una víctima y que al equipo que debe gestionarlo le altera su rutina de trabajo diaria, con lo que tiene impacto para todos los involucrados salvo para el actor hostil, si existe. Dicho de otra forma: nadie quiere tener un incidente de ningún tipo. Si pudiéramos evitarlo, lo haríamos. Si pudiéramos planificarlo, lo haríamos. Pero no podemos, y seguramente antes o después lo suframos en primera persona.

Dicho esto, creo toca ver la parte positiva: la gestión de incidentes no sólo es una simple disciplina dentro de eso que hoy llamamos ciberseguridad, sino que es quizás la más necesaria. Y es la más necesaria porque antes o después tendremos un incidente y tendremos que saber cómo responder. Y como se dice en este libro, ese "saber cómo responder" no puede esperar a que el incidente suceda: hay que prepararse antes. Mucho antes, cuando tenemos la posibilidad de sentarnos delante

de un folio en blanco y empezar a pensar y diseñar qué haremos para responder. Desde luego, cuando el incidente se materializa, no estamos en esta situación.

Más allá de su necesidad, la gestión de incidentes es una disciplina apasionante. Un incidente enseña mucho no sólo del ámbito tecnológico, que también, sino de otros igual de importantes, como el geopolítico o el económico. Nos hace ver las problemáticas de diferentes víctimas, nos ayuda a ponernos en la piel de organizaciones atacadas a las que alguien, por algún motivo, les ha hecho daño. Un incidente nos enseña a conocer a los actores hostiles, sus formas de trabajo, sus intereses, sus necesidades, etc., y a darnos cuenta de que en ocasiones los *malos* no son tan malos ni los *buenos* son tan buenos.

Pero aparte del interés puramente objetivo de la gestión de incidentes, y quizás esto sea lo más importante, un incidente nos enseña mucho de las personas con las que colaboramos para resolverlo: pasar días (y noches) juntos, trabajando codo con codo en largas jornadas, muchas veces lejos de casa, convierte a los que hasta ese momento *sólo* eran compañeros de trabajo en compañeros de trinchera, en amigos. Basta un incidente serio (un compromiso por APT, un ransomware operado con alto impacto, etc.) para identificar a esas personas de las que uno se puede fiar ciegamente y con las que puede contar para todo, en lo profesional y en lo personal.

Si es que alguien ha llegado hasta aquí, no pretendo aburrir más al lector. Si me permiten un consejo, expriman este libro y prepárense para el día en que tengan un incidente de seguridad. Cuando llegue el momento, tengan a mano este libro y café, e intenten hacerlo lo mejor posible. Y aprendan, sobre todo aprendan, porque volverán a tener un incidente.

Como no podía ser de otra forma, no podía acabar sin dar las gracias a Maite no sólo por el trabajo desarrollado en este libro y por permitirme prologarlo, sino especialmente por su trabajo diario en S2 Grupo… y por los incidentes gestionados durante todos estos años. Y por muchos más.

Antonio Villalón Huerta
Director de Seguridad, S2 Grupo

PREFACIO

La información y los sistemas que la tratan son recursos muy valiosos para las organizaciones, sin los cuales el desarrollo de sus actividades se vería muy mermado. Cualquier incidente de seguridad sobre dichos sistemas podría provocar daños irreparables en la organización, sobre todo si afecta a su información corporativa o a los sistemas que la alojan (fugas de datos, accesos no autorizados a la información, denegación de servicios, etc.).

Todas las organizaciones y empresas, estén vinculadas o no a las tecnologías digitales, son susceptibles de sufrir las consecuencias de incidentes de ciberseguridad que afectan a los sistemas de información, bien por ser víctimas directas o bien porque los sufra algún tercero vinculado. Este hecho provoca que sea necesario dotar a las organizaciones de una capacidad de gestión de incidentes de ciberseguridad que les permita dar una respuesta correcta, ágil y proporcional con el objetivo de minimizar el impacto y la frecuencia de dichos incidentes.

El **objeto del presente libro** es definir las directrices necesarias para establecer en los lectores una capacidad de gestión ante incidentes de ciberseguridad, contemplando todas las fases del ciclo de vida de esa gestión. Los contenidos, además, han sido adaptados para los requeridos en el módulo profesional 5021 "Incidentes de ciberseguridad", que se engloba dentro del ciclo formativo "Curso de Especialización de Ciberseguridad en Entornos de las Tecnologías de la Información"[3] (Título LOE).

Se proporcionará el conocimiento necesario para establecer una capacidad de detección de incidentes implantando los controles, las herramientas y los

3 https://www.todofp.es/en/que-estudiar/loe/informatica-comunicaciones/ciberseguridad-entornos-tecnologias-informacion.html

mecanismos necesarios para su monitorización e identificación. Del mismo modo, se formará al lector en las líneas de actuación necesarias para analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.

Las líneas de actuación que permitirán alcanzar los objetivos previstos versarán, entre otros, sobre:

- Detección de incidentes mediante distintas herramientas de monitorización.
- Implantación de las medidas necesarias para responder a los incidentes detectados.
- Identificación de la normativa nacional e internacional aplicable en la organización.
- Notificación de incidentes tanto interna como externa, si aplica, mediante los procedimientos adecuados.
- Elaboración de planes de prevención y concienciación de ciberseguridad.

La estructura del libro se divide en dos bloques principales. Un primer bloque, que contempla los tres primeros capítulos, focalizados en explicar **qué es un incidente de seguridad**, qué **tipos** hay, y cómo deben capacitarse las organizaciones para poder enfrentarse a su gestión. Se estudiará por tanto qué es la **capacidad de respuesta ante incidentes**, cómo funciona un equipo de respuesta ante incidentes, y cuáles son los diferentes actores que conforman la **Organización de la Seguridad**[4] en una compañía, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.

El segundo bloque del libro comienza en el capítulo cuatro, en el que se explica cuál es el **ciclo de vida de la gestión de un incidente**, diferenciando cuatro grandes etapas: planificación, detección, respuesta y lecciones aprendidas.

Para cada una de estas etapas se ha dedicado un capítulo; así, en el capítulo cinco se estudian las tareas que tienen lugar en la **etapa de planificación**. Esto incluye las acciones previas que es necesario hacer para estar preparado ante un incidente de seguridad: elaborar procedimientos, establecer relaciones de confianza con terceros de interés, entrenar al equipo de respuesta ante incidentes, concienciar a

4 Establecer un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

los empleados en materia de ciberseguridad y, entre otros, monitorizar todas aquellas fuentes de datos que nos ayudarán a detectar cualquier tipo de situación que pueda desencadenar un incidente de seguridad.

En el capítulo seis, se continúa el ciclo de vida de gestión de incidentes con la etapa de **detección y valoración del incidente**, capítulo en el que se explica cómo los analistas gestionan aquellos eventos procedentes de la plataforma de monitorización, que señalan que posiblemente se está ante un incidente de seguridad.

El capítulo siete, que corresponde a la etapa más activa dentro del ciclo de vida de gestión de incidentes, **la etapa de respuesta**, se centra en explicar cómo se debe contener y erradicar un incidente de seguridad, así como qué se debe tener en cuenta para recuperar la normalidad tras el incidente. El ciclo sería cerrado en el capítulo ocho, donde una vez se ha erradicado el incidente y vuelto a la normalidad, se debe hacer un ejercicio de retrospectiva en el que se determine si se ha hecho una gestión del incidente de manera óptima o se han encontrado puntos de mejora: las llamadas lecciones aprendidas. El capítulo nueve contempla **ejemplos** sobre como se deberían tratar varios tipos de incidentes en su ciclo completo, para poner en práctica todo lo aprendido en capítulos anteriores.

Todo lo que no se puede medir no se puede mejorar y, es por esto que en el último capítulo del libro se dan unas directrices básicas sobre qué **métricas** se deben tener en cuenta para mejorar la gestión de incidentes se seguridad en nuestro ámbito.

Con esta visión tanto teórica como práctica, el lector conocerá las bases tanto de la detección de incidentes, como de su análisis y respuesta, dotándole de las herramientas básicas para iniciarse en el mundo profesional de la gestión de incidentes de ciberseguridad.

1

QUÉ ES UN INCIDENTE DE SEGURIDAD

Son diferentes las definiciones que se pueden encontrar al respecto.

De acuerdo con la normativa ISO 27001[5] [1] un incidente de seguridad de la información sería:

"Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información".

De forma más simplificada, INCIBE[6] define un incidente de ciberseguridad como

"Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa".

Es interesante matizar que los términos "suceso" y "evento" son sinónimos y se podrían definir como [9]:

---

5 Las normas ISO son un conjunto de estándares con reconocimiento internacional que especifican requerimientos que pueden ser empleados en organizaciones para garantizar que los servicios y productos ofrecidos cumplen con su objetivo. Una de las normas ISO más importante es la ISO 27001 que versa sobre la Seguridad de la Información que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

6 INCIBE es el Instituto Nacional de Ciberseguridad dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

- **Suceso**: ocurrencia o cambio de un conjunto particular de circunstancias [UNE Guía 73:2010].
- **Suceso de seguridad de la información**: ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad [UNE-ISO/IEC 27000:2014].
- **Evento**: (Operación del Servicio) un cambio de estado significativo para la cuestión de un elemento de configuración o un servicio de TI[7]. El término "evento" también se usa como alerta o notificación creada por un servicio de TI, elemento de configuración o herramienta de monitorización. Los eventos requieren normalmente que el personal de operaciones de TI tome acciones, y a menudo conllevan el registro de Incidentes. [ITIL:2007][8]

Se debe tener presente pues que un evento de seguridad de la información se refiere a algo que puede afectar a los niveles de riesgo, sin afectar de forma necesaria al negocio o a la información. Sin embargo, un incidente de seguridad de la información se refiere a algo que afecta de forma negativa tanto a los procesos del negocio como a la información [2].

- Algunos ejemplos de incidentes de ciberseguridad serían los siguientes:
- Accesos no autorizados a información corporativa (intrusiones, Amenazas Persistentes Avanzadas[9] [3], etc.).
- Código dañino en los sistemas corporativos (gusanos, troyanos, virus, *ransomware*, *rootkits*, *backdoors* (RAT[10]), *downloaders*, etc.).

---

7 TI equivale a las siglas de Tecnologías de la Información. También es posible encontrar IT, por sus siglas en inglés Information Technology.

8 ITIL equivale a las siglas Information Technology Infraestructure Library. Es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma.

9 Amenazas Persistentes Avanzadas o APT por sus siglas en inglés (Advanced Persistent Threat) son una serie de amenazas con altas capacidades, habitualmente bien financiadas y que suelen ser orquestadas por grupos organizados con una avanzada capacidad de ataque. Sus objetivos son muy dirigidos y suelen estar relacionados con el ciberespionaje de alto nivel. Para más información se recomienda la lectura del libro "Amenazas Persistentes Avanzadas" de Antonio Villalón citado en la bibliografía.

10 RAT equivale a las siglas en inglés Remote Access Tool.

- Código no autorizado en los sistemas corporativos (por ejemplo, *software* pirata).
- Ataques remotos (denegación de servicio, reconocimiento activo del perímetro, etc.).
- Ataques a los contenidos (*Defacement*[11], distribución de contenido fraudulento o malicioso, etc.).

Es habitual encontrar a diario en prensa noticias sobre incidentes de ciberseguridad que comprometen las actividades de las organizaciones o los datos de los ciudadanos, como los prolíficos ataques por *ransomware* (secuestro de información a cambio de beneficio económico), ataques de denegación de servicio, ataques a cadena de suministro (*Supply Chain Attack*), ciberespionaje, campañas de *phishing,* etc. Y es que, existe una gran variedad de ciberamenazas por las que un actor hostil puede alcanzar sus objetivos o motivaciones:

- Ciberespionaje (robo de información en beneficio propio o de un tercero como un Estado u organización).
- Ciberdelito (beneficio económico, daño reputacional, etc.).
- Ciberterrorismo (provocación de daños en el plano físico, ataques a infraestructuras críticas, etc.).
- Ciberactivismo (reivindicación ideológica, protesta, etc.).
- Ciberguerra (superioridad en el ciberespacio…).[12]

No obstante, los incidentes de ciberseguridad no siempre son causados por atacantes, sino que pueden estar asociados a accidentes o errores no intencionados. En cualquier caso, deben ser gestionados de la forma más idónea posible, esto es, minimizando al máximo su impacto, restaurando los niveles de operación lo antes posible y previniendo, en la medida de lo posible, la ocurrencia de los mismos.

---

11 El Defacement es un tipo de ataque que se realiza contra un sitio web, en el que se modifica la apariencia de alguna de sus páginas, para llevar a cabo algún tipo de accion fraudulenta o vandalismo. https://www.incibe.es/aprendeciberseguridad/defacement

12 No cabe duda de que, durante los últimos años, el número de operaciones en el ciberespacio con una motivación política ha ido en aumento. Desde la II Guerra Mundial no ha habido un conflicto bélico entre dos naciones del primer mundo. Esto evidencia cómo las grandes naciones han trasladado el choque de intereses a metodologías menos clásicas, como puede ser la utilización de guerras subsidiarias, la guerra comercial y, desde hace algunos años, la ciberguerra.
Para ampliar esta información se recomienda la lectura del libro "*Omnium contra Omnes: Análisis político-militar de la guerra en el ciberespacio"* referenciado en la bibliografía [4].

1.1 NORMATIVA DE REFERENCIA

En este apartado se citan los estándares más utilizados actualmente en gestión de incidentes de ciberseguridad, tanto a nivel nacional como internacional.

ISO 27035

La familia de normas relativas a la gestión de la seguridad de la información por excelencia es la norma ISO 27000 y dentro de ella, el estándar definido en gestión de incidentes de seguridad de la información es la norma ISO 27035, publicada en 2011 [5]. Se trata de la estandarización del informe técnico ISO/IEC TR 18044, publicado en 2004, el cual define los objetivos a cumplir en la gestión de incidentes de seguridad y como llegar a alcanzarlos en todo su ciclo de vida.

Los objetivos que marca la norma ISO 27035, de aplicación en cualquier ámbito a la hora de llevar a cabo la gestión de incidentes de seguridad, se pueden resumir en:

- Detección y gestión de los eventos de seguridad que se produzcan determinando si corresponden o no a un incidente.
- Respuesta a los incidentes de forma proporcional, ágil y adecuada de manera que se minimice el impacto asociado a los incidentes acontecidos.
- Extracción de lecciones aprendidas a partir de los incidentes gestionados de forma que se mejore el estado global de la seguridad corporativa, incluyendo la optimización de los procedimientos de gestión de incidentes.

NIST

NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*), organismo dependiente del Departamento de Comercio de Estados Unidos.

Como resultado de la creciente cantidad de ciberataques a sistemas de infraestructuras críticas y al impacto que dichos ataques pudieran tener en el contexto de la seguridad nacional de Estados Unidos, el 12 de febrero de 2013 el Presidente Barack Obama redactó la Orden Ejecutiva (EO) de Mejora de Ciberseguridad de Infraestructuras Críticas (*Executive Order 13636 – Improving Critical Infrastructure Cybersecurity*) en donde se delegaba en el NIST el desarrollo de un marco de trabajo para la reducción de riesgos asociados con este tipo de entornos, con el soporte del Gobierno, la industria y los usuarios.[13]

13 https://blog.isecauditors.com/2016/12/guia-rapida-para-entender-marco-trabajo-de-ciberseguridad-del-NIST.html

Algunos de los requerimientos NIST CSF fueron:

- Identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica.
- Proporcionar un enfoque prioritario, flexible, repetible, basado en el rendimiento y rentabilidad.
- Ayudar a identificar, evaluar y gestionar el riesgo cibernético.
- Incluir orientación para medir el desempeño de la implementación del Marco de Ciberseguridad.
- Identificar áreas de mejora que deben abordarse a través de la colaboración futura con sectores particulares y organizaciones que desarrollan estándares.

A raíz de este trabajo, NIST ofrece un conjunto de documentos de libre descarga, la serie NIST SP 800, que describe las políticas de seguridad informática, procedimientos y directrices que proporcionan información que cubre tanto la gestión como las prácticas operativas de seguridad de la información.

Con respecto a las acciones de respuesta a incidentes de ciberseguridad, NIST cuenta con una guía especializada [6] dentro de esta serie, denominada "*Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Techology (SP 800-61)*" que pretende ayudar a las organizaciones a obtener la capacidad de respuesta ante incidentes necesaria, así como dar una serie de directrices y pautas para llevar a cabo una completa gestión de un incidente de seguridad.

ENS

En España, el Esquema Nacional de Seguridad (ENS) es una normativa que aplica al sector público y puede servir de orientación al sector privado, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información. Tal y como recoge el Real Decreto 3/2010.[14]:

14 El Esquema Nacional de Seguridad está recogido en el Real Decreto 3/2010, que desarrolla lo previsto en el artículo 42 de la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos. El RD 3/2010 fue modificado a su vez por el Real Decreto 951/2015, hasta ofrecer el texto consolidado actual, que podemos leer en la publicación electrónica del BOE. [7]

"La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios…",

En las decisiones en materia de ciberseguridad, de acuerdo con el ENS, se contemplan los siguientes principios básicos [8]:

- La seguridad se entenderá como un **proceso integral** constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.
- El análisis y **gestión de riesgos** será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- **Prevención, reacción y recuperación**. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.
- **Líneas de defensa**. El sistema ha de disponer de una estrategia de protección formada por múltiples capas de seguridad. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.
- **Reevaluación periódica**. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
- **La seguridad como función diferenciada**. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

El Centro Criptológico Nacional (CCN)[15] es el encargado de la difusión de guías específicas [9] para el mejor cumplimiento del ENS y ofrece una serie de

15 El Centro Criptológico Nacional (CCN) es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.
El CCN fue creado en el año 2004, a través del Real Decreto 421/2004, adscrito al Centro Nacional de Inteligencia (CNI). De hecho, en la Ley 11/2002, de 6 de mayo, reguladora del CNI, se encomienda a dicho Centro el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información y de protección de la información clasificada, a la vez que se confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional. Por ello, el CCN comparte con el CNI medios, procedimientos, normativa y recursos. (Fuente: cni.es)

directrices para la gestión de incidentes, que engloban aspectos como la clasificación (taxonomía) de los incidentes, su peligrosidad, su impacto, e incluso por qué es necesario notificar un incidente o cuáles son los incidentes de obligada notificación.

Uno de los principales documentos relacionado con estas directrices es la Guía de Seguridad de las TIC **CCN-STIC 817 "Esquema Nacional de Seguridad. Gestión de ciberincidentes"** [10] publicada por el CCN en abril de 2020. El CCN desarrolla esta guía como respuesta al mandato recogido en el artículo 36 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, que señala [7]:

"El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Response Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN"

El objeto de dicha guía es ayudar al cumplimiento del ENS a través del establecimiento de las capacidades de respuesta ante incidentes y su adecuado tratamiento, dirigiéndose especialmente a equipos de respuesta a incidentes, responsables de seguridad de la información, responsables de sistemas de la información y en general, a gestores del ámbito de la ciberseguridad y administradores de sistemas de información y/o comunicaciones.

Otra guía nacional interesante a mencionar en este epígrafe, y que va alineada con la publicada por el CCN, es la "**Guía Nacional de Notificación y Gestión de Ciberincidentes**" [11] aprobada por el Consejo Nacional de Ciberseguridad[16] el día 21 de febrero de 2020 y que se define como:

16 El Consejo de Ciberseguridad Nacional es el órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, en el marco de la Ley 50/1997, de 27 de noviembre, del Gobierno. El Consejo Nacional de Ciberseguridad, presidido por el secretario de Estado director del Centro Nacional de Inteligencia y director del Centro Criptológico Nacional, se crea por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013.
El Consejo Nacional de Ciberseguridad es el encargado de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilita la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional. (Fuente: ccn.cni.es)

"La referencia estatal respecto a la notificación de ciberincidentes (bien sea la comunicación de carácter obligatoria o potestativa), así como en lo relativo a la demanda de capacidad de respuesta a los incidentes de ciberseguridad.

Asimismo, este documento se consolida como una referencia de mínimos en el que toda entidad, pública o privada, ciudadano u organismo, encuentre un esquema y la orientación precisa acerca de a quién y cómo debe reportar un incidente de ciberseguridad acaecido en el seno de su ámbito de influencia…"

Esta guía remarca que la gestión de incidentes de ciberseguridad, y particularmente la notificación a su autoridad competente o de referencia, constituye un imperativo legal para determinadas organizaciones públicas y privadas de España, tal y como se verá en siguientes puntos de este libro.

Adicionalmente a las guías citadas, mencionar que desde INCIBE-CERT[17] se ha publicado el anexo "**Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía**" [12] que pretende servir de apoyo en las tareas propias de la gestión de incidentes de seguridad y en las particularidades de la comunicación con este organismo si corresponde.

El marco regulador a nivel nacional viene definido tomando como referencia la siguiente normativa, tal y como se indica en la Guía Nacional de Notificación y Gestión de Ciberincidentes:

- De carácter general:
  - Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.
  - Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
  - Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
  - Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

17 INCIBE-CERT es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.
En el caso de la gestión de incidentes que afecten a operadores críticos del sector privado, INCIBE-CERT está operado conjuntamente por INCIBE y OCC, Oficina de Coordinación de Ciberseguridad del Ministerio del Interior. (Fuente: incibe-cert.es)

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Disposición adicional novena. Gestión de incidentes de ciberseguridad que afecten a la red de Internet de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Reglamento de Ejecución (UE) 2018/151 de la Comisión Europea de 30 de enero de 2018 por el que se establecen normas para la aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales.

- De carácter particular al ámbito del sector público:
  - Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
  - Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público.
  - Real Decreto de 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.
  - Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, para las entidades del Sector público de su ámbito de aplicación. Modificado en RD 951/2015.
  - Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad publicada en BOE nº 95 de 18 de abril de 2018.

- De carácter particular al ámbito de las infraestructuras críticas:
  - Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas.
  - Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las Infraestructuras Críticas.
  - Plan Nacional de Protección de Infraestructuras Críticas (PNPIC), aprobado mediante Instrucción núm. 1/2016, de la Secretaría de Estado de Seguridad.
  - Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.
  - Acuerdo Marco de Colaboración en materia de Ciberseguridad entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de

Telecomunicaciones y para la Sociedad de la Información de 21 de octubre de 2015.

- De carácter particular a las redes militares y de defensa:
  - Real Decreto 998/2017, de 24 de noviembre, por el que se desarrolla la estructura orgánica básica del MDEF y modifica el Real Decreto 424/2016, de 11 de noviembre.
  - Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.
  - Orden DEF 166/2015, 21 de enero, que desarrolla la organización básica de las FAS (deroga la Orden Ministerial 10/2013).

1.2 TAXONOMÍA DE LOS INCIDENTES

Puesto que no todos los incidentes poseen las mismas particularidades ni tienen las mismas implicaciones, cada organización debe establecer una taxonomía de los incidentes a gestionar, lo que ayudará posteriormente a su análisis, contención y erradicación.

Crear una taxonomía no es una tarea sencilla. Puede haber diferentes formas de clasificar los incidentes y no siempre es fácil o posible determinar cual es la mejor. Muchas organizaciones a menudo terminan desarrollando su propia taxonomía para uso interno. No obstante, se recomienda adoptar taxonomías inspiradas en las proporcionadas por organismos de referencia, de forma que incluyan un mapeo de las clasificaciones de incidentes con un marco legal.

De acuerdo con la "Guía de Seguridad de las TIC CCN-STIC 817. Esquema Nacional de Seguridad. Gestión de ciberincidentes" [10], son varios los factores a considerar a la hora de establecer criterios de clasificación: tipo de la amenaza (código dañino, intrusiones, fraude, etc.), origen de la amenaza, la categoría de seguridad de los sistemas afectados, el perfil de los usuarios comprometidos, el número y tipología de los sistemas involucrados en el incidente, el impacto que el incidente puede tener en la organización, etc.

ENISA (*European Union Agency for Cybersecurity*)[18] ha publicado varios documentos relacionados con las taxonomías, como son "*ENISA Report: Information sharing and common taxonomies between CSIRTs and Law Enforcement (Dec 2015)",*

18 La ENISA, Agencia de la Unión Europea para la Ciberseguridad, es un centro de conocimientos especializados para la seguridad cibernética en Europa. La ENISA ayuda a la UE y los países que la integran a estar mejor equipados y preparados para prevenir, detectar y dar respuesta a los problemas de seguridad de la información.

"ENISA Report: A good practice guide of using taxonomies in incident prevention and detection (Dec 2016)" o "Reference Incident Classification Taxonomy (Jan 2018)". Este último documento es el que tanto la Guía CCN-STIC 817 como la Guía Nacional de Notificación y Gestión de Ciberincidentes toman como referencia para establecer su propuesta de taxonomía, que viene a resumirse en la siguiente tabla:

CLASIFICACIÓN/TAXONOMÍA DE LOS INCIDENTES		
Clasificación	Tipo de incidente	Descripción
Contenido abusivo	*Spam*	Correo electrónico masivo no solicitado.
	Delito de odio	Contenido difamatorio o discriminatorio. Ej.: ciberacoso, amenazas a colectivos o personas.
	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con la pornografía infantil, apología de la violencia, etc.
Código dañino	Sistema infectado	Sistema comprometido con *malware*.
	Servidor de C&C (*Command and Control*, Mando y Control)[19]	Contacto de los sistemas afectados con servidor de Mando y Control.
	Distribución de *malware* o configuración del mismo	Recurso usado para la distribución de *malware* o bien que aloje ficheros de configuración del mismo.
Information Gathering (Obtención de información)	Escaneo de Redes	Envío de peticiones a un sistema para descubrir información de la tecnología utilizada, servicios ofrecidos, así como de vulnerabilidades que puedan presentar
	Análisis/interceptación de paquetes (*Sniffing*)	Observación y registro del tráfico de red.
	Ingeniería Social	Obtención de información a través de engaño, bulos, etc.

19 Un Servidor de Mando y Control es un equipo que da órdenes a dispositivos infectados con malware y que recibe información de esos dispositivos.

Intento de intrusión	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema mediante la explotación de vulnerabilidades conocidas (habitualmente disponen de un identificador estandarizado denominado CVE[20]).
	Intento de acceso con vulneración de credenciales	Intento de acceso a través de ataques de fuerza bruta, ruptura de contraseñas, etc.
	Ataque desconocido	Ataque empleando un *exploit*[21] desconocido
Intrusión	Compromiso de cuenta con/sin privilegios	Compromiso de un sistema en el que atacante puede haber adquirido una cuenta con privilegios (Ej.: cuenta de Administrador) o sin ellos.
	Compromiso de aplicaciones	Compromiso de una aplicación a través de la explotación de vulnerabilidades de *software*. Ej.: inyección SQL, inyección remota de código, etc.
	Intrusión física	Por ejemplo, acceso no autorizado al Centro de Proceso de Datos (CPD).
Disponibilidad	Denegación de Servicio (DoS) o Denegación Distribuida de servicio (DDoS)	Ataque que afecta a la disponibilidad de los sistemas.
	Mala configuración	Una configuración incorrecta del *software* que pueda provocar una caída de un determinado servicio.
	Sabotaje	Sabotaje físico. Ej.: corte de cables, incendios provocados.
	Interrupciones	Perdida de disponibilidad por causas ajenas no intencionadas. Ej.: un desastre natural.
Compromiso de la información	Acceso no autorizado a la información	Ej.: robo de credenciales de acceso mediante interceptación de tráfico o el acceso a documentación en papel.
	Modificación no autorizada de información	Ej.: modificación por un atacante de una entrada en una base de datos.
	Pérdida de datos	Ej.: por fallo de disco duro o robo físico.

Fraude	Uso no autorizado de recursos	Uso de recursos corporativos para fines inadecuados.
	Derechos de autor	Ofrecimiento o instalación de *software* carente de licencia o protegido por derechos de autor.
	Suplantación de identidad	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos. Habitualmente se hace a través de técnicas de ingeniería social[22].
	Phishing	Suplantación de otra entidad a través del correo electrónico con la finalidad de convencer al usuario para que revele sus credenciales.
Por explotación de vulnerabilidades	Criptografía débil, servicios con acceso potencial no deseado, revelación de información, etc.	Servicios que presentan debilidades o malas configuraciones que ponen en riesgo la seguridad de los mismos haciéndolos susceptibles a ataques.
Ataques dirigidos	Amenazas Persistentes Avanzadas (APT) [3]	Ataques dirigidos, sofisticados, con tácticas de anonimato y persistencia avanzadas.
Otros	Otros	Cualquier tipo de incidente que no tenga cabida en ninguna categoría definida

Figura 1.1. Clasificación/Taxonomía de incidentes según la "Guía nacional de notificación y gestión de ciberincidentes", y la "Guía de Seguridad CCN-STIC 817" que toma como referencia las recomendaciones de ENISA.

20 CVE responde a las siglas Common Vulnerabilities and Exposures. Es una lista de información registrada sobre vulnerabilidades de seguridad conocidas identificadas por un código identificativo (CVE-ID) . Se proporciona asimismo una descripción de la vulnerabilidad, que versiones del software están afectadas, posible solución o mitigación del fallo, si existe exploits para dicha vulnerabilidad etc.
Esta lista es mantenida por *The MITRE Corporation*. Mas información en cve.mitre.org

21 Un exploit es una secuencia de instrucciones que se aprovecha de una vulnerabilidad, error o fallo de configuración para inducir un comportamiento no intencionado o imprevisto en un software. Asiduamente suele permitir al atacante acciones como la toma de control del sistema vulnerado, provocar la caída del sistema, perpetrar ataques de denegación de servicio, etc.
Los *exploits* que afectan a vulnerabilidades no conocidas hasta el momento del ataque, se denominan *exploits* de día cero o *0-day exploits* y en ocasiones, su impacto es demoledor puesto que ni los fabricantes ni las organizaciones tienen información inicial sobre su mitigación.

22 La ingeniería social es la práctica de obtener información confidencial o provocar que un usuario realice determinadas acciones a través de la manipulación de los mismos.

En ocasiones, un mismo incidente puede encajar en varias de las categorías propuestas en la relación anterior. La organización deberá por tanto establecer un criterio homogéneo para la clasificación principal de incidentes de seguridad, con independencia de que de manera secundaria cada incidente se asocie a más categorías.

Es importante en este punto hablar de un criterio de referencia fundamental para la gestión de cada incidente, el nivel de Peligrosidad del mismo. Se define el **Nivel de Peligrosidad del incidente** como un indicador que determina la potencial amenaza que supondría un ataque exitoso. Este indicador dependerá de las propias características de la amenaza y su comportamiento. Habitualmente se determinan cinco niveles de peligrosidad que suelen venir asociados a un código de colores:

De acuerdo a la **Guía Nacional de notificación y gestión de ciberincidentes** [11] la correspondencia entre un incidente y su nivel de peligrosidad sería la siguiente:

- NIVEL DE PELIGROSIDAD CRÍTICO:
  - Amenazas Persistentes Avanzadas.

  NIVEL DE PELIGROSIDAD MUY ALTO:
  - Código dañino (Distribución/Configuración de *malware).*
  - Intrusión (Robo de información).
  - Disponibilidad (Sabotaje, interrupciones).
- NIVEL DE PELIGROSIDAD ALTO:
  - Contenido abusivo (Pornografía infantil, contenido sexual o violento inadecuado).
  - Código dañino (Sistema infectado, Servidor de Mando y Control (C&C)).
  - Intrusión (Compromiso de aplicaciones o de cuentas con privilegios).
  - Intento de intrusión.
  - Disponibilidad (Denegación de servicio (DoS), Denegación distribuido de servicio (DDoS)).
  - Compromiso de la información (Acceso no autorizado a la información, modificación no autorizada de información, pérdida de datos).
  - Fraude (*Phishing*).

- NIVEL DE PELIGROSIDAD MEDIO:
  - Contenido abusivo (Discurso de odio).
  - Obtención de información (Ingeniería social).
  - Intento de intrusión (Explotación de vulnerabilidades conocidas, intento de acceso con vulneración de credenciales).
  - Intrusión (Compromiso de cuentas sin privilegios).
  - Disponibilidad (Mala configuración).
  - Fraude (Uso no autorizado de recursos, derechos de autor, suplantación de identidad).
  - Explotación de vulnerabilidades (Criptografía débil, amplificador de ataques DDoS, servicios con acceso potencial no deseado, revelación de información, sistema vulnerable).
- NIVEL DE PELIGROSIDAD BAJO:
  - Contenido abusivo (*Spam*).
  - Obtención de información (Escaneo de redes, análisis de paquetes).
  - Otros.

Es importante también determinar el **nivel de impacto** asociado a un incidente, para ello se tienen en cuenta diferentes parámetros: impacto en la Seguridad Nacional o en la Seguridad Ciudadana, alteración en la prestación de un servicio esencial o en una infraestructura crítica, tipología de la información o sistemas afectados, grado de afectación a las instalaciones de la organización, posible alteración en la prestación del servicio normal de la organización, tiempo y costes propios y ajenos hasta la recuperación post-incidente, pérdidas económicas, daños reputacionales o extensión geográfica afectada.

Los incidentes se asociarán a alguno de los siguientes niveles de impacto:

En [11] se proporciona de forma orientativa los criterios considerados de determinación del nivel de impacto de los ciberincidentes. Algunos ejemplos:

- NIVEL DE IMPACTO CRÍTICO:
  - Afecta apreciablemente a la seguridad nacional o a la seguridad ciudadana con potencial peligro para la vida de las personas.

- Afecta a una infraestructura crítica.
- Afecta a sistemas clasificados SECRETO.
- Afecta a más del 90% de los sistemas de la organización.
- Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios.

- NIVEL DE IMPACTO MUY ALTO:
  - Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
  - Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
  - Afecta a sistemas clasificados RESERVADO.
  - Afecta a un servicio esencial.
  - Daños reputacionales elevados.

- NIVEL DE IMPACTO ALTO:
  - Afecta a más del 50% de los sistemas de la organización.
  - Extensión geográfica superior a tres CC.AA.

- NIVEL DE IMPACTO MEDIO:
  - Afecta a más del 20% de los sistemas de la organización.
  - El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.

Son claros los beneficios de adoptar un sistema de clasificación. Por ejemplo, clasificar correctamente los incidentes permite a los equipos de respuesta asignar la prioridad adecuada a cada uno de ellos, asegurando que se tratan en primer lugar o que se asignan más recursos a aquellos casos más críticos (de acuerdo a su nivel de peligrosidad o impacto).

Un sistema de clasificación definido puede facilitarnos también aspectos como la elaboración de informes, la agregación y búsqueda de datos en los incidentes, o la alimentación de la plataforma de inteligencia de amenazas. Disponer de una taxonomía permite además obtener indicadores más precisos sobre el tipo de incidentes que está sufriendo una organización, lo que podría ayudar al equipo de seguridad a identificar cuales son las principales amenazas que dan lugar a ellos y adoptar medidas paliativas en su conjunto.