GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES

APROBADO POR EL CONSEJO NACIONAL DE CIBERSEGURIDAD EL DÍA 21 DE FEBRERO DE 2020

GOBIERNO DE ESPAÑA

ÍNDICE

1 INTRODUCCIÓN

El Gobierno de España atribuye a diversos organismos de carácter público las competencias en materia de ciberseguridad relativas al conocimiento, gestión y respuesta de incidentes de ciberseguridad acaecidos en las diversas redes de información y comunicación del país.

De forma particular, 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 de España, tienen a su disposición una serie de organismos de referencia, en los cuales se fundamenta la capacidad de respuesta a incidentes de ciberseguridad (CSIRT) del Gobierno de España:

- **CCN-CERT, del Centro Criptológico Nacional del Centro Nacional de Inteligencia**, con un ámbito competencial en el Sector Público general, autonómico y local, y sistemas que manejan información clasificada.

- **INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España**, con un ámbito competencial en la ciudadanía y el sector privado. Asimismo, INCIBE-CERT es el CERT que presta servicios de respuesta a incidentes a las instituciones afiliadas a RedIRIS, la red académica y de investigación 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 y operadores críticos, cuyas capacidades de respuesta técnica se materializan a través de los CSIRT de referencia. Es asimismo autoridad competente para aquellos operadores de servicios esenciales que son además críticos, siendo en ese caso la Oficina de Coordinación Cibernética la responsable de la coordinación en los supuestos previstos en el segundo párrafo del artículo 11.2 del Real Decreto-ley 12/2018.

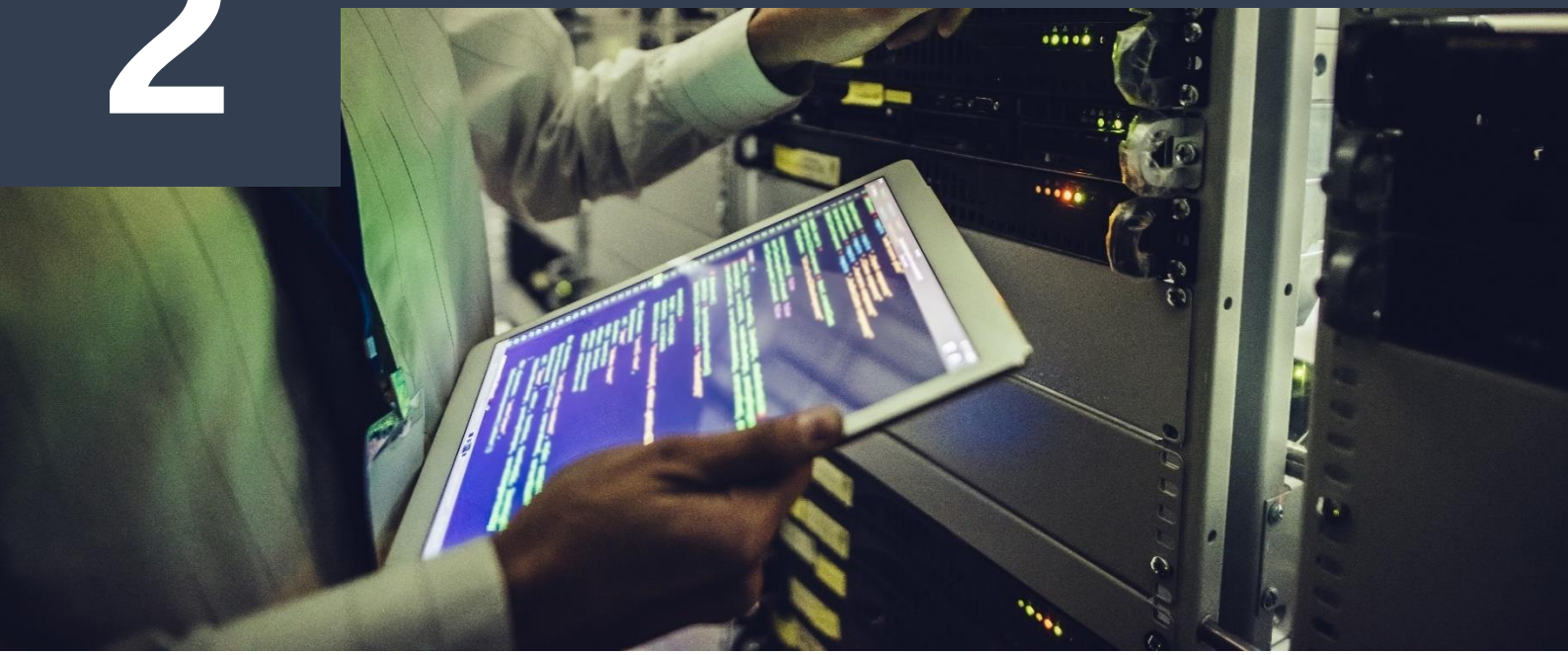
- **ESP-DEF-CERT del Mando Conjunto de Ciberdefensa**, con un ámbito competencial en las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional, apoyando a los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.

La presente Guía nacional de notificación y gestión de ciberincidentes se define como 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 se encuentra alineada con la normativa española, transposiciones europeas, así como documentos emanados de organismos supranacionales que pretenden armonizar la capacidad de respuesta ante incidentes de ciberseguridad.

2 OBJETO DE LA PRESENTE GUÍA



El objeto del presente documento es el de generar un marco de referencia consensuado por parte de los organismos nacionales competentes en el ámbito de la notificación y gestión de incidentes de ciberseguridad. Esto incluye la implantación de una serie de criterios mínimos exigibles y de obligaciones de reporte en aquellos casos que así determine la legislación vigente.

Esta Guía nacional de notificación y gestión de ciberincidentes está especialmente dirigida a:

- Responsables de Seguridad de la Información (RSI), como Responsables Delegados.
- Equipos de respuesta a ciberincidentes y centros de operaciones de ciberseguridad (SOC) internos a las organizaciones.
- CSIRT (*Computer Security Incident Response Team*).
- Administradores de Sistemas de Información y/o Comunicación.
- Personal de Seguridad.
- Personal de apoyo técnico.
- Gestores del ámbito de la ciberseguridad.

La presente guía proporciona a los Responsables de Seguridad de la Información (RSI) las directrices para el cumplimiento de las obligaciones de reporte de incidentes de ciberseguridad acaecidos en el seno de las Administraciones Públicas, las infraestructuras críticas y operadores estratégicos de su competencia, así como el resto de entidades comprendidas en el ámbito de aplicación del Real Decreto-Ley 12/2018. Se expone a continuación un esquema orientativo acerca de autoridades competentes y CSIRT de referencia:

AUTORIDAD COMPETENTE			
Tipo de operador	**Subtipo**	**Características**	**Organismo competente**
Operador de servicios esenciales	Operador Crítico	-	**CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD (CNPIC)**
	No operador crítico	Comprendido en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público	**CENTRO CRIPTOLÓGICO NACIONAL (CCN)**
		Resto	**AUTORIDAD SECTORIAL**
Proveedor de Servicios Digitales	Sector privado	-	**SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL**
	Sector público	Comprendido en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público	**CENTRO CRIPTOLÓGICO NACIONAL (CCN)**

Tabla 1. Autoridad competente

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) DE REFERENCIA		
Tipo de operador	**Características**	Organismo competente
Operador de servicios esenciales	Sector Público (entidades incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015)	**CCN-CERT**
	Sector Privado (entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015)	**INCIBE-CERT**
Proveedor de Servicios Digitales	Sector Público (entidades incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015)	**CCN-CERT**
	Sector Privado (entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015)	**INCIBE-CERT**

Tabla 2. CSIRT de referencia

Asimismo se referencian directrices en el mismo sentido, potestativas para los RSI de las empresas privadas no englobadas en otras ya referenciadas con anterioridad, de sistemas de información y comunicación de instituciones afiliadas a RedIRIS y ciudadanos que a título particular deseen contactar con los organismos competentes.

De este documento emanan los siguientes ítems:

- Taxonomía homogénea en cuanto a clasificación, peligrosidad e impacto de los incidentes de ciberseguridad.

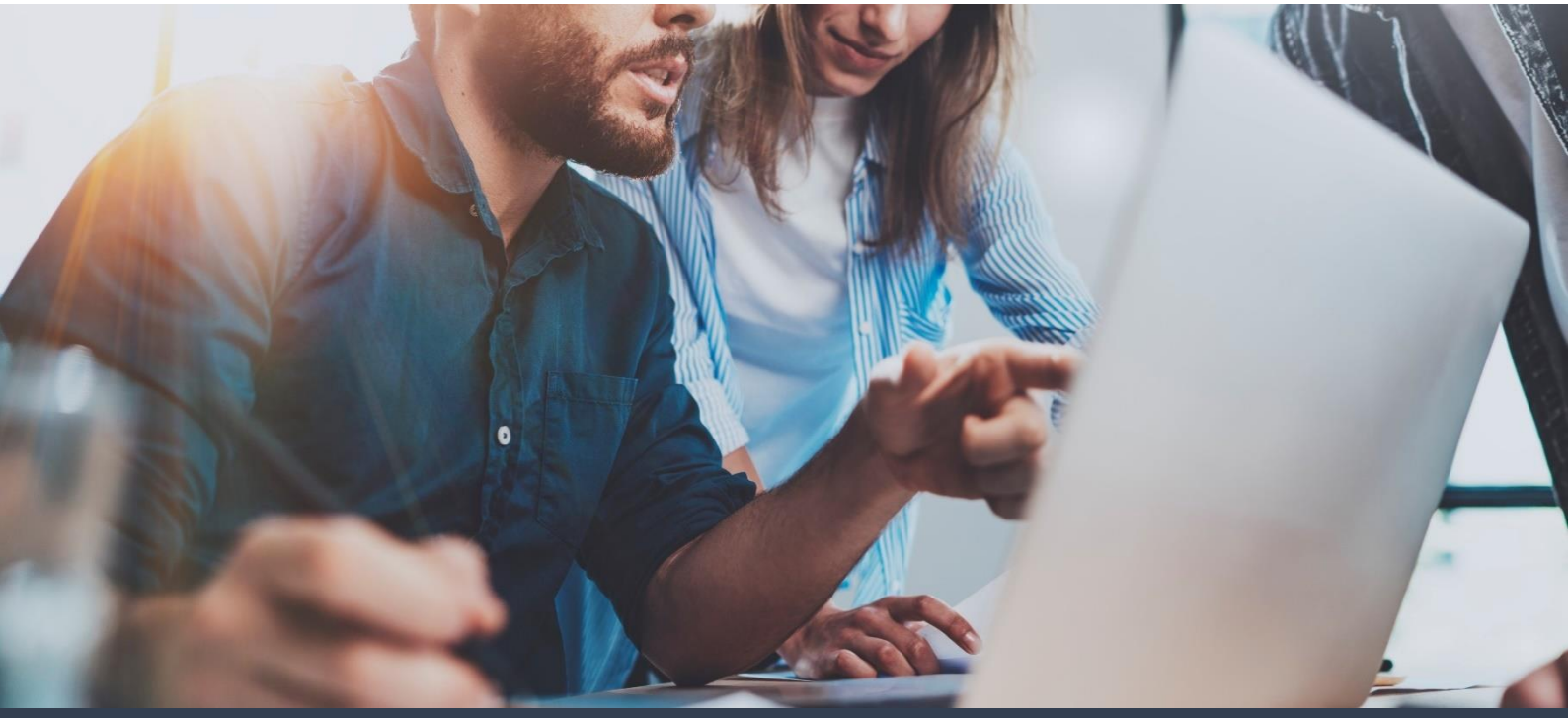
- Especificaciones de las autoridades competentes y CSIRT de referencia a nivel nacional, en materia de conocimiento, gestión y resolución de incidentes de ciberseguridad.

- Definición expresa de los incidentes de ciberseguridad que deben de notificarse a la autoridad competente según establece la legislación vigente y por los canales definidos a tal efecto, en función de la peligrosidad e impacto de los mismos.

- Metodología de notificación y seguimiento de incidentes de ciberseguridad (ventanilla única).

- Requerimientos particulares según la particularidad del afectado, emanados de las autoridades competentes.

Los criterios que se recogen en esta guía atienden a buenas prácticas generalmente reconocidas en la gestión de incidentes y, como tales, pueden servir de referencia en el diseño e implementación de este tipo de servicios en cualquier otro ámbito.



3 ALCANCE

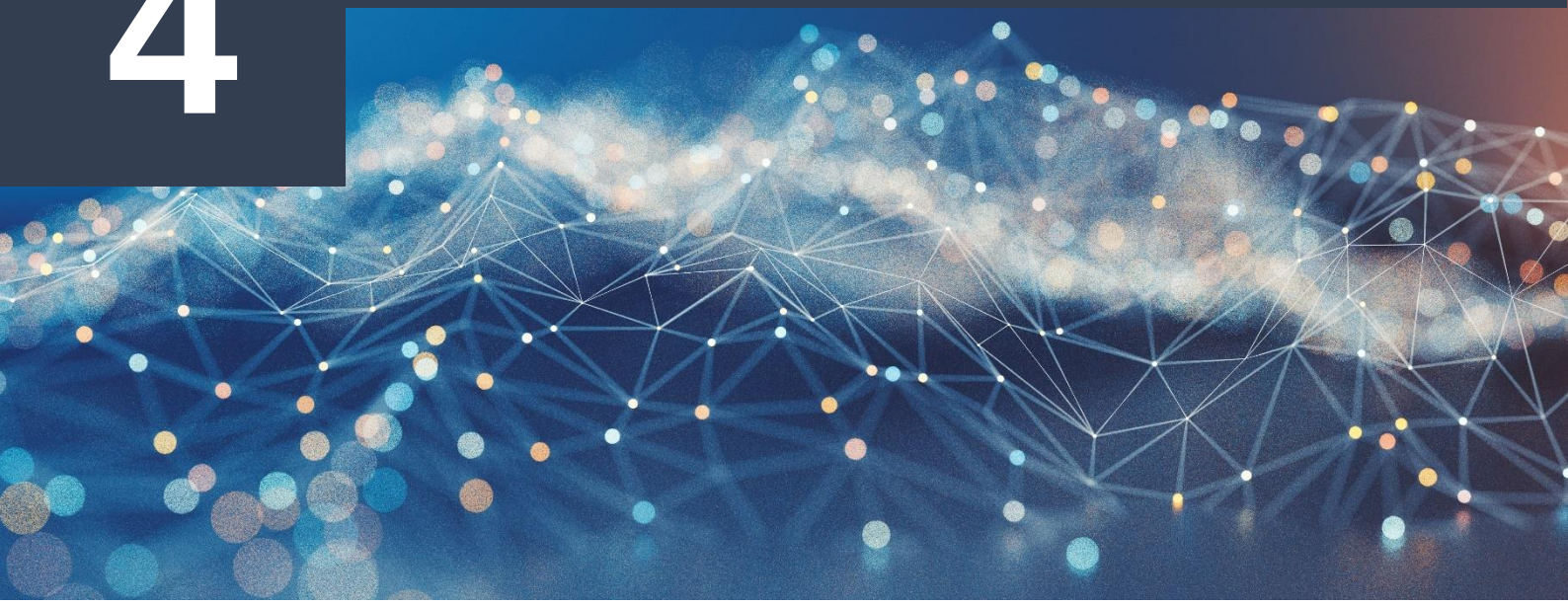
Los organismos públicos o empresas privadas obligadas a notificar un ciberincidente bajo alguna regulación, deberán notificar aquellos ciberincidentes acaecidos en su infraestructura tecnológica que se encuadren dentro del **alcance de la norma**, los **niveles de peligrosidad** y los **niveles de impacto** referenciados en el presente documento. De igual forma podrán reportar otros ciberincidentes o ciberamenazas que consideren oportuno, atendiendo a los siguientes criterios:

- Necesidad o conveniencia para el organismo de contar con el apoyo del CSIRT de referencia para la investigación o resolución de ciberincidentes.

- Beneficios o interés general para la seguridad del conjunto de la comunidad de ciberseguridad, así como para el aumento de la toma de consciencia situacional del estado de la ciberseguridad a nivel estatal por parte de los organismos públicos competentes.

En relación a los ciudadanos y empresas no incluidos en el ámbito de protección de infraestructuras críticas, o del sector público, o del Real Decreto-ley 12/2018, la notificación de incidentes de ciberseguridad tendrá, en todo caso, un carácter potestativo y voluntario. Este público objetivo encontrará en el presente documento una serie de directrices a modo de buenas prácticas.

4 VENTANILLA ÚNICA DE NOTIFICACIÓN



La información solicitada en cada caso, en función de la naturaleza del afectado, deberá ser remitida de acuerdo al cauce establecido por su autoridad competente o CSIRT de referencia. En base a todo ello, la metodología de reporte será la que se expone en el siguiente flujograma:

Ilustración 1. Sistema de ventanilla única

SISTEMA DE VENTANILLA ÚNICA

1. El sujeto afectado enviará un correo electrónico (o ticket) al CSIRT de referencia (INCIBE-CERT o CCN-CERT) notificando el incidente.
2. El CSIRT de referencia, dependiendo del incidente, pone en conocimiento del mismo al organismo receptor implicado o a la autoridad nacional competente.
    - Si afecta a la Defensa Nacional, al CSIRT de referencia ESP-DEF-CERT.
    - Si afecta a una Infraestructura Crítica de la Ley PIC 8/2011, al CNPIC
    - Si afecta al RGPD, a la AEPD.
    - Si es un incidente de AAPP bajo el ENS de peligrosidad ALTA, MUY ALTA o CRÍTICA, al CCN-CERT
    - Si es un incidente de obligado reporte según el RD 12/2018, a la Autoridad Nacional correspondiente:
        - **RGPD**: se remite a la URL del portal de la AEPD.
        - **BDE**: se remite la plantilla de notificación .XLS del BDE.
        - **PIC**: se remite la plantilla de notificación .XLS del CNPIC.
        - **ENS**: se remite la plantilla de notificación .DOC al CCN-CERT.
        - **NIS**: se remite la plantilla de notificación de la Autoridad Nacional competente.
3. El Organismo receptor implicado o Autoridad Nacional competente se pone en contacto con el afectado para recabar información
        - **RGPD**: se remite a la URL del portal de la AEPD.
        - **BDE**: se remite la plantilla de notificación .XLS del BDE.
        - **PIC**: se remite la plantilla de notificación .XLS del CNPIC.
        - **ENS**: se remite la plantilla de notificación .DOC al CCN-CERT.
        - **NIS**: se remite la plantilla de notificación de la Autoridad Nacional competente.
4. El sujeto afectado comunica los datos necesarios al Organismo receptor implicado o Autoridad Nacional competente.
5. Si procede, desde la Oficina de Coordinación Cibernética (CNPIC), se pone la información a disposición de las Fuerzas y Cuerpos de Seguridad del Estado y Ministerio Fiscal para iniciar la investigación policial y judicial (art. 14.3 RD Ley 12/2018).

De acuerdo con el Artículo 11.2 del RD Ley 12/2018, de 7 de septiembre, en los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

4.1. REPORTE DE INCIDENTES A CCN-CERT

Se realizará como canal preferente a través de la aplicación habilitada al efecto: LUCIA[1], y de forma secundaria a través del correo electrónico de gestión de incidentes de ciberseguridad incidentes@ccn-cert.cni.es preferiblemente mediante mensajería cifrada con la clave PGP de este CERT[2].

4.2. REPORTE DE INCIDENTES A INCIBE-CERT

Los ciberincidentes se reportan a INCIBE-CERT a través de un usuario que, como afectado final o identificado como punto de contacto por la entidad afectada, accede al servicio de respuesta a través de los medios proporcionados por este CERT.

Si el reporte se realiza a través de correo electrónico, el buzón de correo genérico para la notificación de incidentes es incidencias@incibe-cert.es.

Como encargado de realizar las funciones de alerta temprana, respuesta preventiva y reactiva de los incidentes de seguridad de la red académica y de investigación española (RedIRIS), el servicio se presta a través de la dirección iris@incibe-cert.es.

Por su parte, los Operadores de servicios esenciales accederán al servicio a través de la cuenta pic@incibe-cert.es u otros mecanismos que facilite INCIBE-CERT. La gestión de estos incidentes a través de INCIBE-CERT está operada conjuntamente entre INCIBE y el CNPIC.

En todos los casos, siempre que la información remitida a INCIBE-CERT se realice por correo electrónico, se enviará preferiblemente cifrada con la clave PGP correspondiente a cada uno de los buzones de este CERT[3].

El reporte a través de correo electrónico es complementario a cualquier otra vía que pudiera ser ofrecida por INCIBE-CERT como pueden ser formularios de contacto, Interfaz de Programación de Aplicaciones (API), portal web, etc.

4.3. REPORTE DE INCIDENTES A ESP-DEF-CERT

El CCN-CERT y el INCIBE-CERT cooperarán con ESP-DEF-CERT, del Ministerio de Defensa, en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional.

La comunicación con ESP-DEF-CERT se realizará por correo electrónico mediante mensajería cifrada con la clave pública PGP. En caso de urgencia, podrá contactarse con el Oficial de Servicio. Los datos concretos para la comunicación se encuentran en el siguiente enlace: http://www.emad.mde.es/CIBERDEFENSA/ESPDEF-CERT/

[1] https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia.html

[2] https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html

[3] https://www.incibe-cert.es/sobre-incibe-cert/claves-publicas-pgp

5 CLASIFICACIÓN/TAXONOMÍA DE LOS CIBERINCIDENTES

Puesto que no todos los ciberincidentes poseen las mismas características ni tienen las mismas implicaciones, se considera necesario disponer de una taxonomía[4] común de los posibles incidentes que se registren, lo que ayudará posteriormente a su análisis, contención y erradicación. La *Tabla 3. Clasificación/Taxonomía de los ciberincidentes* se empleará para la asignación de una clasificación específica a un incidente registrado en las redes y sistemas de información cuando se realice la comunicación a la autoridad competente o CSIRT de referencia.

CLASIFICACIÓN/TAXONOMÍA DE LOS CIBERINCIDENTES		
Clasificación	**Tipo de incidente**	**Descripción y ejemplos prácticos**
Contenido abusivo	Spam	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito de odio	Contenido difamatorio o discriminatorio. Ej: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	Sistema infectado	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit.

[4] https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para distribución de malware. Ej: recurso de una organización empleado para distribuir malware.
	Configuración de malware	Recurso que aloje ficheros de configuración de malware Ej: ataque de webinjects para troyano.
Obtención de información	Escaneo de redes (scanning)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas.
Intento de intrusión	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando exploit desconocido.
Intrusión	Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.

	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej: inyección SQL.
	Robo	Intrusión física. Ej: acceso no autorizado a Centro de Proceso de Datos.
Disponibilidad	DoS (Denegación de servicio)	Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
	Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural.
Compromiso de la información	Acceso no autorizado a información	Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Pérdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.
Fraude	Uso no autorizado de recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez.

	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	Criptografía débil	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
	Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
	Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
	Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Otros	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Tabla 3. Clasificación/Taxonomía de los ciberincidentes

6 NOTIFICACIÓN DE INCIDENTES DE CIBERSEGURIDAD

En este apartado se ofrece la información relativa a la notificación a la autoridad competente o CSIRT de referencia de un incidente de ciberseguridad que sea registrado. Para ello, se incluyen los criterios empleados y las tablas a consultar para asignar los niveles de peligrosidad e impacto correspondientes en cada caso.

6.1. CRITERIOS PARA LA NOTIFICACIÓN

Para la notificación de los incidentes de ciberseguridad se utilizará como criterio de referencia el **Nivel de peligrosidad** que se asigne a un incidente, sin perjuicio de que a lo largo del desarrollo, mitigación o resolución del mismo, se categorice con un determinado **Nivel de impacto** que haga aconsejable la comunicación del incidente a la autoridad competente o CSIRT de referencia.

En todo caso, cuando un determinado suceso pueda asociarse a más de un tipo de incidente contenido en la *Tabla 3. Clasificación/Taxonomía de los ciberincidentes* debido a sus características potenciales, éste se asociará a aquel que tenga un Nivel de peligrosidad superior de acuerdo a los criterios expuestos en este apartado.

6.1.1. Nivel de peligrosidad del ciberincidente

El indicador de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en los sistemas de información o comunicación del ente afectado, así como para los servicios prestados o la continuidad de negocio en caso de haberla. Este indicador se fundamenta en las características intrínsecas a la tipología de amenaza y su comportamiento.

Los incidentes se asociarán a alguno de los siguientes niveles de peligrosidad: **CRÍTICO, MUY ALTO, ALTO**, **MEDIO, BAJO.**

Ilustración 2. Niveles de peligrosidad del ciberincidente

A continuación se incluye la *Tabla 4. Criterios de determinación del nivel de peligrosidad de un ciberincidente.* Mediante la consulta de esta tabla, las entidades notificantes de información podrán asignar un determinado nivel de peligrosidad a un incidente.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES		
Nivel	**Clasificación**	**Tipo de incidente**
CRÍTICO	Otros	APT
MUY ALTO	Código dañino	Distribución de malware
		Configuración de malware
	Intrusión	Robo
	Disponibilidad	Sabotaje
		Interrupciones
ALTO	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Sistema infectado
		Servidor C&C (Mando y Control)
	Intrusión	Compromiso de aplicaciones
		Compromiso de cuentas con privilegios
	Intento de intrusión	Ataque desconocido
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos
	Fraude	Phishing

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
	Vulnerable	Criptografía débil
		Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información
		Sistema vulnerable
BAJO	Contenido abusivo	Spam
	Obtención de información	Escaneo de redes (scanning)
		Análisis de paquetes (sniffing)
	Otros	Otros

Tabla 4. Criterios de determinación del nivel de peligrosidad de un ciberincidente

6.1.2. Nivel de impacto del ciberincidente

El indicador de impacto de un ciberincidente se determinará evaluando las consecuencias que tal ciberincidente ha tenido en las funciones y actividades de la organización afectada, en sus activos o en los individuos afectados. De acuerdo a ello, se tienen en cuenta aspectos como las consecuencias potenciales o materializadas que provoca una determinada amenaza en un sistema de información y/o comunicación, así como en la propia entidad afectada (organismos públicos o privados, y particulares).

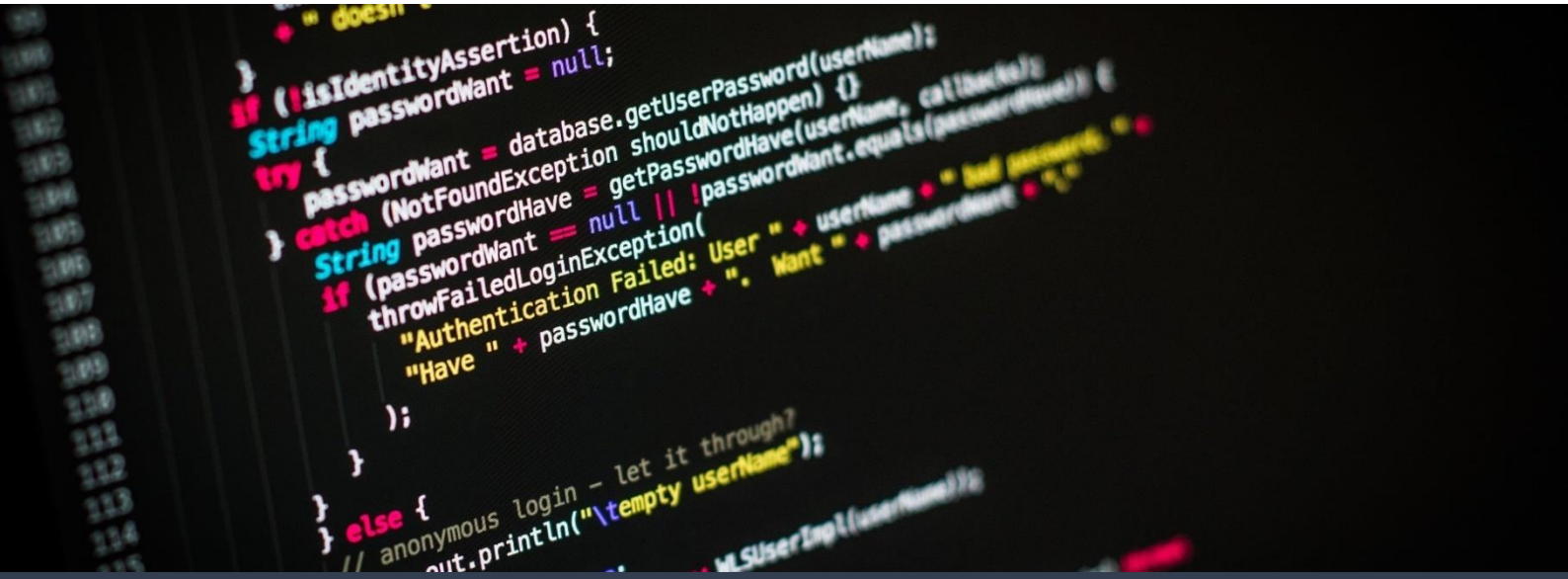
Los criterios empleados para la determinación del nivel de impacto asociado a un ciberincidente atienden a los siguientes parámetros:

- Impacto en la Seguridad Nacional o en la Seguridad Ciudadana.
- Efectos 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 interrupción en la prestación del servicio normal de la organización.
- Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
- Pérdidas económicas.
- Extensión geográfica afectada.
- Daños reputacionales asociados.

Los incidentes se asociarán a alguno de los siguientes niveles de impacto: **CRÍTICO, MUY ALTO, ALTO**, **MEDIO, BAJO** o **SIN IMPACTO.**

CRÍTICO	MUY ALTO	ALTO	MEDIO	BAJO	SIN IMPACTO

Ilustración 3. Niveles de impacto de un ciberincidente



A continuación se incluye la *Tabla 5. Criterios de determinación del nivel de impacto de un ciberincidente*. Mediante la consulta de esta tabla, las entidades notificantes de información podrán asignar un determinado nivel de impacto a un incidente.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE IMPACTO DE LOS CIBERINCIDENTES	
Nivel	**Descripción**
CRÍTICO	Afecta apreciablemente a la Seguridad Nacional.
	Afecta 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.
	El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
	Impacto económico superior al 0,1% del P.I.B. actual.
	Extensión geográfica supranacional.
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.
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 un servicio esencial.
	Afecta a sistemas clasificados RESERVADO.
	Afecta a más del 75% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios.
	El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
	Impacto económico entre el 0,07% y el 0,1% del P.I.B. actual.
	Extensión geográfica superior a 4 CC.AA. o 1 T.I.S.
	Daños reputacionales a la imagen del país (marca España).
	Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.
ALTO	Afecta a más del 50% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios.
	El ciberincidente precisa para resolverse entre 5 y 30 Jornadas–Persona.

	Impacto económico entre el 0,03% y el 0,07% del P.I.B. actual.
	Extensión geográfica superior a 3 CC.AA.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
MEDIO	Afecta a más del 20% de los sistemas de la organización.
	Interrupción en la presentación del servicio superior al 5% de usuarios.
	El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.
	Impacto económico entre el 0,001% y el 0,03% del P.I.B. actual.
	Extensión geográfica superior a 2 CC.AA.
	Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
BAJO	Afecta a los sistemas de la organización.
	Interrupción de la prestación de un servicio.
	El ciberincidente precisa para resolverse menos de 1 Jornadas-Persona.
	Impacto económico entre el 0,0001% y el 0,001% del P.I.B. actual.
	Extensión geográfica superior a 1 CC.AA.
	Daños reputacionales puntuales, sin eco mediático
SIN IMPACTO	No hay ningún impacto apreciable.

Tabla 5. Criterios de determinación del nivel de impacto de un ciberincidente

T.I.S.; Hace referencia a "Territorios de Interés Singular". Se considera como tal a las ciudades de Ceuta y Melilla y a cada una de las islas que forman los archipiélagos de las Islas Baleares y las Islas Canarias.
P.I.B; Hace referencia a "Producto Interior Bruto". Se considera P.I.B. actualizado a 2017: 1.163.663M €

6.1.3. Niveles con notificación obligatoria asociada

Los incidentes se asociarán a uno de los niveles de peligrosidad e impacto establecidos en este apartado, teniendo en cuenta la obligatoriedad de notificación de todos aquellos que se categoricen con un nivel **CRÍTICO, MUY ALTO O ALTO** para todos aquellos **sujetos obligados** a los que les sea aplicable normativa específica de acuerdo a lo contemplado en esta "Guía nacional de notificación y gestión de ciberincidentes" en función de su naturaleza. En ese caso, **deberán comunicar, en tiempo y forma, los incidentes que registren en sus redes y sistemas de información y estén obligados a notificar por superar los umbrales de impacto o peligrosidad establecidos en esta guía[5].**

[5] **Los proveedores de servicios digitales definidos en el Real Decreto-ley 12/2018 se regirán de acuerdo con lo establecido en el REGLAMENTO DE EJECUCIÓN (UE) 2018/151** DE LA COMISIÓN 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

6.2. INTERACCIÓN CON EL CSIRT DE REFERENCIA

Los CSIRT de referencia disponen de herramientas de notificación y *ticketing* de incidentes para lograr una mejor gestión y seguimiento del incidente con los usuarios. Cada CSIRT puede proporcionar diversos métodos de interacción con estas herramientas para facilitar la interacción durante todo el ciclo de vida del incidente.

No obstante, en caso de no disponer de las herramientas proporcionadas por los CSIRT de referencia, se considera válido el uso de correo electrónico.

6.3. APERTURA DEL INCIDENTE

Siempre que el CSIRT de referencia recibe una notificación sobre un posible ciberincidente, el equipo técnico realiza un análisis inicial que determinará si el caso es susceptible de ser gestionado por el mismo. Esta apertura puede producirse por un reporte del afectado, por una detección del CSIRT como parte de las labores de detección que realizan o por un tercero que reporta al CSIRT un incidente que afecta a su comunidad de referencia.

Si aplica la gestión del ciberincidente por parte del CSIRT, se registrará la información reportada y se asignarán una clasificación y unos valores iniciales de peligrosidad e impacto que serán comunicados al remitente, iniciándose posteriormente las acciones necesarias para la resolución del ciberincidente.

Durante el registro de un ciberincidente, el CSIRT asignará a cada caso un identificador único que estará presente durante todas las comunicaciones relacionadas con el incidente. Si las comunicaciones se realizan por correo electrónico, este identificador

cuenta los proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo.

aparece en el campo “asunto” y no debe modificarse o eliminarse ya que esto ralentizaría la gestión y la resolución final del ciberincidente.

A lo largo del proceso de gestión del ciberincidente, el CSIRT podrá comunicarse con el remitente o con terceras partes para solicitar o intercambiar información adicional que agilice la resolución del problema.

Asimismo, las autoridades competentes podrán establecer canales de comunicación oportunos según se desarrolle reglamentariamente.

6.4. INFORMACIÓN A NOTIFICAR

Para una correcta gestión y tratamiento de incidente registrado, se hace necesario disponer de datos e informaciones precisas acerca del mismo. Por ello, en la *Tabla 6. Información a notificar en un ciberincidente a la autoridad competente* se especifica a modo de orientación una serie de puntos que la entidad afectada por el ciberincidente puede aportar en su comunicación a la autoridad competente o CSIRT de referencia.

No obstante lo establecido en el párrafo anterior, todos aquellos sujetos obligados a los que les sea aplicable normativa específica de acuerdo a lo contemplado en esta “Guía nacional de notificación y gestión de ciberincidentes”, deberán comunicar en tiempo y forma toda aquella información relativa al incidente registrado que les sea exigible.

En todo caso, el sujeto obligado comunicará, en la notificación inicial, todos aquellos campos acerca de los que tenga conocimiento en ese momento, siendo posteriormente perceptiva la cumplimentación de todos los campos de la *Tabla 6. Información a notificar en un ciberincidente a la autoridad competente* en la notificación final del incidente.

Qué notificar	Descripción
Asunto	Frase que describa de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
OSE/PSD	Denominación del operador de servicios esenciales o proveedor de servicios digitales que notifica.
Sector estratégico	Energía, transporte, financiero, etc.
Fecha y hora del incidente[6]	Indicar con la mayor precisión posible cuándo ha ocurrido el ciberincidente.
Fecha y hora de detección del incidente	Indicar con la mayor precisión posible cuándo se ha detectado el ciberincidente.
Descripción	Describir con detalle lo sucedido.
Recursos tecnológicos afectados	Indicar la información técnica sobre el número y tipo de activos afectados por el ciberincidente, incluyendo direcciones IP, sistemas operativos, aplicaciones, versiones…

[6] Indicando la zona horaria en formato UTC.

Origen del incidente	Indicar la causa del incidente si se conoce. Apertura de un fichero sospechoso, conexión de un dispositivo USB, acceso a una página web maliciosa, etc.
Taxonomía (clasificación)	Posible clasificación y tipo de ciberincidente en función de la taxonomía descrita.
Nivel de Peligrosidad	Especificar el nivel de peligrosidad asignado a la amenaza. Consultar Tabla 4. Criterios de determinación del nivel de peligrosidad de un ciberincidente.
Nivel de Impacto	Especificar el nivel de impacto asignado al incidente. Consultar Tabla 5. Criterios de determinación del nivel de impacto de un ciberincidente.
Impacto transfronterizo	Indicar si el incidente tiene impacto transfronterizo en algún Estado miembro de la Unión Europea. Especificar.
Plan de acción y contramedidas	Actuaciones realizadas hasta el momento en relación al ciberincidente. Indicar el Plan de acción seguido junto con las contramedidas implantadas.
Afectación	Indicar si el afectado es una empresa o un particular y las afectaciones de acuerdo a los criterios indicados en la Tabla 5. Criterios de determinación del nivel de impacto de un ciberincidente.
Medios necesarios para la resolución (J-P)	Capacidad empleada en la resolución del incidente en Jornadas-Persona.
Impacto económico estimado (Si se conoce)	Costes asociados al incidente, tanto de carácter directo como indirecto.
Extensión geográfica (Si se conoce)	Local, autonómico, nacional, supranacional, etc.
Daños reputacionales. (Si se conocen)	Afectación a la imagen corporativa del operador.
Adjuntos	Indicar la relación de documentos adjuntos que se aportan para ayudar a conocer la causa del problema o a su resolución (capturas de pantalla, ficheros de registro de información, correos electrónicos, etc.)
Regulación afectada	ENS / RGPD /NIS / PIC / Otros
Se requiere actuación de FFCCSE	Si / No

Tabla 6. Información a notificar en un ciberincidente a la autoridad competente

6.5. VENTANA TEMPORAL DE REPORTE

Todos aquellos **sujetos obligados** que se vean afectados por un incidente de obligada notificación a la autoridad competente, a través del CSIRT de referencia, remitirán, en tiempo y forma, aquellas notificaciones inicial, intermedia y final requeridas de acuerdo a la *Tabla 7. Ventana temporal de reporte para sujetos obligados*.

- La notificación inicial es una comunicación consistente en poner en conocimiento y alertar de la existencia de un incidente.

- La notificación intermedia es una comunicación mediante la que se actualizarán los datos disponibles en ese momento relativos al incidente comunicado.

- La notificación final es una comunicación final mediante la que se amplían y confirman los datos definitivos relativos al incidente comunicado.

No obstante esto, se aportarán todas aquellas notificaciones adicionales intermedias o posteriores que se consideren necesarias.

La comunicación se realizará siempre por escrito mediante el uso de correo electrónico o sistema proporcionado por el CSIRT de referencia del operador, tomando la estructura de la *Tabla 6. Información a notificar en un ciberincidente a la autoridad competente*.

Nivel de peligrosidad o impacto	Notificación inicial	Notificación intermedia	Notificación final
CRÍTICO	Inmediata	24 / 48 horas	20 días
MUY ALTO	Inmediata	72 horas	40 días
ALTO	Inmediata	-	-
MEDIO	-	-	-
BAJO	-	-	-

Tabla 7. Ventana temporal de reporte para sujetos obligados

Los tiempos reflejados en la *Tabla 7. Ventana temporal de reporte para sujetos obligados* para la “notificación intermedia” y la “notificación final” tienen como referencia el momento de remisión de la “notificación inicial”. La “notificación inicial” tiene como referencia de tiempo el momento de tener conocimiento del incidente.

6.6. ESTADOS Y VALORES DE CIERRE

Durante las distintas fases de gestión de un ciberincidente, el CSIRT de referencia mantendrá el incidente en estado abierto, realizando en coordinación con el afectado las acciones necesarias y los seguimientos adecuados.

Una solución, y el cierre del ciberincidente asociado, no suponen siempre una resolución satisfactoria del problema. En algunos casos no es posible alcanzar una solución adecuada por diferentes razones, como pueden ser la falta de respuesta por parte de algún implicado o la ausencia de evidencias que permitan identificar el origen del problema.

La *Tabla 8. Estados de los ciberincidentes* muestra los diferentes estados que puede tener un ciberincidente, en un instante dado, detallando los distintos tipos de cierre.

Estado	Descripción
Cerrado (Resuelto y sin respuesta)	No hay respuesta por parte del organismo afectado en un periodo determinado. No obstante, el incidente parece estar resuelto.
Cerrado (Resuelto y con respuesta)	El organismo afectado ha solventado la amenaza y notifica a su CSIRT de referencia el cierre del ciberincidente.
Cerrado (Sin impacto)	La detección ha resultado positiva pero el organismo no es vulnerable o no se ve afectado por el ciberincidente.
Cerrado (Falso positivo)	La detección ha sido errónea.
Cerrado (Sin resolución y sin respuesta)	Si el ciberincidente no ha sido resuelto por el organismo afectado y este no ha comunicado con el CSIRT de referencia, es cerrado con este estado.
Cerrado (Sin resolución y con respuesta)	No se ha alcanzado una solución al problema o el afectado indica que no sabe solventarlo incluso con las indicaciones proporcionadas por el CSIRT.
Abierto	Estado que va desde que el organismo afectado notifica la amenaza al CSIRT de referencia, o bien este último lo comunica al afectado, hasta que se produce el cierre del mismo por alguna de las causas anteriormente descritas.

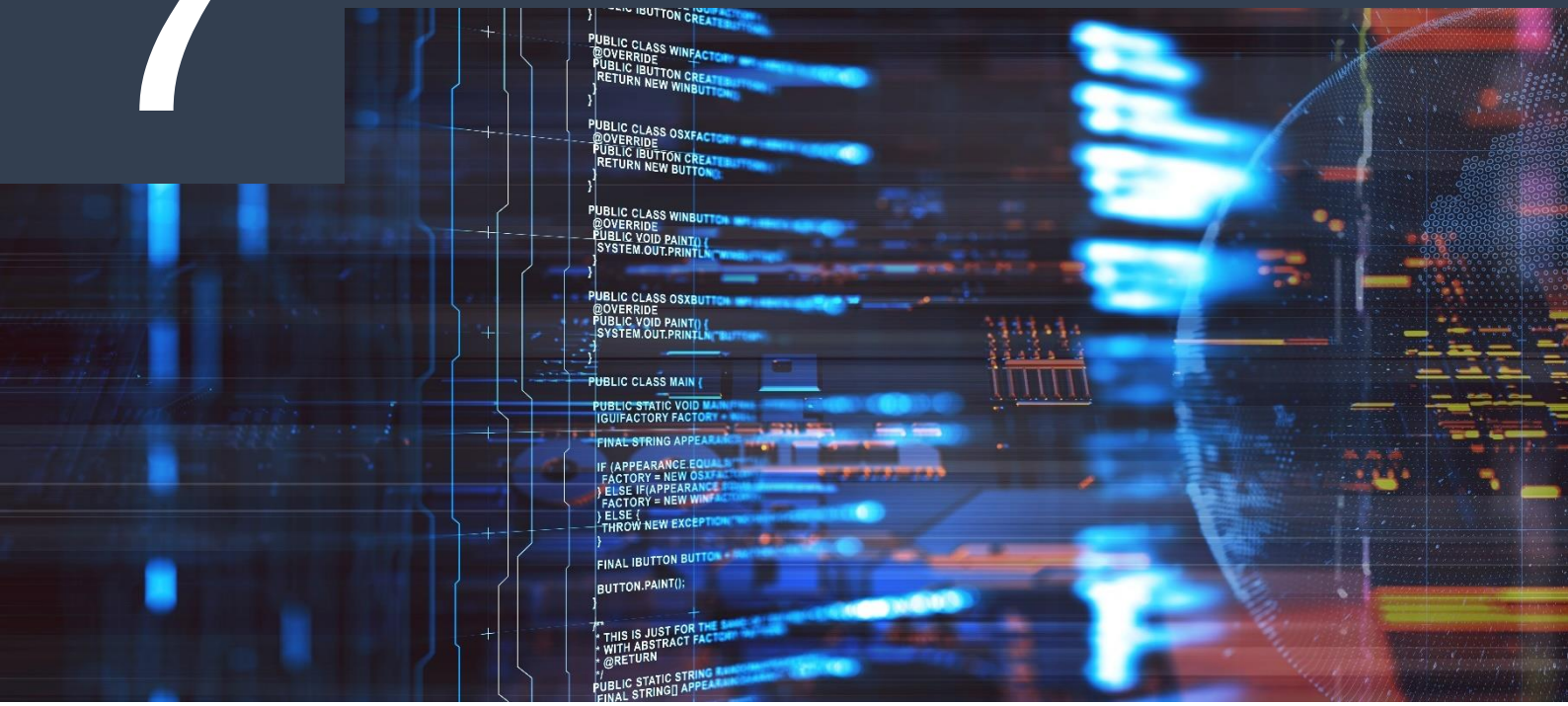
Tabla 8. Estados de los ciberincidentes

La *Tabla 9. Tiempos de cierre del ciberincidente sin respuesta* muestra los días tras los que se cerrará un ciberincidente sin respuesta, en función de su nivel de peligrosidad o impacto.

Nivel de peligrosidad o impacto	Cierre del ciberincidente (días naturales)
CRÍTICO	120
MUY ALTO	90
ALTO	45
MEDIO	30
BAJO	21

Tabla 9. Tiempos de cierre del ciberincidente sin respuesta

7 GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD



Se conoce como gestión de ciberincidentes a un conjunto ordenado de acciones enfocadas a prevenir en la medida de lo posible la ocurrencia de ciberincidentes y, en caso de que ocurran, restaurar los niveles de operación lo antes posible. El proceso de gestión de incidentes consta de diferentes fases y, aunque todas son necesarias, algunas pueden estar incluidas como parte de otras o tratarse de manera simultánea.

Ilustración 4. Fases de la gestión de un ciberincidente

A continuación, se describen brevemente las diferentes fases de la gestión de ciberincidentes.

7.1. PREPARACIÓN

Se trata de una fase inicial en la que toda entidad debe estar preparada para cualquier suceso que pudiera ocurrir. Una buena anticipación y entrenamiento previo es clave para realizar una gestión eficaz de un incidente, para lo que hace falta tener en cuenta tres pilares fundamentales: las personas, los procedimientos y la tecnología.

Algunos de los puntos más relevantes a tener en cuenta en esta fase son:

- Disponer de información actualizada de contacto, tanto de personal interno como externo, a implicar en otras fases de gestión del ciberincidente, así como las distintas vías de contacto disponibles en cada caso.
- Mantener las políticas y procedimientos actualizados. Especialmente todos los relativos a gestión de incidentes, recogida de evidencias, análisis forense o recuperación de sistemas.
- Herramientas a utilizar en todas las fases de gestión de un ciberincidente.
- Formación del equipo humano para mejorar las capacidades técnicas y operativas.
- Realizar análisis de riesgos que permita disponer de un plan de tratamiento de riesgos que permita controlarlos pudiendo ser mitigados, transferidos o aceptados.
- Ejecución de ciberejercicios a fin de entrenar las capacidades y procedimientos técnicos, operativos, de gestión y coordinación.

7.2. IDENTIFICACIÓN

El objetivo de esta fase es tener la capacidad de identificar o detectar cualquier ciberincidente que pueda sufrir un organismo o entidad y con la menor dilación posible, para lo cual es importante realizar una monitorización lo más completa posible. Teniendo en cuenta la máxima de que no todos los eventos o alertas de ciberseguridad son ciberincidentes.

Una correcta identificación o detección se basa en los siguientes principios:

- Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
- Recolectar información situacional que permita detectar anomalías.
- Disponer de capacidades para descubrir ciberincidentes y comunicarlos a los contactos apropiados.
- Recopilar y almacenar de forma segura todas las evidencias.

- Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

7.3. CONTENCIÓN

En el momento que se ha identificado un ciberincidente la máxima prioridad es contener el impacto del mismo en la organización de forma que se puedan evitar lo antes posible la propagación a otros sistemas o redes evitando un impacto mayor, y la extracción de información fuera de la organización.

Ésta suele ser la fase en la que se realiza el triaje que consiste en evaluar toda la información disponible en ese momento realizar una clasificación y priorización del ciberincidente en función del tipo y de la criticidad de la información y los sistemas afectados. Adicionalmente se identifican posibles impactos en el negocio y en función de los procedimientos se trabaja en la toma de decisiones con las unidades de negocio apropiadas y/o a los responsables de los servicios potencialmente afectados.

Durante esta fase se debe:

- Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
- Recolectar información situacional que permita detectar anomalías.
- Disponer de capacidades para descubrir ciberincidentes y comunicarlos a los contactos apropiados.
- Recopilar y almacenar de forma segura todas las evidencias.
- Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

7.4. MITIGACIÓN

Las medidas de mitigación dependerán del tipo de ciberincidente, ya que en algunos casos será necesario contar con apoyo de proveedores de servicios, como en el caso de un ataques de denegación de servicio distribuido (*DDoS*), y en otros ciberincidentes puede suponer incluyo el borrado completo de los sistemas afectados y recuperación desde una copia de seguridad.

A pesar de que las medidas de mitigación dependen del tipo de ciberincidente y la afectación que haya tenido, algunas recomendaciones en esta fase son:

- Determinar las causas y los síntomas del ciberincidente para determinar las medidas de mitigación más eficaces.
- Identificar y eliminar todo el software utilizado por los atacantes. A menudo la forma que ofrece más garantías de eliminar todo rastro de un incidente pasa por un nuevo plataformado de la máquina.

- Recuperación de la última copia de seguridad limpia.

- Identificar servicios utilizados durante el ataque, ya que en ocasiones los atacantes utilizan servicios legítimos de los sistemas atacados.

7.5. RECUPERACIÓN

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante no precipitarse en la puesta en producción de sistemas que se han visto implicados en ciberincidentes.

Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un periodo de tiempo con medidas adicionales de monitorización.

7.6. ACTUACIONES POST-INCIDENTE

Una vez que el ciberincidente está controlado y la actividad ha vuelto a la normalidad, es momento de llevar a cabo un proceso al que no se le suele dar toda la importancia que merece: las lecciones aprendidas.

Conviene pararse a reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados a la misma. La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda volver a repetir, además de mejorar los procedimientos.

Por último se realizará un informe del ciberincidente que deberá detallar la causa del ciberincidente y coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados), así como las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.

8 MÉTRICAS E INDICADORES

De cara a la evaluación de la implantación, eficacia y eficiencia del proceso de gestión de ciberincidentes por la autoridad competente o CSIRT de referencia, se incluyen a continuación las tablas necesarias para la asignación de métricas e indicadores de referencia recomendadas para medir el nivel de implantación y eficacia del proceso de gestión de incidentes de cada organización.

8.1. MÉTRICAS DE IMPLANTACIÓN

M1	**Indicador**	Alcance del sistema de gestión de incidentes	
	Objetivo	Saber si todos los sistemas de información están adscritos al servicio.	
	Método	Se cuentan cuántos servicios están bajo control. (Si se conociera cuántos servicios hay en total, se podría calcular un porcentaje). # servicios imprescindibles para la organización. # servicios importantes para la organización.	
	Caracterización	Objeto	100%
		Umbral amarillo	Imprescindibles: 4/5 (80%) Importantes: 2/3 (67%)
		Umbral rojo	Imprescindibles: 2/3 (67%) Importantes: 1/2 (50%)
		Frecuencia medición	Trimestral
		Frecuencia reporte	Anual

Tabla 10. Métricas de implantación

8.2. MÉTRICAS DE RESOLUCIÓN DE CIBERINCIDENTES

M2	**Indicador**	Resolución de ciberincidentes de nivel de impacto ALTO / MUY ALTO / CRÍTICO	
	Objetivo	Ser capaces de resolver prontamente incidentes de alto impacto.	
	Método	Se mide el tiempo que se tarda en resolver un incidente con un alto impacto en sistemas de la organización: desde que se notifica hasta que se resuelve. T(50) tiempo que se tarda en cerrar el 50% de los incidentes T (90) tiempo que se tarda en cerrar el 90% de los incidentes	
	Caracterización	Objeto	T(50) = 0 && T(90) = 0
		Umbral amarillo	T(50) > 4d || T(90) > 5d
		Umbral rojo	T(50) > 14d || T(90) > 18d
		Frecuencia mediación	Anual
		Frecuencia reporte	Anual
M3	**Indicador**	Resolución de ciberincidentes de nivel de impacto BAJO / MEDIO	
	Objetivo	Ser capaces de resolver prontamente incidentes de impacto medio.	
	Método	Se mide el tiempo que se tarda en resolver un incidente con un impacto en sistemas de la organización: desde que se notifica hasta que se resuelve. T(50) tiempo que se tarda en cerrar el 50% de los incidentes T(90) tiempo que se tarda en cerrar el 90% de los incidentes	
	Caracterización	Objeto	T(50) = 0 && T(90) = 0
		Umbral amarillo	T(50) > 10d || T(90) > 30d
		Umbral rojo	T(50) > 15d || T(90) > 45d
		Frecuencia medición	Anual
		Frecuencia de reporte	Anual

Tabla 11. Métricas de resolución de ciberincidentes

8.3. MÉTRICAS DE RECURSOS

M4	**Indicador**	Recursos consumidos	
	Objetivo	Conocer si es necesario aumentar la fuerza de trabajo	
	Método	Estimación del número de horas-hombre dedicadas a resolver incidentes de seguridad. Fórmula: #horas dedicadas a incidentes / #horas formalmente contratadas para seguridad TIC.	
	Caracterización	Objeto	<20%
		Umbral amarillo	20%
		Umbral rojo	50%
		Frecuencia mediación	Trimestral
		Frecuencia reporte	Anual

Tabla 12. Métricas de recursos

8.4. MÉTRICAS DE GESTIÓN DE INCIDENTES

M5	**Indicador**	Estado de cierre los incidentes	
	Objetivo	Ser capaces de gestionar incidentes de seguridad	
	Método	Se mide el número de incidentes que han sido cerrados sin respuesta. Fórmula: # incidentes de seguridad cerrados sin respuesta / # total de incidentes notificados	
	Caracterización	Objeto	<10%
		Umbral amarillo	20%
		Umbral rojo	50%
		Frecuencia mediación	Trimestral
		Frecuencia reporte	Anual
M6	**Indicador**	Estado de cierre los incidentes de peligrosidad MUY ALTA/ CRÍTICA	
	Objetivo	Ser capaces de gestionar incidentes de seguridad de alta peligrosidad	
	Método	Se mide el número de incidentes que han sido cerrados sin respuesta. Fórmula: # incidentes de seguridad cerrados sin respuesta / # total de incidentes notificados	
	Caracterización	Objeto	0%
		Umbral amarillo	5%
		Umbral rojo	20%
		Frecuencia medición	Trimestral
		Frecuencia reporte	Anual

Tabla 13. Métricas de gestión de incidentes

A1

ANEXO 1. NOTIFICACIÓN EN EL ÁMBITO DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Aquellas entidades cuya autoridad competente en materia de notificación de incidentes, de acuerdo a la normativa vigente, sea el **Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)**, deberán cumplir lo preceptuado en el presente anexo en lo que se refiere a la notificación de incidentes acaecidos en las redes y sistemas de información que soportan los servicios esenciales prestados por sus infraestructuras.

Para ello, el operador afectado deberá tener en cuenta lo reseñado en este anexo en relación a las obligaciones de notificación en función de que se cumplan unos determinados criterios relativos al nivel de peligrosidad y/o impacto asociados al incidente. Se incluye a su vez la información necesaria en cuanto al contenido de las comunicaciones a realizar, el marco temporal exigible y las preceptivas comunicaciones al Ministerio Fiscal u otros organismos.

Asimismo, aquellos proveedores de los sujetos obligados por este anexo que proporcionen sus productos o servicios a éstos, y cuyas actividades tengan afección directa a la prestación de un Servicio Esencial, deberán cumplir con los mismos criterios exigibles a los operadores. En todo caso, el operador afectado será el responsable último del cumplimiento de los requerimientos exigibles en este texto.

COMUNICACIONES OBLIGATORIAS

Para la notificación de los incidentes de ciberseguridad se utilizará como criterio de referencia el **Nivel de peligrosidad** que se asigne a un incidente, sin perjuicio de que a lo largo del desarrollo, mitigación o resolución del mismo, se categorice con un determinado **Nivel de impacto** que requiera la comunicación del incidente al CNPIC a través del CSIRT de referencia

No obstante lo establecido en el párrafo anterior, el Ministerio del Interior, a través de la Secretaría de Estado de Seguridad podrá exigir la comunicación de cualquier incidente acaecido en las redes o sistemas de información que soportan los servicios esenciales prestados por sus infraestructuras de acuerdo a la aplicación de un determinado Nivel de Alerta Antiterrorista (NAA) o Nivel de Alerta en Infraestructuras Críticas (NAIC).

Notificación obligatoria en función del nivel de peligrosidad del ciberincidente

Conforme a los criterios indicados en el cuerpo de este texto, en los que se asigna un determinado nivel de peligrosidad a un incidente, será obligatoria la notificación de todos aquellos que sean categorizados con un nivel de peligrosidad **CRÍTICO, MUY ALTO o ALTO**.

Para una definición más precisa del nivel de peligrosidad asociado a cada incidente registrado en las redes y sistemas de información del operador, se seguirá la *Tabla 4. Criterios de determinación del nivel de peligrosidad de un ciberincidente* en la que se asigna un nivel de peligrosidad determinado en función de la clasificación del incidente

Notificación obligatoria en función del nivel de impacto del ciberincidente

Conforme a los criterios indicados en el cuerpo de este texto en los que se asigna un determinado nivel de impacto a un incidente, será obligatoria la notificación de todos aquellos que sean categorizados con un nivel de impacto **CRÍTICO, MUY ALTO o ALTO**.

Para una definición más precisa del nivel de impacto asociado a cada incidente registrado, se seguirá la *Tabla 5. Criterios de determinación del nivel de impacto de un ciberincidente* en la que se asigna un nivel de impacto determinado en función de una serie de efectos provocados por el incidente en las redes o sistemas de información del operador.

COMUNICACIÓN AL MINISTERIO FISCAL Y OTROS ORGANISMOS

Cuando un incidente sea comunicado dentro del marco competencial de este anexo a la “Guía nacional de notificación y gestión de ciberincidentes”, y presente caracteres de infracción delictiva, el Centro Nacional de Protección de Infraestructuras y Ciberseguridad dará cuenta de ello, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior al Ministerio Fiscal y a las FFCCSE a los efectos oportunos, trasladándoles toda aquella información que posean en relación al hecho.

FLUJOGRAMAS DE REPORTE Y RESPUESTA OPERATIVA PIC

En las siguientes imágenes se pueden observar los flujogramas informativos en los que se detalla el proceso de notificación y gestión de un incidente y el proceso de respuesta operativa ante la comunicación de un ciberincidente acaecido en las redes o sistemas de información que soportan los servicios esenciales prestados por las infraestructuras de un operador.

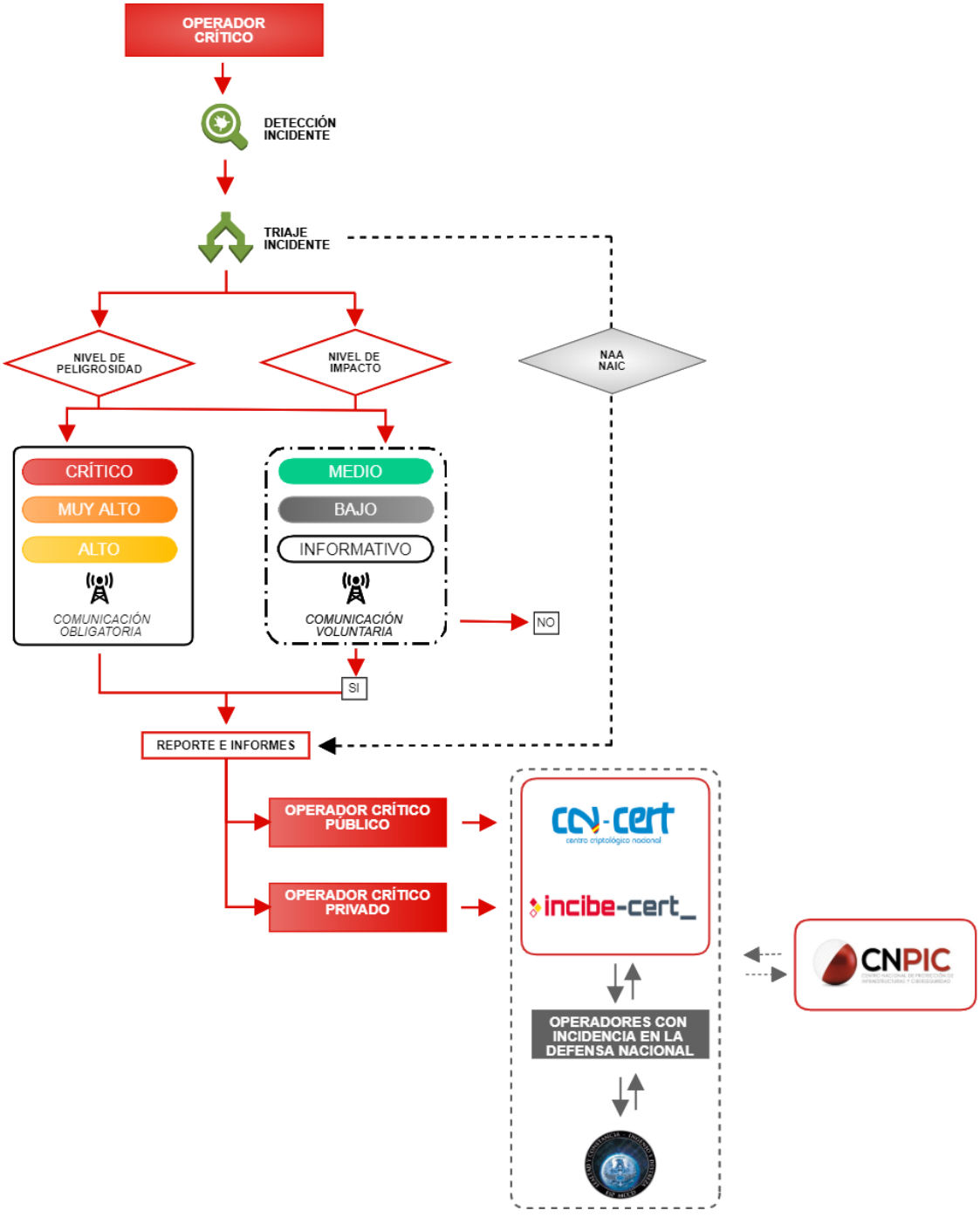


Ilustración 5. Flujograma de gestión y notificación en el ámbito PIC

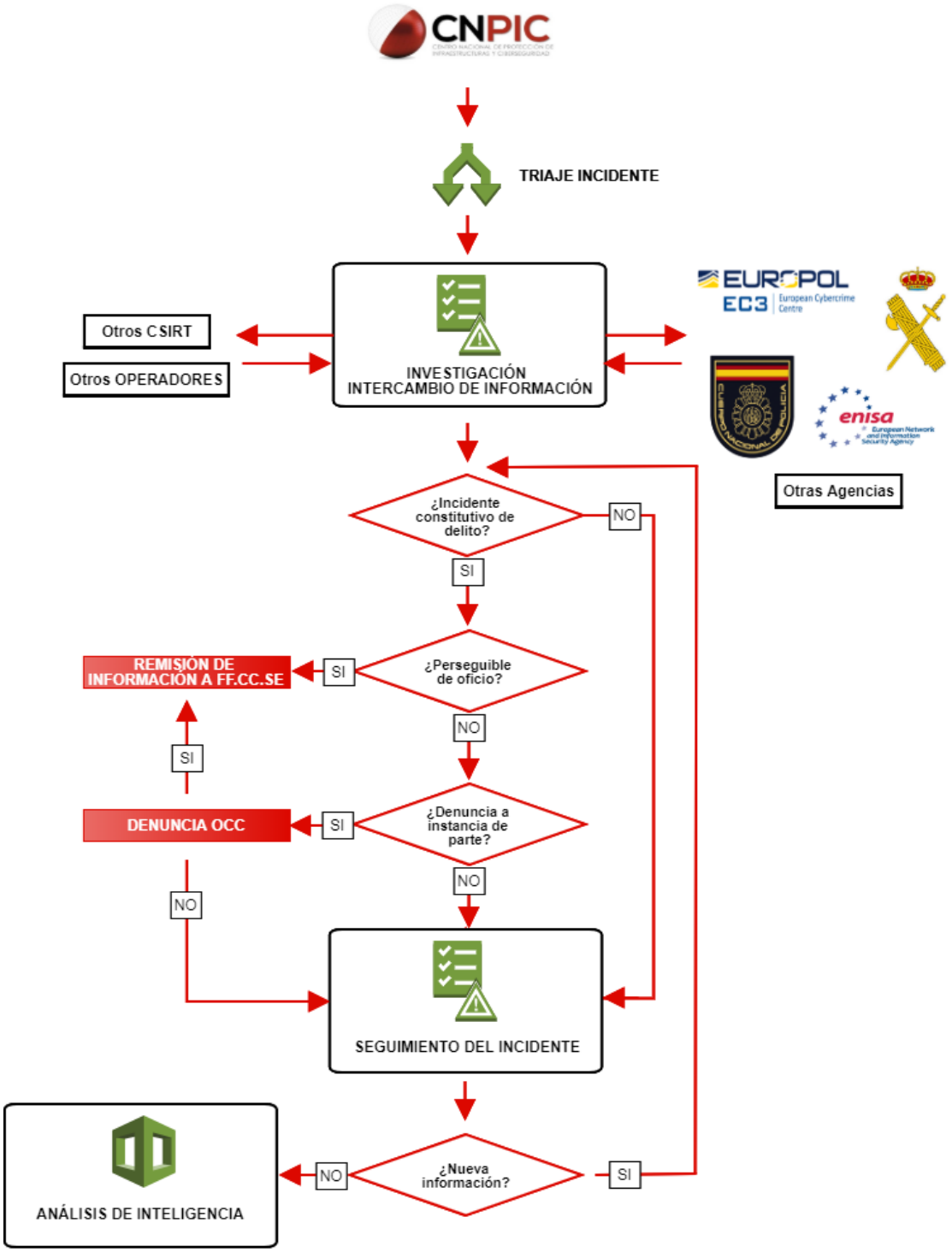


Ilustración 6. Flujograma de respuesta operativa en el ámbito PIC

A2 ANEXO 2. NOTIFICACIÓN EN EL ÁMBITO DEL SECTOR PÚBLICO

Los organismos del Sector Público notificarán los incidentes según especifica la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad publicada en el BOE nº 95 de 18 de abril de 2018 y la Guía CCN-STIC 817 de Gestión de Ciberincidentes.

Notificación obligatoria de los incidentes con nivel de impacto Alto, Muy alto y Crítico

Las notificaciones efectuadas por las entidades del ámbito de aplicación de la citada Instrucción Técnica de Seguridad al Centro Criptológico Nacional (CCN) se realizará en los términos indicados en los artículos 36 y 37 del Real Decreto 3/2010, de 8 de enero.

Para ello, se notificarán los incidentes de seguridad que tengan un impacto significativo en la seguridad de la información manejada o los servicios prestados en relación con la categoría del sistema, determinada de acuerdo con lo dispuesto en los artículos 43, 44 y Anexo I del Real Decreto 3/2010, de 8 de enero.

En todo caso, serán de obligatoria notificación al CCN en el momento en que se produzcan, los incidentes de seguridad que por su nivel de impacto potencial sean calificados con el nivel de CRÍTICO, MUY ALTO o ALTO, mediante el empleo de las herramientas desarrolladas al efecto de la notificación de incidentes (LUCIA).

A3

ANEXO 3. NOTIFICACIÓN EN EL ÁMBITO DEL SECTOR PRIVADO

Las entidades de derecho privado notificarán los ciberincidentes a INCIBE-CERT según se recoge en el artículo 11 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, a través de los canales y las herramientas que INCIBE-CERT establezca. La gestión de los casos se realizará conforme al “Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía".

La ciudadanía podrá notificar los ciberincidentes a INCIBE-CERT, según se recoge también en el artículo 11 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en el que se cita que INCIBE-CERT será, así mismo, equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades no incluidas anteriormente en el apartado 1 del mismo artículo 11, pudiendo utilizar los canales y herramientas que INCIBE-CERT facilite. La gestión de los casos se realizará conforme al “Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía".

A4

ANEXO 4. MARCO REGULADOR

La gestión de incidentes de ciberseguridad, y de forma particular la notificación a su autoridad competente o CSIRT de referencia, constituye un imperativo legal para determinadas organizaciones públicas y privadas de España.

La elaboración de la presente "Guía nacional de notificación y gestión de ciberincidentes" ha tomado como referencia la siguiente normativa a nivel nacional.

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.
- 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

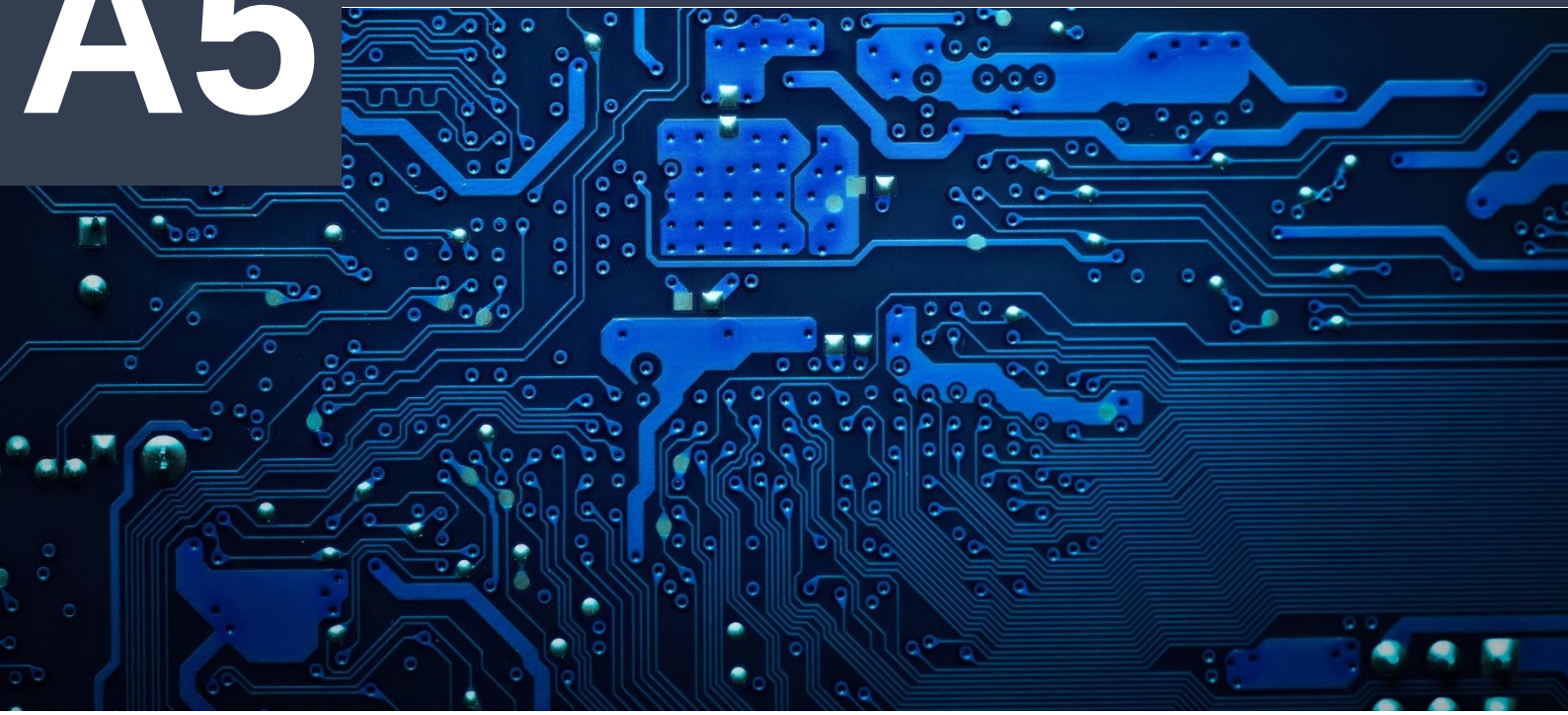
- Real Decreto 998/2017, de 24 de noviembre, por el que se desarrolla la estructura orgánica básica del MDEF y modifica el Real Decreto 424/2016, de 11 de noviembre.

- 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).

A5

ANEXO 5. GLOSARIO DE TÉRMINOS



CONTENIDO ABUSIVO

- **Correo masivo no solicitado (SPAM)**: Correo electrónico no solicitado que se envía a un gran número de usuarios, o bien una alta tasa de correos electrónicos enviados a un mismo usuario en un corto espacio de tiempo.

- **Acoso**: Referido a acoso virtual o ciberacoso, se trata del uso de medios de comunicación digitales para acosar a una persona, o grupo de personas, mediante ataques personales, divulgación de información privada o íntima, o falsa.

- **Extorsión**: Obligar a una persona o mercantil, mediante el empleo de violencia o intimidación, a realizar u omitir actos con la intención de producir un perjuicio a esta, o bien con ánimo de lucro de la que lo provoca.

- **Mensajes ofensivos**: Comunicaciones no esperadas o deseadas, así como acciones o expresiones que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

- **Delito**: Cualquier acción tipificada como delito de acuerdo a lo establecido en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- **Pederastia**: Cualquier comportamiento relacionado con los descritos en el Título VIII del Código Penal, relativos a la captación o utilización de menores de edad o personas con discapacidad necesitadas de especial protección en actos que atenten contra su indemnidad o libertad sexual.

- **Racismo**: Cualquier infracción penal, incluyendo infracciones contra las personas o las propiedades, donde la víctima, el local o el objetivo de la infracción se elija por su real o percibida, conexión, simpatía, filiación, apoyo o pertenencia a un grupo social, raza, religión o condición sexual.

- **Apología de la violencia**: Exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor.

CONTENIDO DAÑINO

- **Malware (código dañino)**: Palabra que deriva de los términos *malicious* y *softwar*e. Cualquier pieza de software que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como malware. Así pues malware es un término que engloba varios tipos de programas dañinos.

- **Virus**: Tipo de malware cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso o consentimiento del usuario. Se propaga mediante la ejecución en el sistema de software, archivos o documentos con carga dañina, adquiriendo la capacidad de replicarse de un sistema a otro. Los métodos más comunes de infección se dan a través de dispositivos extraíbles, descargas de Internet y archivos adjuntos en correos electrónicos. No obstante también puede hacerlo a través de scripts, documentos, y vulnerabilidades XSS presentes en la web. Es reseñable que un virus requiere la acción humana para su propagación a diferencia de otro malware, véase *Gusano*.

- **Gusano**: Programa malicioso que tiene como característica principal su alto grado de dispersabilidad. Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos específicos o ampliamente utilizados.

- **Troyano**: Tipo de malware que se enmascara como software legítimo con la finalidad de convencer a la víctima para que instale la pieza en su sistema. Una vez instalado, el software dañino tiene la capacidad de desarrollar actividad perjudicial en segundo plano. Un troyano no depende una acción humana y no tiene la capacidad de replicarse, no obstante puede tener gran capacidad dañina en un sistema a modo de troyanos o explotando vulnerabilidades de software.

- **Programa espía (spyware)**: Tipo de malware que espía las actividades de un usuario sin su conocimiento o consentimiento. Estas actividades pueden incluir keyloggers, monitorizaciones, recolección de datos así como robo de datos. Los spyware se pueden difundir como un troyano o mediante explotación de software.

- **Rootkit**: Conjunto de software dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones. Denotar que por maquina se entiende todo el espectro de sistemas IT, desde smartphones hasta ICS. El propósito por tanto de un rootkit es enmascarar eficazmente payloads y permitir su existencia en el sistema.

- **Dialer**: Tipología de malware que se instala en una máquina y, de forma automática y sin consentimiento del usuario, realiza marcaciones telefónicas a número de tarificación especial. Estas acciones conllevan costes económicos en la víctima al repercutir el importe de la comunicación.

- **Ransomware**: Se engloba bajo este epígrafe a aquel malware que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados.

- **Bot dañino**: Una botnet es el nombre que se emplea para designar a un conjunto de máquinas controladas remotamente con finalidad generalmente maliciosa. Un bot es una pieza de software maliciosa que recibe órdenes de un atacante principal que controla remotamente la máquina. Los servidores C&C habilitan al atacante para controlar los bots y que ejecuten las órdenes dictadas remotamente.

- **RAT**: Del inglés *Remote Access Tool*, se trata de una funcionalidad específica de control remoto de un sistema de información, que incorporan determinadas familias o muestras de software dañino (malware).

- **C&C**: Del inglés *command and control*, se refiere a paneles de mando y control (también referenciados como C2), por el cual atacantes cibernéticos controlan determinados equipos zombie infectados con muestras de la misma familia de software dañino. El panel de comando y control actúa como punto de referencia, control y gestión de los equipos infectados.

- **Conexión sospechosa**: Todo intercambio de información a nivel de red local o pública, cuyo origen o destino no esté plenamente identificado, así como la legitimidad de los mismos.

OBTENCIÓN DE INFORMACIÓN

- **Escaneo de puertos (Scanning)**: Análisis local o remoto mediante software, del estado de los puertos de una máquina conectada a una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

- **Escaneo de red (Scanning)**: Análisis local o remoto mediante software, del estado de una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

- **Escaneo de tecnologías**: Análisis local o remoto mediante software, de las tecnologías presentes o disponibles en una red determinada o un sistema de información concreto, mediante el cual se obtienen la referencias del hardware/software presente, así como su versión, y potenciales vulnerabilidades.

- **Transferencia de zona DNS (AXFR IXFR)**: Transacción de los servidores DNS utilizada para la replicación de las bases de datos entre un servidor primero y los secundarios. Estas transacciones pueden ser completas (AXFR) o incrementales (IXFR).

- **Análisis de paquetes (Sniffing)**: Análisis mediante software del tráfico de una red con la finalidad de capturar información. El tráfico que viaje no cifrado podrá ser capturado y leído por un atacante.

- **Ingeniería social**: Técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.

- **Phishing**: Estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta empleando métodos de ingeniería social..

- **Spear Phishing**: Variante del phishing mediante la que el atacante focaliza su actuación sobre un objetivo concreto

INTRUSIONES

- **Explotación**: Cualquier práctica mediante la cual un atacante cibernético vulnera un sistema de información y/o comunicación, con fines ilícitos o para los cuales no está debidamente autorizado.

- **Inyección SQL**: Tipo de explotación, consistente en la introducción de cadenas mal formadas de SQL, o cadenas que el receptor no espera o controla debidamente; las cuales provocan resultados no esperados en la aplicación o programa objetivo, y por la cual el atacante produce efectos inesperados y para los que no está autorizado en el sistema objetivo.

- **Cross Site Scripting XSS (Directo o Indirecto)**: Ataque que trata de explotar una vulnerabilidad presente en aplicaciones web, por la cual un atacante

inyecta sentencias mal formadas o cadenas que el receptor no espera o controla debidamente.

- **Cross Site Request Forgery (CSFR)**: Falsificación de petición en sitios cruzados. Es un tipo de exploit dañino de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un clic, cabalgamiento de sesión, y ataque automático. Al contrario que en los ataques XSS, los cuales explotan la confianza que un usuario tiene en un sitio en particular, el Cross Site Request Forgery explota la confianza que un sitio tiene en un usuario en particular.

- **Defacement**: Tipología de ataque a sitios web en el que se implementa un cambio en la apariencia visual de la página. Para ello suelen emplearse técnicas cómo inyecciones SQL o algún tipo de vulnerabilidad existente en la página o en el servidor.

- **Inclusión de ficheros (RFI y LFI)**: Vulnerabilidad que permite a un atacante mostrar o ejecutar archivos remotos alojados en otros servidores a causa de una mala programación de la página que contiene funciones de inclusión de archivos. La Inclusión local de archivos (LFI) es similar a la vulnerabilidad de Inclusión de archivos remotos, excepto que en lugar de incluir archivos remotos solo se pueden incluir archivos locales, es decir, archivos en el servidor actual para su ejecución.

- **Evasión de sistemas de control**: Proceso por el cual una muestra de software dañino, o un conjunto de acciones orquestadas por un atacante cibernético, consiguen vulnerar o esquivar los sistemas o políticas de seguridad establecidas por un determinado sistemas de información y comunicación.

- **Pharming**: Ataque informático que aprovecha vulnerabilidades de los servidores DNS (Domain Name System). Al tratar de acceder el usuario al sitio web, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web maliciosa que suplanta la auténtica, y en la que el atacante podrá obtener información sensible de los usuarios.

- **Ataque por fuerza bruta**: Proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de todas las combinaciones posibles, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

- **Ataque por diccionario**: Proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de un diccionario previamente generado con determinadas combinaciones de caracteres, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

- **Robo de credenciales de acceso**: Acceso o sustracción no autorizada a credenciales de acceso a sistemas de información y/o comunicación.

DISPONIBILIDAD

- **DoS (Denial of Service) o Ataque de denegación de servicio**: Conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

- **DDoS (Distributed Denial of Service) o Denegación distribuida de servicio**: Variante de DoS en el que la remisión de peticiones se lleva a cabo de forma coordinada desde varios puntos hacia un mismo destino. Para ello se emplean redes de bots, generalmente sin el conocimiento de los usuarios.

- **Sabotaje/Terrorismo/Vandalismo**: Ataques implementados con el objetivo de provocar la interrupción o degradación de la prestación de un servicio, provocando daños relevantes en la continuidad del servicio de una institución o daños reputacionales relevantes cometidos con propósitos ideológicos, políticos o religiosos.

- **Disrupción sin intención dañina**: Acciones que pueden provocar la interrupción o degradación de la prestación de un servicio, provocando daños relevantes en la continuidad del servicio de una institución o daños reputaciones relevantes.

- **Inundación SYN o UDP**: Procedimientos usados para la realización de ataque DoS o DDoS consistente en iniciar una gran cantidad de sesiones impidiendo al servidor atender las peticiones licitas.

- **DNS Open-Resolver**: Servidor DNS capaz resolver consultas DNS recursivas procedentes de cualquier origen de Internet. Este tipo de servidores suele emplearse por usuarios malintencionados para la realización de ataques DDoS.

- **Mala configuración**: Fallo de configuración en el software que está directamente asociado con una pérdida de disponibilidad de un servicio.

COMPROMISO DE LA INFORMACIÓN

- **Acceso no autorizado a la información o ciberespionaje**: Proceso por el cual un usuario no autorizado accede a consultar contenido para el cual no está autorizado.

- **Modificación no autorizada de información**: Proceso por el cual un usuario no autorizado accede a modificar contenido para el cual no está autorizado.

- **Borrado no autorizado de información**: Proceso por el cual un usuario no autorizado accede a borrar contenido para el cual no está autorizado.

- **Exfiltración de información**: Proceso por el cual un usuario difunde información en canales o fuentes en las cuales no está prevista o autorizada la compartición de esa información.

- **Acceso no autorizado a sistemas**: Proceso por el cual un usuario accede sin vulnerar ningún servicio, sistema o red, a sistemas de información y/o comunicación para los cuales no está debidamente autorizado, o no tiene autorización tácita o manifiesta.

- **Ataque POODLE / Ataque FREAK**: Proceso por el que se consigue que un servidor haga uso de un protocolo de comunicaciones no seguro, que originalmente no estaba previsto, con el objetivo de poder exfiltrar información.

FRAUDE

- **Uso no autorizado de recursos**: Empleo de tecnologías y/o servicios por usuarios que no están debidamente autorizados por la Dirección o negociado competente.

- **Suplantación de identidad**: Actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o acoso.

- **Derechos de propiedad intelectual**: La propiedad intelectual es el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación.

- **Otros fraudes**: Engaño económico con la intención de conseguir un beneficio, y con el cual alguien resulta perjudicado.

VULNERABILIDADES

- **Tecnología vulnerable**: Conocimiento por parte de los administradores de tecnologías, servicios o redes, de vulnerabilidades presentes en estas.

- **Política de seguridad precaria**: Política de seguridad de la organización deficiente, mediante la cual existe la posibilidad de que durante un espacio de tiempo determinado, atacantes cibernéticos realizaron accesos no autorizados a sistemas de información, no pudiendo determinar fehacientemente este extremo.

OTROS

- **Ciberterrorismo**: Delitos informáticos previstos en los art. 197 bis y ter y 264 a 264 quater de la Ley Orgánica 10/1995 de Código Penal cuando dichos delitos se cometan con las finalidades previstas en el artículo 573.1 del mismo texto. Estas finalidades son:

    - Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.
    - Alterar gravemente la paz pública.
    - Desestabilizar gravemente el funcionamiento de una organización internacional.
    - Provocar un estado de terror en la población o en una parte de ella.

- **Daños informáticos PIC**: Delitos informáticos previstos en los art 264.2 3º y 4º de la Ley Orgánica 10/1995 de Código Penal relacionadas con el borrado, dañado, alteración, supresión, o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una Infraestructura Crítica. Así como conductas graves relacionadas con los términos anteriores que afecten a la prestación de un Servicio Esencial.

- **APT (Advanced Persitent Threat o Amenaza Persistente Avanzada) / AVT (Advanced Volatility Threat)**: Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

- **Dominios DGA**: Procedimiento para generar de forma dinámica dominios donde se alojarán los servidores de Comando y control, técnica usada en redes Botnet para dificultar su detención.

- **Criptografía**: Técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca la clave mediante la cual ha sido cifrado.

- **Proxy**: Ordenador, generalmente un servidor, intermedio usado en las comunicaciones entre otros dos equipos, siendo normalmente usado de manera trasparente para el usuario.

GENERAL

- **Ciberseguridad**: Parte de la seguridad que se ocupa de los delitos cometidos en el ciberespacio y la prevención de los mismos.

- **Ciberespacio**: Espacio virtual que engloba todos los sistemas TIC, tanto sistemas de información como sistemas de control industrial. El ciberespacio se apoya en la disponibilidad de Internet como red de redes, enriquecida con otras redes de transporte de datos.

- **Redes y sistemas de información**: Se entiende por este concepto uno de los tres siguientes puntos:

    - Una red de comunicaciones electrónicas en el sentido del artículo 2, letra a), de la Directiva 2002/21/CE.
    - Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales.
    - Los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados anteriormente para su funcionamiento, utilización, protección y mantenimiento

- **Seguridad en redes y sistemas de información**: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

- **Operador de servicios esenciales**: una entidad pública o privada de uno de los tipos que figuran en el anexo II, que reúna los criterios establecidos en el artículo 5, apartado 2 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo.

- **Servicio digital**: un servicio en el sentido del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo que sea de uno de los tipos que figuran en el anexo III.

- **Proveedor de servicios digitales**: toda persona jurídica que preste un servicio digital.

- **Ciberincidente**: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

- **Gestión de ciberincidentes**: todos los procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

- **Ciberamenaza**: Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

- **Taxonomía**: Clasificación u ordenación en grupos de objetos o sujetos que poseen unas características comunes.

- **RGPD**: Reglamento General de Protección de Datos, reglamento EU 2016/679.
- **OpenPGP**: Estándar basado en el programa PGP, del inglés *Pretty Good Privacy,* cuya finalidad es proteger la información mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.
- **Webinject**: Herramienta gratuita y de código abierto diseñada principalmente para automatizar la prueba de las aplicaciones y servicios web.
- **Telnet**: Protocolo de red que permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.
- **RDP**: Remote Desktop Protocol. Protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre una terminal y un servidor Windows.
- **VNC (Virtual Network Computing)**: Programa de software libre basado en una estructura cliente-servidor que permite observar remotamente las acciones del ordenador servidor a través de un ordenador cliente.
- **SNMP (Simple Network Management Protocol)**: Protocolo de red utilizado para el intercambio de mensajes para la administración de dispositivos en red.
- **Redis**: Motor de base de datos en memoria, basado en el almacenamiento en tablas de hashes.
- **ICMP**: Protocolo de control de mensajes de Internet
- **Copia de seguridad limpia**: Punto de restauración de un sistema de la que se tiene la seguridad de no estar comprometida.


GOBIERNO
DE ESPAÑA