GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES



GOBIERNO DE ESPAÑA

APROBADA POR EL CONSEJO NACIONAL DE CIBERSEGURIDAD EL DÍA 9 DE ENERO DE 2019

ÍNDICE

1. INTRODUCCIÓN 3
2. OBJETO DE LA PRESENTE GUÍA 5
3. ALCANCE 8
4. VENTANILLA ÚNICA DE NOTIFICACIÓN 9

4.2. Reporte del incidente a CNN-CERT 10
4.3. Reporte de incidentes a INCIBE- CERT 10
4.4. Reporte de incidentes a ESPDEF-CERT 11

5. CLASIFICACIÓN/TAXONOMÍA DE LOS CIBERINCIDENTES 12
6. NOTIFICACIÓN DE INCIDENTES DE CIBERSEGURIDAD 17

6.1. Criterios para la notificación 17
6.2. Interacción con el CSIRT de referencia 23
6.3. Apertura del incidente 23
6.4. Información a notificar 24
6.5. Estados y valores de cierre 25

7. GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD 26

7.1. Preparación 27
7.2. Identificación 27
7.3. Contención 28
7.4. Mitigación 29
7.5. Recuperación 29
7.6. Actuaciones post-incidente 29

8. MÉTRICAS E INDICADORES 30

8.1. Métricas de implantación 30
8.2. Métricas de eficacia 31
8.3. Métricas de eficiencia 32
8.4. Métricas de gestión de incidentes 32

9. ANEXO 1. NOTIFICACIÓN EN EL ÁMBITO DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS 33

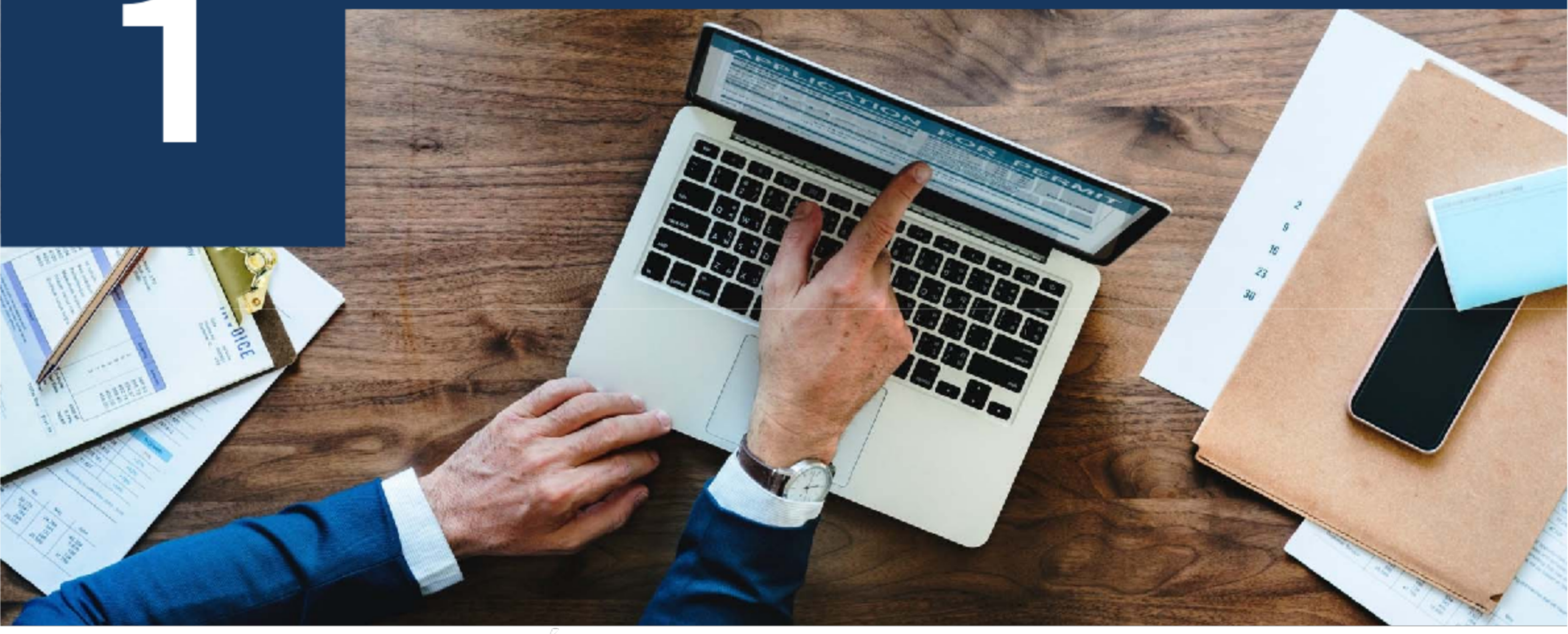
9.1. Comunicaciones obligatorias 33
9.2. Contenidos de la notificación e informes 34
9.3. Contenidos mínimos a notificar 35
9.4. Ventana temporal de reporte y remisión de informes 37
9.5. Comunicación al Ministerio Fiscal y a otros organismos 37
9.6. Flujogramas de reporte y de respuesta operativa PIC 38

10. ANEXO 2. ORGANISMOS DE REFERENCIA 41
11. ANEXO 3. MARCO REGULADOR 45

11.1. De carácter general 45
11.2. De carácter particular al ámbito del sector público 46
11.3. De carácter particular al ámbito de las infraestructuras críticas 46
11.4. De carácter particular a las redes militares y de defensa 47

12. ANEXO 4. GLOSARIO DE TÉRMINOS 48

1 INTRODUCCIÓN



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 local, autonómico y nacional.

- **INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España**, con un ámbito competencial en los ciudadanos, empresas, operadores de servicios esenciales e instituciones afiliadas a RedIRIS, la red académica y de investigación española. INCIBE-CERT será operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

- **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 coordinar las actividades de los CSIRT de referencia.

- **ESPDEF-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.

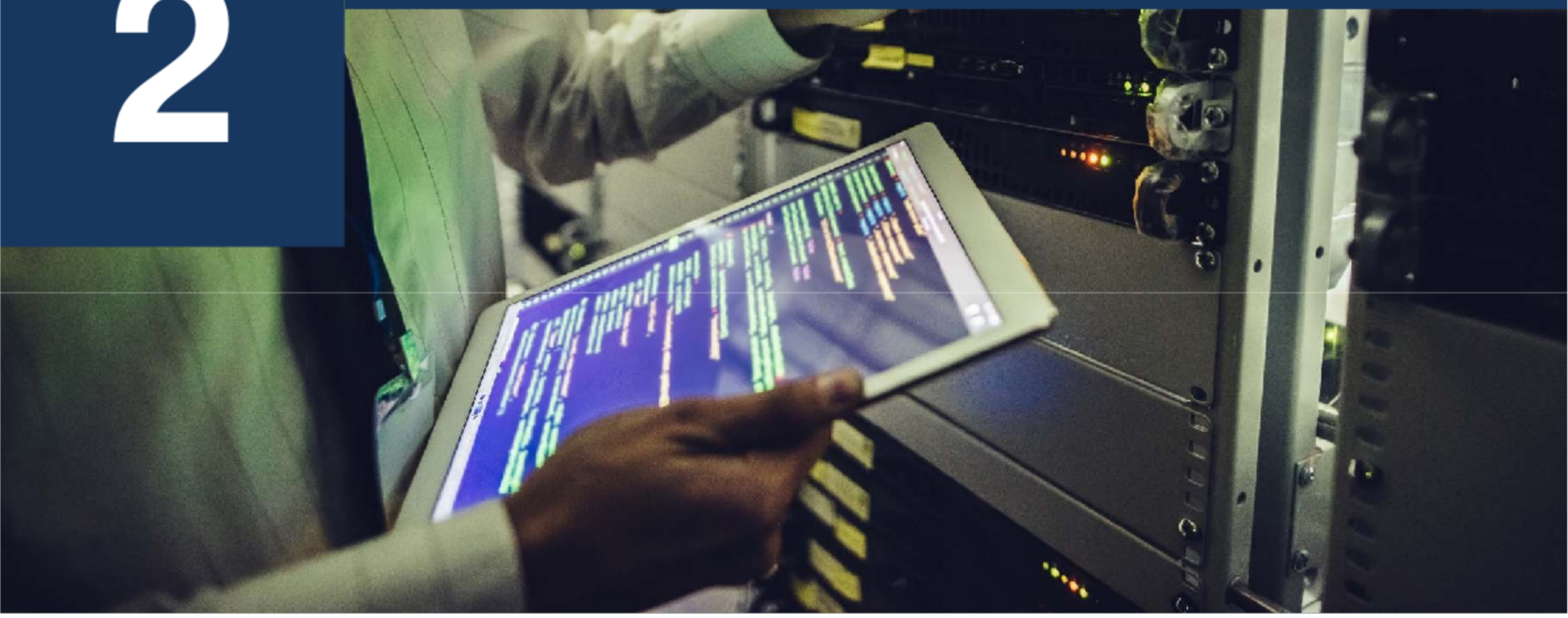
La presente Guía nacional de notificación y gestión de ciberincidentes se define como la referencia estatal respecto a la notificación de ciberincidentes (bien sea la comunicación de carácter obligatoria o potestativa), así como en lo relativo a la demanda de capacidad de respuesta a los incidentes de 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



2. OBJETO

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 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	Sujeto al Esquema Nacional de Seguridad (ENS)	**CENTRO CRIPTOLÓGICO NACIONAL (CCN)**
		No Sujeto al Esquema Nacional de Seguridad (ENS)	**AUTORIDAD SECTORIAL**
Proveedor de Servicios Digitales	Sector privado	-	**SECRETARÍA DE ESTADO PARA EL AVANCE DIGITAL**
	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)**

Ilustración 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**

Ilustración 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



3. GESTIÓN DE INCIDENTE

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 considere 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

. GESTIÓN DE INCI

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:



SISTEMA DE VENTANILLA UNICA

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 la autoridad nacional competente:
   - Si afecta a la Defensa Nacional, al ESPDEFCERT
   - Si afecta a 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 MUY ALTA o CRÍTICA, al CCN-CERT
   - Si es un incidente de obligatorio reporte según el RD Ley 12/2018, a la autoridad nacional competente correspondiente.
     - **RGPD**: se remite 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 a 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 sujeto afectado para recabar datos del incidente.
   - **RGPD**: confirmación de notificación en portal AEPD.
   - **BDE**: envío de plantilla de notificación .XLS rellenada al BDE.
   - **PIC**: envío de plantilla de notificación .XLS rellenada al CNPIC.
   - **ENS**: envío de plantilla de notificación .DOC rellenada al CCN-CERT.
   - **NIS**: se remite la plantilla de notificación de la autoridad nacional competente.
4. El sujeto afectado comunica las 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).

Ilustración 3. Sistema de ventanilla única

4.2. REPORTE DEL INCIDENTE 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].

4.3. 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 (formulario de reporte o un buzón de correo electrónico). El buzón de correo genérico para la

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

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

notificación de incidentes es incidencias@incibe-cert.es. Las entidades afiliadas a RedIRIS accederán al servicio a través de 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, la información remitida a INCIBE-CERT preferiblemente se enviará por correo electrónico cifrado con la clave PGP correspondiente a cada uno de los buzones de este CERT[3].

4.4. REPORTE DE INCIDENTES A ESPDEF-CERT

La comunicación con ESPDEF-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/



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 *Ilustración 4. 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.

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

Contenido dañino	Sistema infectado	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit
	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.
	Malware dominio DGA	Nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por malware para contactar con un servidor de Mando y Control (C&C).
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.
	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.
	Ciberterrorismo	Uso de redes o sistemas de información con fines de carácter terrorista.
	Daños informáticos PIC	Borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

Ilustración 4. 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 *Ilustración 4. 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 5. Niveles de peligrosidad de un ciberincidente

A continuación se incluye la *Ilustración 6. 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
		Ciberterrorismo
		Daños informáticos PIC
MUY ALTO	Código dañino	Distribución de malware
		Configuración de malware
	Intento de intrusión	Ataque desconocido
	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)
		Malware dominio DGA
	Intento de intrusión	Compromiso de aplicaciones

	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 con privilegios
	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)
	Intrusión	Compromiso de cuenta sin privilegios
	Otros	Otros

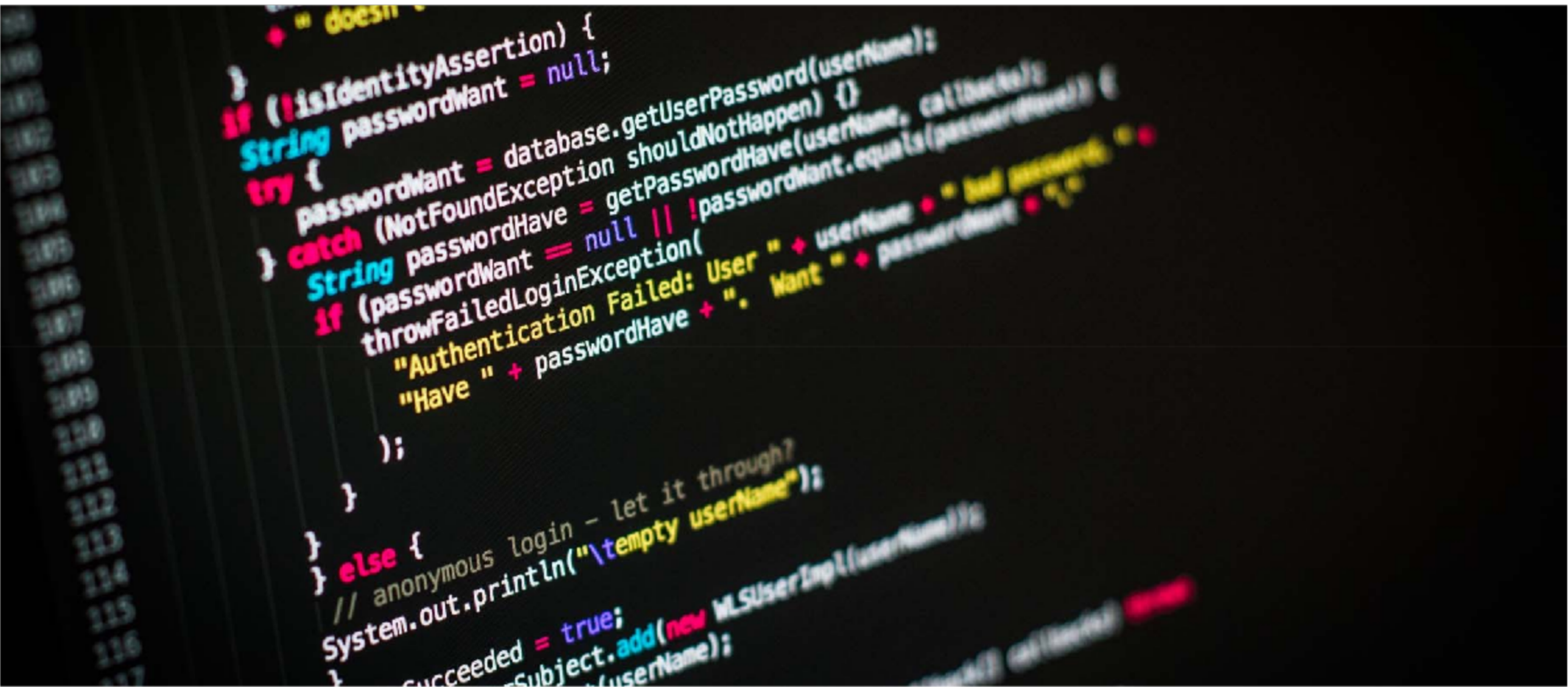
Ilustración 6. Criterios de determinación del Nivel de peligrosidad de un ciberincidente

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 peligrosidad: **CRÍTICO, MUY ALTO, ALTO**, **MEDIO, BAJO o SIN IMPACTO.**



Ilustración 7. Niveles de impacto de un ciberincidente

A continuación, se incluye la *Ilustración 8. 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 PELIGROSIDAD 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 30 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 10 y 30 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 10 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.

Ilustración 8. 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.**

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. El uso de este método de notificación será el preferente en la comunicación con el CSIRT. 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. Este identificador aparece en el campo “asunto” de las comunicaciones por correo electrónico y no debe modificarse o eliminarse ya que esto ralentizaría la gestión de las comunicaciones 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. Además, estas terceras partes, en especial, las autoridades competentes, podrán ponerse en contacto directo con el sujeto afectado.

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 *Ilustración 9. Información mínima 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.

Qué notificar	Descripción
Asunto	Frase que describe de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
Descripción	Describir con detalle lo sucedido.

Afectado	Indicar si el afectado es una empresa o un particular.
Fecha y hora del incidente[5]	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.
Taxonomía del incidente	Posible clasificación del ciberincidente en función de la taxonomía descrita. Se especificará: clasificación y tipo de incidente.
Recursos afectados	Indicar la información técnica sobre el número y tipo de activos afectados por el ciberincidente, incluyendo direcciones IP, sistemas operativos, aplicaciones, versiones…
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.
Contramedidas	Actuaciones realizadas para resolver el ciberincidente hasta el momento de la notificación a la autoridad competente o CSIRT de referencia.
Impacto	Impacto estimado en la entidad, en función del nivel de afectación del ciberincidente.
Adjuntos	Incluir documentos adjuntos que puedan aportar información que ayude 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

Ilustración 9. Información mínima a notificar en un ciberincidente a la autoridad competente

6.5. 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.

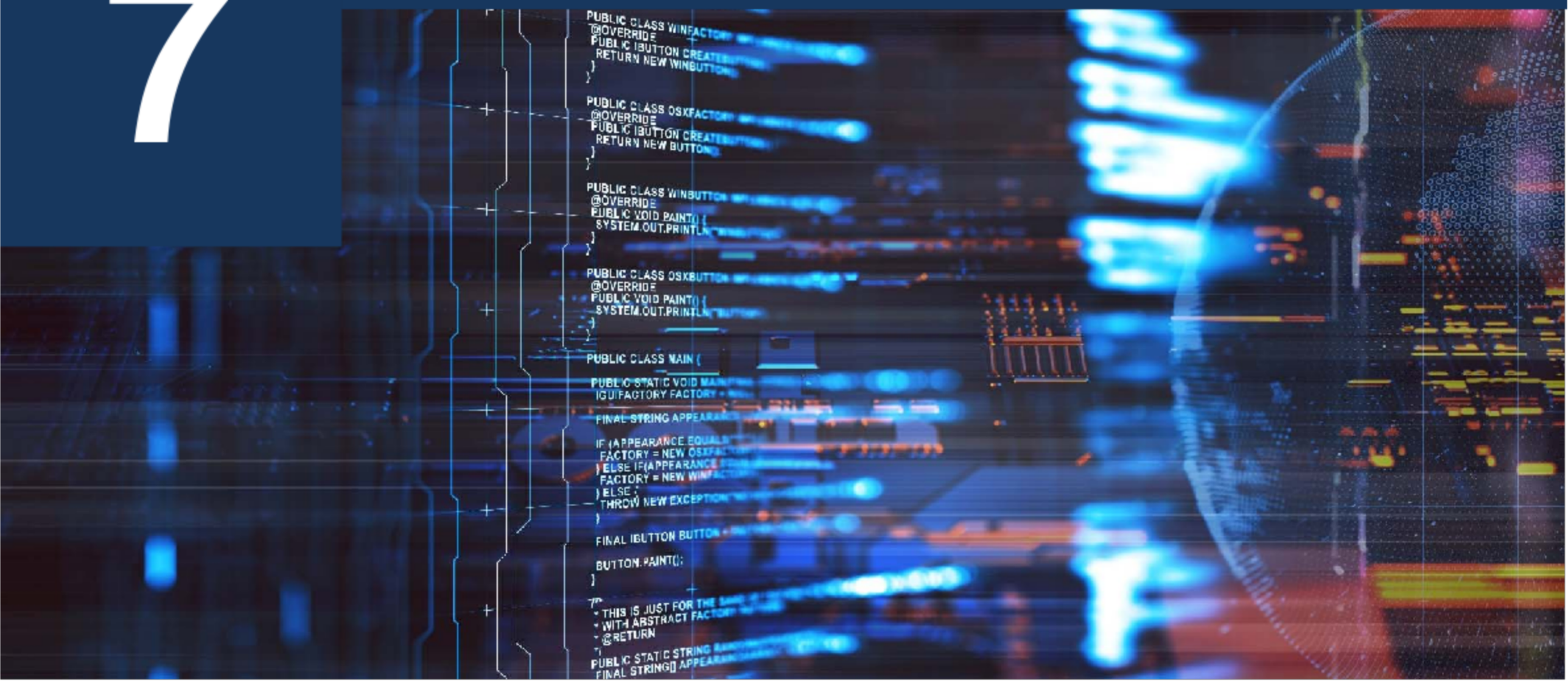
La tabla siguiente muestra los diferentes estados que puede tener un ciberincidente, en un instante dado, detallando los distintos tipos de cierre.

[5] Indicando la zona horaria en formato UTC.

Estado	Descripción
Cerrado (Resuelto y sin respuesta)	No hay respuesta por parte del organismo afectado en un periodo determinado.
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)	Pasado un periodo de 60 días, si el ciberincidente no ha sido cerrado por el organismo afectado, es cerrado por el CSIRT de referencia, 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.

Ilustración 10. Estados de los ciberincidentes

7 GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD



Se conocen 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 11. 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 identificar o detectar un ciberincidente 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 *triage* 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.

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.
- 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 evolución 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

Ilustración 12

8.2. MÉTRICAS DE EFICACIA

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

Ilustración 13

8.3. MÉTRICAS DE EFICIENCIA

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

Ilustración 14

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
	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	
		Objeto	0%

	Caracterización	Umbral amarillo	5%
		Umbral rojo	20%
		Frecuencia medición	Trimestral
		Frecuencia reporte	Anual

Ilustración 15

9 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.

9.1. 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).

9.1.1. 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 *Ilustración 5. Niveles de peligrosidad de un ciberincidente,* en la que se asigna un nivel de peligrosidad determinado en función de la clasificación del incidente.

9.1.2. Notificación obligatoria en función del nivel 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 *Ilustración 8. 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.

9.2. CONTENIDOS DE LA NOTIFICACIÓN E INFORMES

9.2.1. Notificación del ciberincidente

La NOTIFICACIÓN DEL INCIDENTE es una comunicación entre el operador y el CNPIC a través de su CSIRT de referencia, consistente en poner en conocimiento y alertar de la existencia de un ciberincidente que se hubiere producido en las redes o sistemas de información que soportan los servicios esenciales prestados por las infraestructuras del operador.

Esta comunicación podrá llevarse a cabo, si es necesario, a través de llamada telefónica o correo electrónico a los puntos de contacto facilitados por el CNPIC y el CSIRT de referencia. La notificación aportará los datos de los que disponga el operador en el momento inicial, tomando como referencia los campos de la tabla CONTENIDOS MÍNIMOS A NOTIFICAR contenida en este anexo. Esta información incluirá, entre otros datos, información que permita determinar cualquier efecto transfronterizo del incidente.

9.2.2. Informes del ciberincidente

El INFORME DEL INCIDENTE es una comunicación entre el operador y el CNPIC a través de su CSIRT de referencia, consistente en la aportación por escrito de la mayor cantidad posible de datos requeridos acerca del ciberincidente que se hubiere producido en las redes o sistemas de información que soportan los servicios esenciales prestados por las infraestructuras del operador. Esta información se actualizará con los datos disponibles en cada momento mediante la elaboración de sucesivos informes.

La comunicación se realizará siempre por escrito mediante el uso de correo electrónico o herramienta proporcionada por el CSIRT de referencia del operador. El informe aportará los datos actualizados de los que disponga el operador, tomando la estructura de la tabla CONTENIDOS MÍNIMOS A NOTIFICAR contenida en este anexo.

Para ello, los operadores afectados por un incidente con obligatoriedad de reporte remitirán, como mínimo, y en tiempo y forma, los informes inicial, adicional y final previstos en este anexo, aportando todos aquellos informes adicionales intermedios que se consideren necesarios por el CNPIC o el operador.

9.3. CONTENIDOS MÍNIMOS A NOTIFICAR

Una vez detectado un incidente, la notificación del mismo y la elaboración de los informes que sean pertinentes se realizará mediante una comunicación de datos e informaciones de interés al CNPIC a través del CSIRT de referencia de acuerdo a lo contemplado en la *Ilustración 16. Contenidos mínimos a notificar en el ámbito PIC*

Qué notificar	Descripción
Asunto	Frase que describe de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
Operador	Denominación del operador.
Sector estratégico	Energía, transporte, financiero, etc.
Descripción	Describir con detalle lo sucedido.
Afectado	Indicar si el afectado es una empresa o un particular.

Fecha y hora del incidente[6].	Indicar con la mayor precisión posible cuándo ha ocurrido el ciberincidente.
Fecha y hora de detección	Indicar con la mayor precisión posible cuándo se ha detectado el ciberincidente.
Taxonomía del incidente	Posible clasificación del ciberincidente en función de la taxonomía descrita. Se especificará: clasificación y tipo de incidente.
Recursos afectados	Indicar la información técnica sobre el número y tipo de activos afectados por el ciberincidente, incluyendo direcciones IP, sistemas operativos, aplicaciones, versiones…
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.
Contramedidas	Actuaciones realizadas para resolver el ciberincidente hasta el momento de la notificación a la autoridad competente, a través del CSIRT de referencia.
Impacto	Impacto estimado en la entidad, en función del nivel de afectación del ciberincidente.
Adjuntos	Incluir documentos adjuntos que puedan aportar información que ayude 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
Nivel de Peligrosidad	Especificar el nivel de peligrosidad asignado a la amenaza. Consultar *Ilustración 5. Niveles de peligrosidad de un ciberincidente*
Nivel de Impacto	Especificar el nivel de impacto asignado al incidente. Consultar *Ilustración 7. Niveles de impacto de un ciberincidente*
Estado actual del ciberincidente	Estado de la investigación técnica, legal, daños reputacionales, etc.
Extensión geográfica	Local, autonómico, nacional, supranacional, etc.
Impacto económico estimado	Costes hasta el momento, y coste estimado en relación a las tareas necesarias.
Daños reputacionales	Afectación a la imagen corporativa del operador.
Medios necesarios para la resolución (JP)	Capacidad empleada en la resolución del incidente en Jornadas-Persona.
Organismos involucrados en la investigación	AGPD, CNN-CERT, INCIBE-CERT, etc.

[6] Indicando la zona horaria en formato UTC.

Se requiere actuación de FFCCSE	Si / No - ¿Cuál?

Ilustración 16. Contenidos mínimos a notificar en el ámbito PIC

9.4. VENTANA TEMPORAL DE REPORTE Y REMISIÓN DE INFORMES

Todos aquellos operadores obligados a notificar un incidente al amparo de este anexo deberán realizar esta comunicación de acuerdo a un marco temporal de referencia expresado en la *Ilustración 17. Ventana de reporte en el ámbito PIC*

NIVEL DE PELIGROSIDAD O IMPACTO	VENTANA DE REPORTE Y REMISIÓN DE INFORMES					
	Notificación del incidente		Informe del incidente			
	CARÁCTER	ESPACIO TEMPORAL DE NOTIFICACIÓN	CARÁCTER	ESPACIO TEMPORAL DE REMISIÓN DEL INFORME		
				Inicial	Adicional	Final
CRÍTICO	OBLIGATORIO	INMEDIATA	OBLIGATORIO	INMEDIATO	48 HORAS	20 DÍAS LABORALES
MUY ALTO		12 HORAS		48 HORAS	72 HORAS	40 DÍAS LABORALES
ALTO		48 HORAS		96 HORAS	POTESTATIVO	POTESTATIVO
MEDIO	POTESTATIVO	-	POTESTATIVO	-	-	-
BAJO		-		-	-	-

Ilustración 17. Ventana de reporte en el ámbito PIC

9.5. COMUNICACIÓN AL MINISTERIO FISCAL Y OTROS ORGANISMOS

La Oficina de Coordinación Cibernética (OCC) del Ministerio del Interior, integrada en la estructura del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), y dependiente funcionalmente del Secretario de Estado de Seguridad (SES), es el organismo competente para coordinar e impulsar la respuesta operativa por parte de las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE), y especialmente por sus unidades tecnológicas.

Por todo ello, 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.

Asimismo, la OCC está en contacto permanente con organismos nacionales e internacionales, con los cuales realiza intercambios de información estratégica y

operativa para la toma de consciencia situacional del estado de las ciberamenazas y la mejora del nivel de ciberseguridad a nivel global.

9.6. FLUJOGRAMAS DE REPORTE Y DE 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.

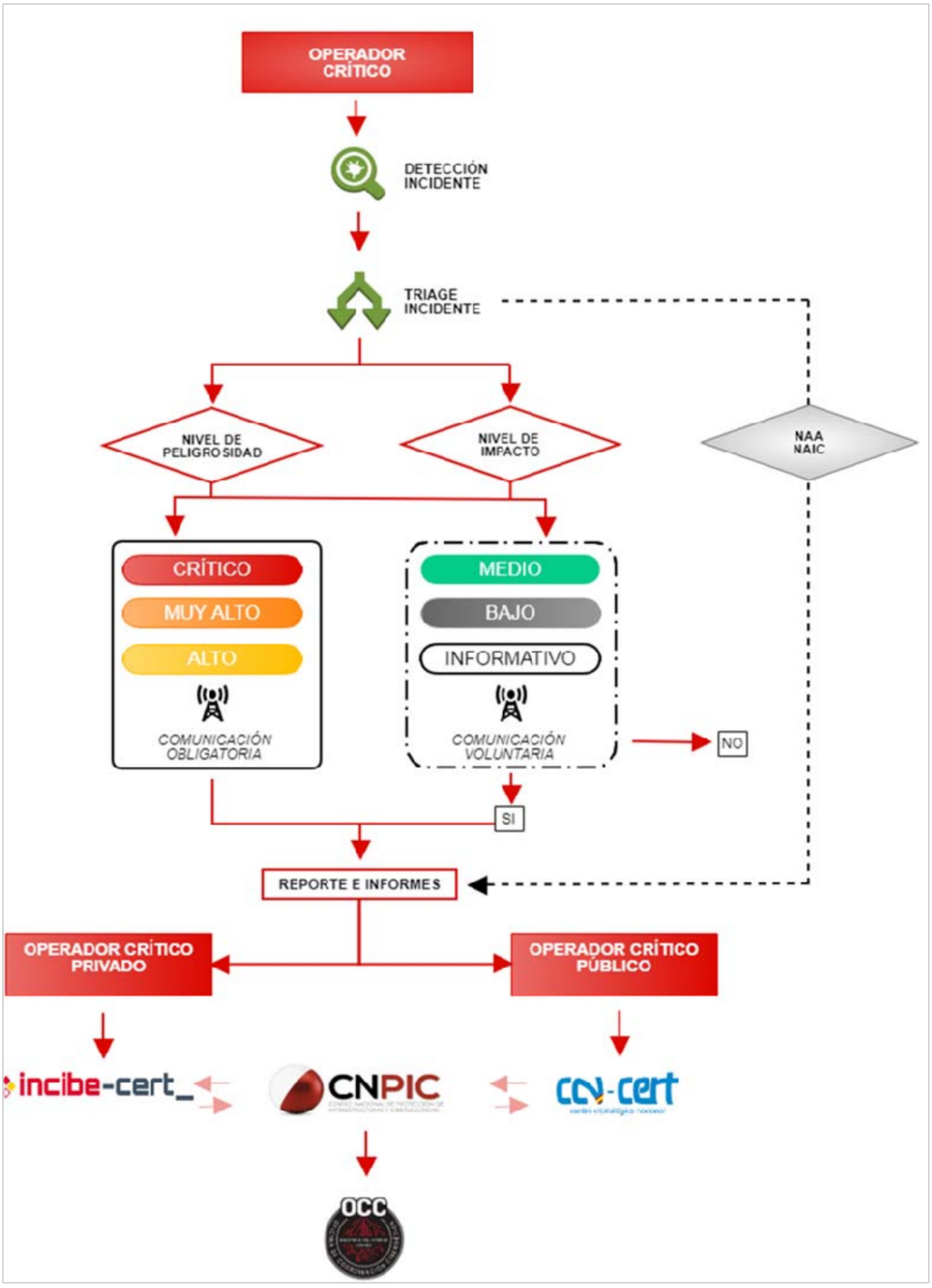


Ilustración 18. Flujograma de gestión y notificación en el ámbito PIC.

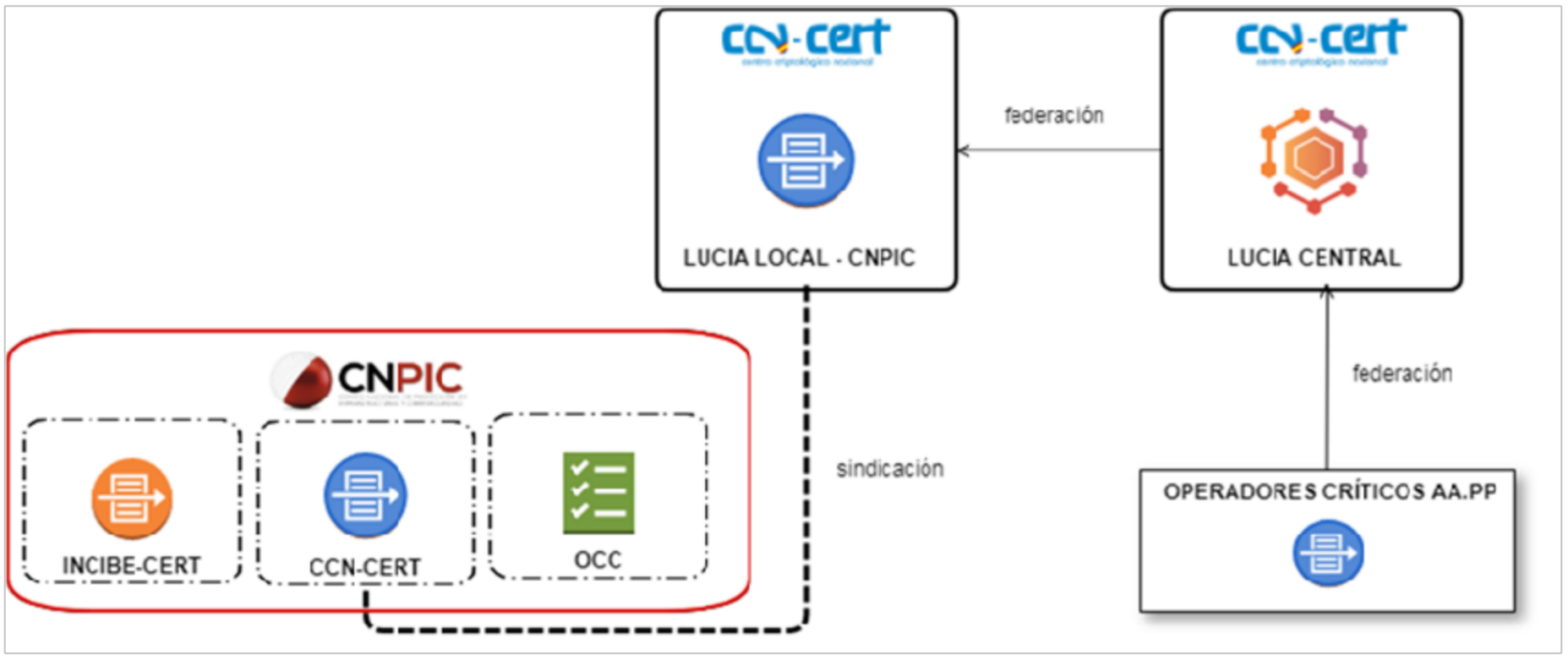


Ilustración 19. Flujograma de reporte de incidentes de Operadores Críticos de del Sector Público.

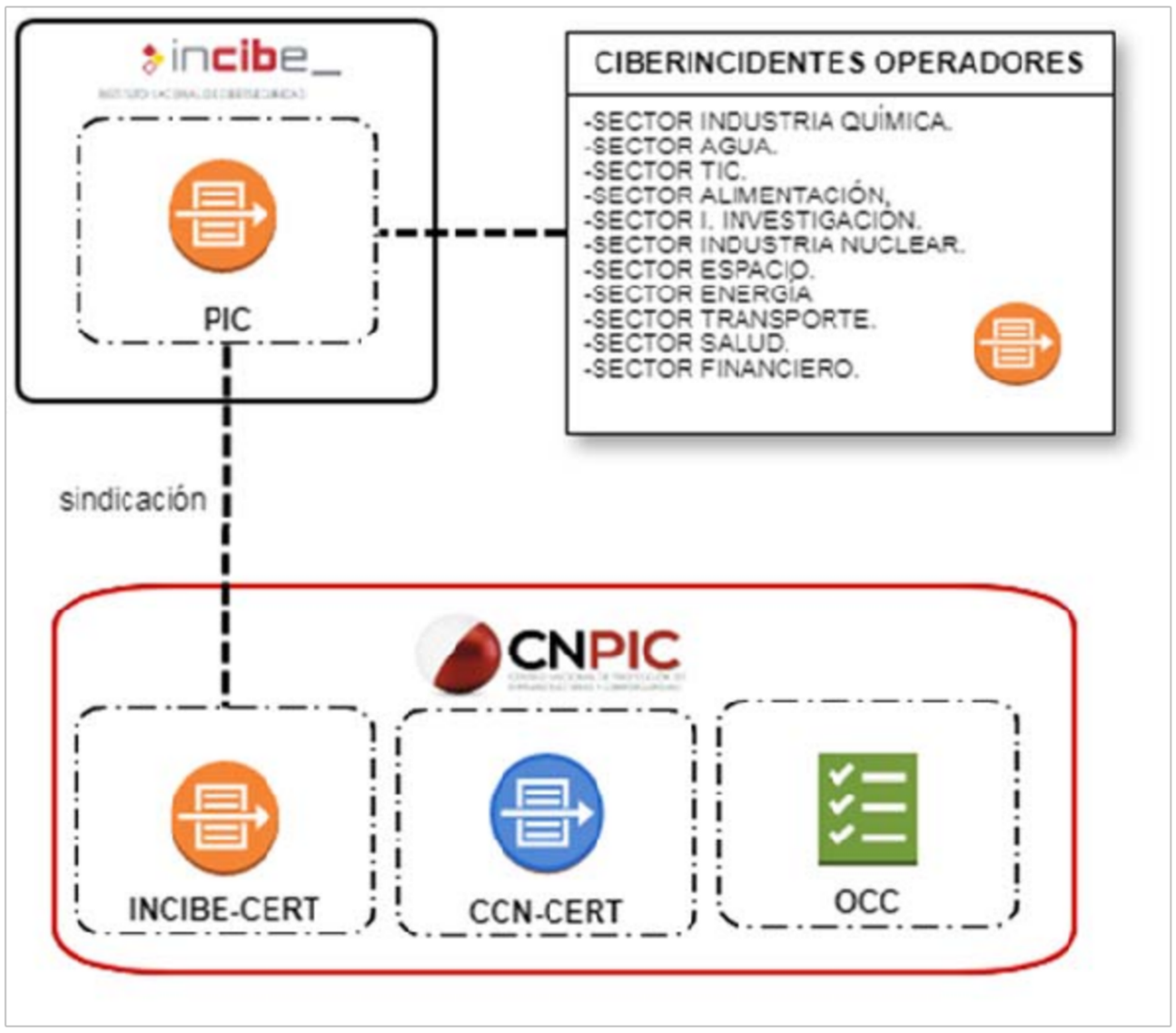


Ilustración 20. Flujograma de reporte de incidentes de Operadores Críticos del Sector Privado.

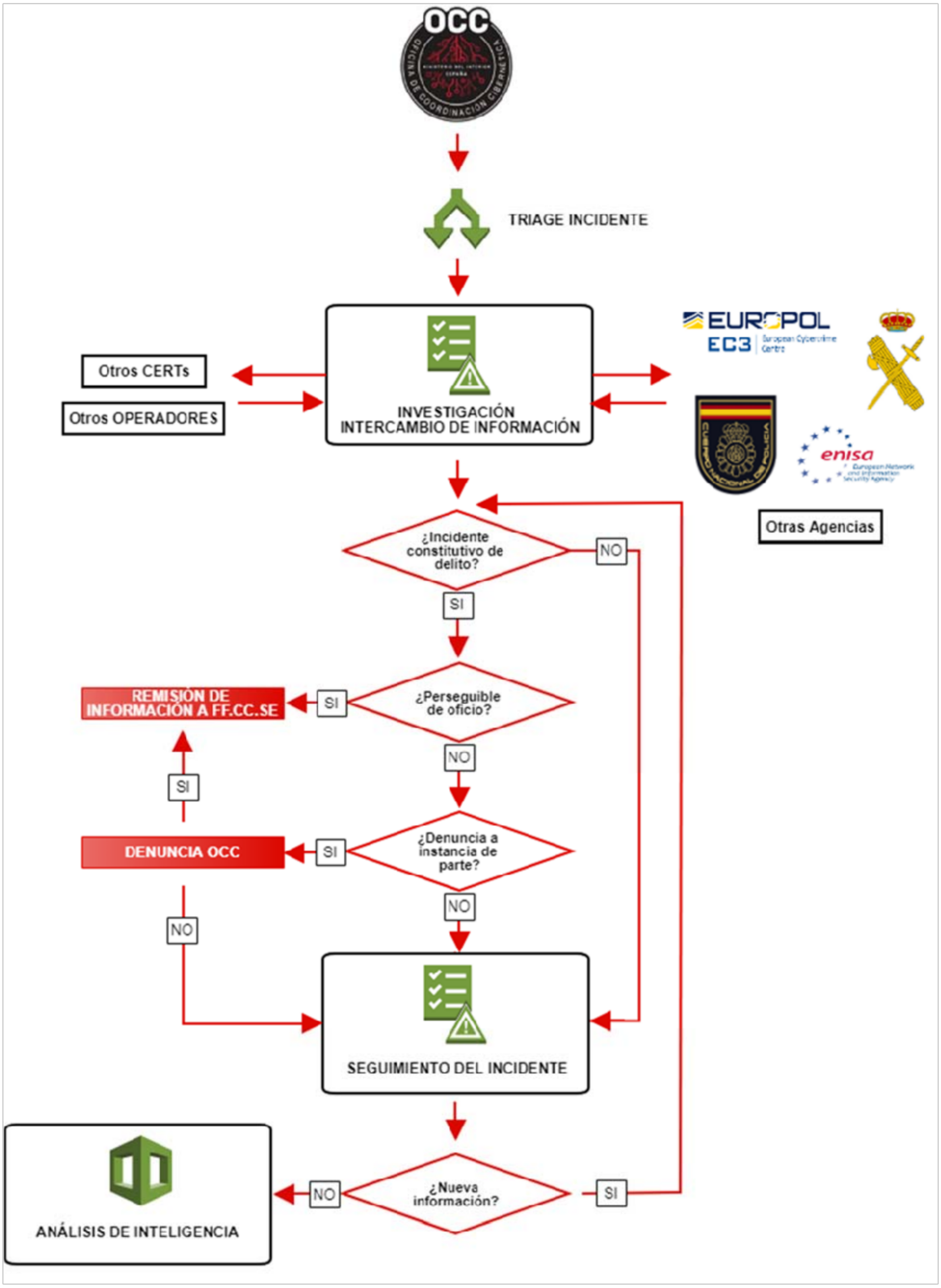
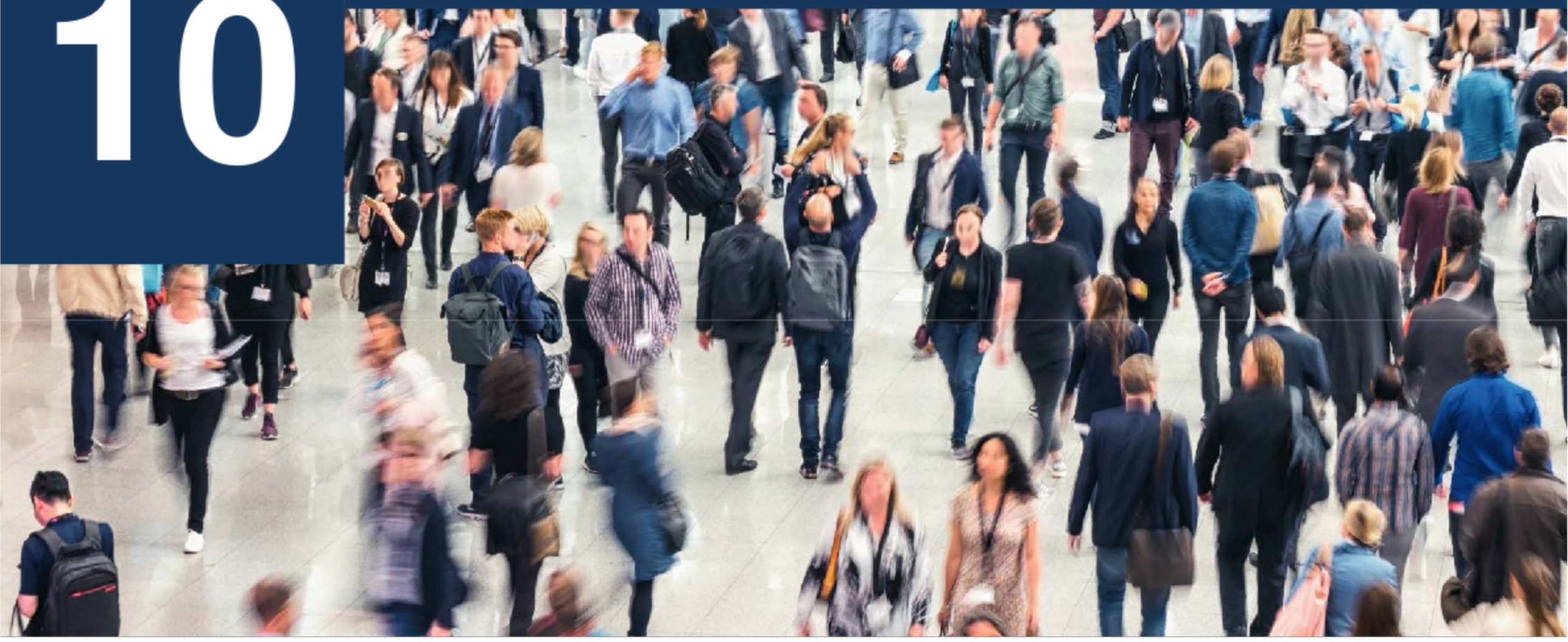


Ilustración 21. Flujograma de respuesta operativa en el ámbito PIC.

10 ANEXO 2. ORGANISMOS DE REFERENCIA



El **Centro Criptológico Nacional (CCN)** es el organismo responsable de coordinar la acción de los diferentes organismos del Sector Público 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.

El **CCN-CERT** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del **Centro Criptológico Nacional**. Este servicio se creó a finales del año 2006 como CERT gubernamental español, y sus funciones quedan recogidas en el

capítulo VII del RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (modificado por el RD 951/2015). Este texto legal, en su artículo 37 señala los servicios que el CCN-CERT ya prestaba desde su constitución (en parte recogidos en el RD 421/2004 de regulación del CCN).

El artículo 36 del RD 3/2010 establece la obligación de notificar incidentes severos en su comunidad de actuación. Este artículo ha sido desarrollado por la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad publicada en BOE nº 95 de 18 de Abril de 2018.

La S.M.E. **Instituto Nacional de Ciberseguridad de España** M.P., S.A. **(INCIBE)** es una sociedad dependiente de la Secretaría de Estado para el Avance Digital (SEAD) y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional.

INCIBE-CERT es el equipo de respuesta a ciberincidentes de INCIBE y el CERT[7] o CSIRT[8] Nacional competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en España para la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre, siendo –por tanto- el CSIRT de referencia para **ciudadanos y entidades de derecho privado** así como para todos aquellos **proveedores de servicios digitales** no incluidos en la citada Ley.

Adicionalmente, el INCIBE-CERT es operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiere a la gestión de incidentes que afecten a los **operadores críticos**[9].

[7] Del inglés, Computer Emergency Response Team. Sinónimo de CSIRT

[8] Del inglés, Computer Security Incident Response Team. Sinónimo de CERT

[9] Artículo 11 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Por último, el INCIBE-CERT es el equipo de respuesta a incidentes para instituciones afiliadas a **RedIRIS** (la red académica y de investigación española).

El **Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)** es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las Infraestructuras Críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior. El CNPIC depende de la Secretaría de Estado de Seguridad (SES), máxima responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio del Interior.

El CNPIC fue creado en el año 2007, mediante Acuerdo de Consejo de Ministros de 2 de noviembre, siendo sus competencias reguladas por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las Infraestructuras Críticas; y por el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las Infraestructuras Críticas.

La **Oficina de Coordinación Cibernética (OCC)** es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad, creado mediante Instrucción del Secretario de Estado de Seguridad 15/2014, de 19 de noviembre, estando sus funciones reguladas por el Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. Depende funcionalmente de la Secretaría de Estado de Seguridad y orgánicamente del CNPIC.

La OCC ejerce como canal específico de comunicación entre los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad, desempeñando la coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes. Además, es el punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo establecido por la

Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información.

El **Mando Conjunto de Ciberdefensa** (MCCD) es el responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otras que pudiera tener encomendadas, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional. El MCCD fue creado el 19 de febrero mediante la publicación de la Orden Ministerial 10/2013 y depende del Jefe de Estado Mayor de la Defensa (JEMAD).

El **ESPDEF-CERT** es el CERT del **Mando Conjunto de Ciberdefensa** (MCCD) y tiene como ámbito de actuación 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.

11 ANEXO 3. 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:

11.1. DE CARÁCTER GENERAL

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.
- 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.

11.2. 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.

11.3. 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.

11.4. 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).

12 ANEXO 4. 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.

- **Propaganda:** Difusión o divulgación de información, ideas u opiniones de carácter político, religioso, comercial, etc., con la intención de que alguien actúe de una determinada manera, piense según unas ideas o adquiera un determinado producto.

- **Reclutamiento:** Proceso de captación de personas para la consecución de actos ilícitos.

- **Financiación**: Acción de dotar de dinero y de crédito a una empresa, organización o individuo.

CONTENIDO DAÑINO

- **Malware (código dañino)**: La palabra malware deriva de los términos Malicious y Software. 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**: Un virus es un 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 gusanos.

- **Gusano**: Un gusano es un malware similar a un virus, y en ocasiones se considera una subclasificación del mismo. Exactamente igual que un virus, un gusano se difunde de ordenador a ordenador. La principal característica que distingue a un gusano de un virus es el hecho de que el gusano tiene la capacidad de diseminarse sin la necesidad de una acción humana. Un gusano normalmente explota vulnerabilidades del Sistema Operativo o de contraseñas débiles para diseminarse a otros ordenadores.

- **Troyano**: Es un 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)**: Es un 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**: Es un 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:** Es una 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, que no esté plenamente identificado su destino/origen, así como la legitimidad del mismo.

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):** Consiste en el uso de técnicas para la recolección de información acerca de la infraestructura y subdominios de un objetivo, realizado mediante una transferencia de información completa (AXFR) o incremental (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 usado para detectar y analizar posibles vulnerabilidades.

- **Ingeniería social:** Se definen así a todas aquellas 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:** Consiste en la suplantación de la identidad mediante la que el atacante, de forma masiva, trata de obtener información relevante de usuarios para uso dañino. Para ello se emplean métodos de ingeniería social.

- **Spear Phishing**: Se trata de una variante del Phishing mediante la que el atacante focaliza su actuación sobre un objetivo concreto.

INTRUSIONES

- **Explotación**: Consiste en 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**: Es un 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)**: Es un 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 click, 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:** Consiste en una tipología de ataque a sitios web en el que se implementa un cambio en la apariencia visual de web. Para ello suelen emplearse Inyecciones SQL o accesos ilegítimos a servidores FTP.

- **Inclusión de ficheros (RFI y LFI):** Vulnerabilidad que permite a un atacante 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:** Se trata del 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:** Consiste en un 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 combinaciones alfanuméricas, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

- **Descifrado de contraseña:** Proceso de transformar una contraseña protegida por contraseña, en una contraseña en texto claro y legible.

- **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 alfanuméricos, 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:** Consiste en una serie de técnicas que provocan la inoperatividad de un servicio o un recurso. El procedimiento consiste en la implementación masiva de peticiones a un servidor, lo que genera una sobrecarga del servicio y el posterior colapso del mismo al no poder éste atender la gran cantidad de solicitudes que le llegan.

- **DDoS (Denial distributed of Service) o Denegación distribuida de servicio**: Se trata de una 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:** Se trata de 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:** Se trata de incidentes 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:** Procedimientos usados para la realización de ataque DoS o DDoS.

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 autorizadas por la dirección o negociado competente.

- **Suplantación de identidad**: Técnica de simulación de mercantiles o particulares.

- **Violación de 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 queda perjudicado.

VULNERABILIDADES

- **Tecnología vulnerable**: Conocimiento por parte de los administradores de tecnologías, servicios o redes, de vulnerabilidades presentes en estas, no pudiendo aplicar parches de seguridad por no disponer de ellos, o no ser posible la implementación en el estado actual del sistema.

- **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):** Este concepto se define como 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 de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

- **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.

- **OpenPGP:** Pretty Good Privacy o PGP es un programa cuya finalidad es proteger la información distribuida a través de Internet 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):*** Virtual Network Computing. Programa de software libre basado en una estructura cliente-servidor que permite observar las acciones del ordenador servidor remotamente a través de un ordenador cliente.

- **SNMP *(Simple Network Management Protocol):*** Protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

- **Redis:** Motor de base de datos en memoria, basado en el almacenamiento en tablas de hashes.

- **ICMP:** Es el sub protocolo de control y notificación de errores del Protocolo de Internet.

- **Copia de seguridad limpia:** Punto de restauración de un sistema de la que se tiene la seguridad de no estar infectado con ninguna vulnerabilidad.

CON LA COLABORACIÓN DE:

GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES

GOBIERNO
DE ESPAÑA