Seguridad en los Sistemas Informáticos
Tema 4: Notificación y gestión de ciberincidentes

Grado en Ingeniería Informática

Departamento de Ingeniería Informática
Universidad de Cádiz

Curso 2024–2025

Índice

Organismos de referencia

El Gobierno de España atribuye las competencias en materia de ciberseguridad a diversos organismos:

- CCN-CERT: Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- INCIBE-CERT: Instituto Nacional de Ciberseguridad de España.
- CNPIC: Centro Nacional de Protección de Infraestructuras y Ciberseguridad.
- ESPDEF-CERT: Mando Conjunto de Ciberdefensa. Ámbito de redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas, y otros que afecten a la Defensa Nacional.

Guía Nacional de Notificación y Gestión de Ciberincidentes (I)

- La Guía Nacional de Notificación y Gestión de Ciberincidentes fue aprobada por el Consejo Nacional de Ciberseguridad en enero de 2019.
- Esta guía fue actualizada en febrero de 2020.
- Es la referencia estatal sobre la notificación de ciberincidentes.
- También es 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.
- Se encuentra alineada con las normativas españolas y europeas.
- **Nota**: el contenido de esta presentación ha sido extraído de esta guía.

Guía Nacional de Notificación y Gestión de Ciberincidentes (II)

- Esta guía está dirigida a:
  - Responsables de Seguridad de la Información (RSI), como Responsables Delegados.
  - Equipos de respuesta a ciberincidentes o *Computer Security Incident Response Team* (CSIRT).
  - Centros de operaciones de ciberseguridad (SOC) internos a las organizaciones.
  - Administradores de Sistemas de Información y/o Comunicación.
  - Personal de Seguridad.
  - Personal de apoyo técnico.
  - Gestores del ámbito de la ciberseguridad.
- Proporciona a los RSI las directrices para el cumplimiento de las obligaciones de reporte de incidentes de ciberseguridad.

Guía Nacional de Notificación y Gestión de Ciberincidentes (III)

- 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 de:
  - Alcance de la norma.
  - Niveles de peligrosidad.
  - Niveles de impacto.
- La notificación de incidentes de ciberseguridad tendrá un carácter potestativo y voluntario para los ciudadanos y empresas no incluidos en el ámbito de protección de infraestructuras críticas, del sector público o del Real Decreto-ley 12/2018.

Metodología de reporte: ventanilla única de notificación (I)

Fuente: Gobierno de España. Guía Nacional de Notificación y Gestión de Ciberincidents. 2019.

Metodología de reporte: ventanilla única de notificación (II)

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 ESPDEF-CERT.
   - 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.

Metodología de reporte: ventanilla única de notificación (III)

3. El Organismo receptor implicado o autoridad nacional competente se pone en contacto con el sujeto afectado para recabar datos del incidente.
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).

Metodología de reporte: reportes (I)

Reporte de incidentes a CCN-CERT

- Canal preferente: a través de LUCIA (`https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia.html`).
- Canal secundario: incidentes@ccn-cert.cni.es. Mensajería cifrada con la clave PGP (`https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html`).

Reporte de incidentes a INCIBE-CERT

- Formulario de reporte.
- Correo electrónico:
  - incidencias@incibe-cert.es (en general).
  - iris@incibe-cert.es (para entidades afiliadas a RedIRIS).
  - pic@incibe-cert.es (para operadores de servicios esenciales).

  Mensajería cifrada con la clave PGP del CERT correspondiente (`https://www.incibe-cert.es/sobre-incibe-cert/claves-publicas-pgp`).

Metodología de reporte: reportes (II)

Reporte de incidentes a ESPDEF-CERT

- Correo electrónico mediante mensajería cifrada con la clave pública PGP (`http://www.emad.mde.es/CIBERDEFENSA/ESPDEF-CERT/`).
- En caso de urgencia, podrá contactarse con el Oficial de Servicio.

Taxonomía de los ciberincidentes

Los ciberincidentes se clasifican en las siguientes categorías:

- Contenido abusivo.
- Contenido dañino.
- Obtención de información.
- Intento de intrusión.
- Intrusión.
- Disponibilidad.
- Compromiso de la información.
- Fraude.
- Vulnerable.
- Otros.

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, entre otros.

Contenido dañino (I)

Sistema infectado

- Sistema infectado con *malware*.
- Ej: Sistema, ordenador o teléfono móvil infectado con un *rootkit*.

Servidor C&C (Mando y Control)

- Conexión con servidor de mando y control mediante *malware* o sistemas infectados.

Distribución de *malware*

- Recurso usado para distribución de *malware*.
- Ej: recurso de una organización empleado para distribuir *malware*.

Contenido dañino (II)

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.

Obtención de información

Escaneo de redes (*scanning*)

- Envío de peticiones a un sistema para descubrir posibles debilidades.
- Se incluyen también procesos de comprobación 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 (I)

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, etc. Destacamos el *cross site scripting* (XSS).
- Un XSS es un tipo de explotación que permite a los atacantes implantar *scripts* maliciosos en un sitio web para ejecutar dicho *script* en el navegador de un usuario con la finalidad de dirigirlo hacia otro sitio web, robar sus credenciales, o realizar cualquier otro tipo de acción maliciosa.

Intento de intrusión (II)

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 un *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 (CPD).

Disponibilidad (I)

Sabotaje

- Sabotaje físico.
- Ej: cortes de cableados de equipos o incendios provocados.

Interrupciones

- Interrupciones por causas ajenas.
- Ej: desastre natural.

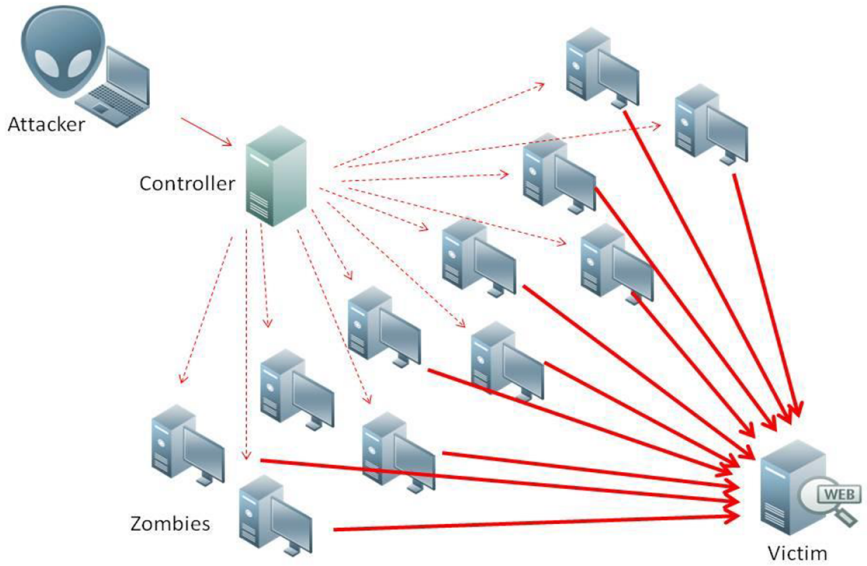
DoS (Denegación de servicio)

- Ataque de denegación de servicio.
- Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.

Disponibilidad (II)

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.



Fuente: `https://www.xataka.com/basics/que-es-un-ataque-ddos-y-como-puede-afectarte`

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 (I)

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.

Fraude (II)

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 (I)

Criptografía débil

- Servicios accesibles públicamente que puedan presentar criptografía débil.
- Ej: servidores web susceptibles de ataques POODLE/FREAK.

Amplificador DDoS

- Servicios accesibles públicamente empleados para la reflexión o amplificación de ataques DDoS.
- Ej: DNS *open-resolvers* o Servidores NTP con monitorización *monlist*.

Vulnerable (II)

Servicios con acceso potencial no deseado

- *Telecomunication Network* (Telnet). Protocolo de red TCP/IP para establecer conexiones remotas con otros ordenadores, servidores, y dispositivos con un sistema compatible en el acceso mediante este sistema de comunicación: Telnet.
- *Remote Desktop Protocol* (RDP). Permite que el escritorio de un equipo informático sea controlado a distancia por un usuario remoto.
- *Virtual Network Computing* (VNC). Es un *software* que permite ver la pantalla del ordenador servidor y controlarlo en uno o varios ordenadores clientes sin importar qué sistema operativo pueda ejecutar el cliente o el servidor.

Vulnerable (III)

Revelación de información

- Acceso público a servicios en los que potencialmente pueda relevarse información sensible.
- Ej: SNMP o Redis.

Sistema vulnerable

- Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

Otros (I)

Ciberterrorismo

- Uso de redes o sistemas de información con fines de carácter terrorista.

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.

Otros (II)

Fuente:
`https://www.b-secure.co/recursos/infografias/pasos-de-las-amenazas-persistentes-avanzadas`

Otros (III)

Daños informáticos PIC

- Borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica.
- Una infraestructura crítica es todo aquel sistema físico o virtual que facilita funciones y servicios esenciales para apoyar a los sistemas a nivel social, económico, medioambiental y político. Un ejemplo de esta puede ser una central eléctrica.
- Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

Criterios para la notificación

- Para la notificación de los incidentes de ciberseguridad a la autoridad competente o CSIRT de referencia se utilizará como criterio de referencia el **nivel de peligrosidad** que se asigne a un incidente.
- El **nivel de impacto** en que se categorice un incidente podría aconsejar la comunicación del incidente.
- Cuando un determinado suceso pueda asociarse a más de un tipo de incidente, este se asociará a aquel que tenga un nivel de peligrosidad superior.

Nivel de peligrosidad del ciberincidente (I)

- 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.
- Los incidentes se asociarán a algunos de los niveles de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO.

Nivel CRÍTICO

- **Otros**: APT, ciberterrorismo y daños informáticos PIC.

Nivel de peligrosidad del ciberincidente (II)

Nivel MUY ALTO

- **Código dañino**: Distribución de *malware* y configuración de *malware*.
- **Intento de intrusión**: Ataque desconocido.
- **Intrusión**: Robo.
- **Disponibilidad**: Sabotaje e interrupciones.

Nivel de peligrosidad del ciberincidente (III)

Nivel ALTO

- **Contenido abusivo**: Pornografía infantil, contenido sexual o violento inadecuado.
- **Código dañino**: Sistema infectado, servidor C&C (Mando y Control) y *malware* dominio DGA.
- **Intrusión**: Compromiso de aplicaciones.
- **Disponibilidad**: DoS (Denegación de servicio) y DDoS (Denegación distribuida de servicio).
- **Compromiso de la información**: Acceso no autorizado a información, modificación no autorizada de información y pérdida de datos.
- **Fraude**: *Phishing*.

Nivel de peligrosidad del ciberincidente (IV)

Nivel MEDIO

- **Contenido abusivo**: Discurso de odio.
- **Obtención de información**: Ingeniería social.
- **Intento de intrusión**: Explotación de vulnerabilidades conocidas e intento de acceso con vulneración de credenciales.
- **Intrusión**: Compromiso de cuentas con privilegios.
- **Fraude**: Uso no autorizado de recursos, derechos de autor y suplantación.
- **Vulnerable**: Criptografía débil, amplificador DDoS, servicios con acceso potencial no deseado, revelación de información y sistema vulnerable.

Nivel de peligrosidad del ciberincidente (V)

Nivel BAJO

- **Contenido abusivo**: *Spam*.
- **Obtención de información**: Escaneo de redes (*scanning*) y análisis de paquetes (*sniffing*).
- **Intrusión**:Compromiso de cuenta sin privilegios.
- **Otros**: Otros.

Nivel de impacto del ciberincidente (I)

- 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.
  - En los individuos afectados.
- Los criterios para determinar el nivel de impacto son:
  - Impacto en la Seguridad Nacional o 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.

Nivel de impacto del ciberincidente (II)

- Los criterios para determinar el nivel de impacto son (cont.):
  - Pérdidas económicas.
  - Extensión geográfica afectada.
  - Daños reputacionales asociados.
- Los incidentes se asociarán a niveles de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO o SIN IMPACTO.

Nivel de impacto del ciberincidente (III)

Nivel 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 $>$ 30 días/pers.
- 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.

Nivel de impacto del ciberincidente (IV)

Nivel 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 resolverse entre 10 y 30 días/pers.
- Impacto económico entre el 0,07 % y el 0,1 % del P.I.B.
- Extensión geográfica superior a 4 CC.AA.
- Daños reputacionales a la imagen del país (marca España).
- Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.

Nivel de impacto del ciberincidente (V)

Nivel 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 resolverse entre 5 y 10 días/pers.
- Impacto económico entre el 0,03 % y el 0,07 % del P.I.B.
- 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.

Nivel de impacto del ciberincidente (VI)

Nivel 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 días/pers.
- Impacto económico entre el 0,001 % y el 0,03 % del P.I.B.
- Extensión geográfica superior a 2 CC.AA.
- Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).

Nivel de impacto del ciberincidente (VII)

Nivel BAJO

- Afecta a los sistemas de la organización.
- Interrupción de la prestación de un servicio.
- El ciberincidente precisa para resolverse menos de 1 día/pers.
- Impacto económico entre el 0,0001 % y el 0,001 % del P.I.B.
- Extensión geográfica superior a 1 CC.AA.
- Daños reputacionales puntuales, sin eco mediático.

Nivel SIN IMPACTO

- No hay ningún impacto apreciable.

Niveles con notificación obligatoria asociada

- Es obligatorio la notificación de todos aquellos incidentes que se categoricen con un nivel CRÍTICO (inmediata), MUY ALTO (12 horas) O ALTO (48 horas).
- 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.

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.
- En caso de no disponer de estas herramientas, se considerará válido el uso de correo electrónico.

Apertura del incidente (I)

- Tras recibir una notificación sobre un posible ciberincidente, el equipo técnico del CSIRT realiza un análisis inicial que determinará si debe ser gestionado.
- Esta apertura puede producirse por un:
  - Un reporte del afectado.
  - Una detección del CSIRT.
  - Por un tercero que reporta al CSIRT un incidente.
- Si aplica la gestión del ciberincidente:
  - Se registrará la información reportada.
  - Se asignarán una clasificación y unos valores iniciales de peligrosidad e impacto que serán comunicados al remitente.

Apertura del incidente (II)

- Posteriormente se indicarán las acciones necesarias para la resolución del ciberincidente.
- El CSIRT asignará a cada caso un identificador único que estará presente en el campo asunto de todas las comunicaciones relacionadas con el incidente.
- El CSIRT podrá comunicarse con el remitente o con terceras partes para solicitar o intercambiar información adicional que agilice la resolución del problema.

Información a notificar (I)

Información mínima a notificar en un ciberincidente a la autoridad competente

- **Asunto**: Frase que describe de forma general el incidente.
- **Descripción**: Describir con detalle lo sucedido.
- **Afectado**: Indicar si el afectado es empresa o particular.
- **Fecha y hora del incidente**: Indicar cuándo ha ocurrido el ciberincidente.
- **Fecha y hora de detección del incidente**: Indicar cuándo se ha detectado el ciberincidente.
- **Taxonomía del incidente**: Posible clasificación y tipo de incidente en función de la taxonomía descrita.
- **Recursos afectados**: Indicar la información técnica sobre el número y tipo de activos afectados por el ciberincidente, incluyendo direcciones IP, S.O., aplicaciones, versiones.

Información a notificar (II)

Información mínima a notificar en un ciberincidente (cont.)

- **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.

Estados y valores de cierre (I)

- 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.

Estados y valores de cierre (II)

Estados de los ciberincidentes

- **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.

Estados y valores de cierre (III)

Estados de los ciberincidentes (cont.)

- **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.
- **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.

Gestión de incidentes de ciberseguridad (I)

- La gestión de incidentes de ciberseguridad es 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.

Fuente: Gobierno de España. Guía Nacional de Notificación y Gestión de Ciberincidents. 2020.

Gestión de incidentes de ciberseguridad (II)

Fase de preparación

- Fase inicial en la que toda entidad debe estar preparada para cualquier suceso que pudiera ocurrir.
- Debe tenerse en cuenta tres pilares fundamentales: las personas, los procedimientos y la tecnología.
- Los puntos más relevantes a tener en cuenta son:
  - Disponer de información actualizada de contacto.
  - Mantener las políticas y procedimientos actualizados.
  - Herramientas a utilizar en todas las fases.
  - 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.
  - Ejecución de ciberejercicios a fin de entrenar las capacidades y procedimientos técnicos, operativos, de gestión y coordinación.

Gestión de incidentes de ciberseguridad (III)

Fase de identificación

- El objetivo es identificar o detectar un ciberincidente; es importante realizar una monitorización lo más completa posible.
- Una correcta identificación se basa en:
  - 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.

Gestión de incidentes de ciberseguridad (IV)

Fase de contención

- Tras la identificación de un ciberincidente, la máxima prioridad es contener su impacto en la organización para evitar la propagación a otros sistemas o redes.
- Debe realizarse el *triage* (evaluar toda la información disponible para 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.

Gestión de incidentes de ciberseguridad (V)

Fase de contención (cont.)

- Se debe:
  - Documentar todas las acciones realizadas, utilizando alguna herramienta de notificación de incidentes.
  - Recopilar evidencias para realizar un análisis forense de sistemas afectados y preservarlas manteniendo la cadena de custodia.
  - Aplicar medidas de contención a corto plazo, que permitan controlar el impacto temporalmente: desconexión de equipos de la red, filtrado o aislamiento a nivel de red, redirección o bloqueo de tráfico hacia el exterior.
  - Identificar y aplicar medidas de contención a largo plazo: aplicación de parches de seguridad específicos, eliminar procesos sospechosos, eliminar cuentas de usuario desconocidas, cambio de contraseñas de cuentas comprometidas, aplicar filtrados adicionales a nivel de red.

Gestión de incidentes de ciberseguridad (VI)

Fase de mitigación

- 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.

Gestión de incidentes de ciberseguridad (VII)

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.
- Debe definirse un periodo de tiempo con medidas adicionales de monitorización de los sistemas puestos en producción.

Gestión de incidentes de ciberseguridad (VIII)

Fase de post-incidente

- Aprender de lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados.
- Tomar las medidas adecuadas para evitar que una situación similar se pueda volver a repetir, además de mejorar los procedimientos.
- Realizar un informe del ciberincidente que deberá detallar la causa del ciberincidente y coste, y las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.

Métricas

- Métricas e indicadores de referencia recomendados para medir el nivel de implantación y eficacia del proceso de gestión de incidentes de cada organización.

Métricas de gestión de incidentes

- **Indicador**: Estado de cierre de los incidentes.
- **Objetivo**: Ser capaces de gestionar incidentes de seguridad.
- **Indicador**: Estado de cierre de los incidentes de peligrosidad MUY ALTA / CRÍTICA.
- **Objetivo**: Ser capaces de gestionar incidentes de seguridad de alta peligrosidad.

Referencias bibliográficas

- Gobierno de España. Guía Nacional de Notificación y Gestión de Ciberincidentes. Consejo Nacional de Ciberseguridad, ene. 2019.
- Gobierno de España. Guía Nacional de Notificación y Gestión de Ciberincidentes. Consejo Nacional de Ciberseguridad, actualización feb. 2020. `https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes`