Detección y Documentación de Incidentes de Ciberseguridad.

La Importancia de la Detección de Incidentes

Wikipedia. *Sitio de Constantinopla* (CC0)

La detección de incidentes es clave en cualquier ámbito y además es fundamental que se efectúe en tiempo y forma.

En su día, un incidente no detectado a tiempo en uno de bastiones más famosos de la Historia, cambió la concepción del mundo entero y dio lugar al orden internacional tal y como lo conocemos hoy: la caída de Constantinopla en manos de los otomanos.

"Espantoso eco encuentra la noticia en Roma, en Génova, en Venecia. Como el retumbar del trueno se extiende a Francia, a Alemania, y Europa ve, conturbada, que por culpa de su ciega indiferencia ha penetrado por la Kerkaporta, la malhadada y olvidada puerta, una nefasta y devastadora potencia que debilitará sus fuerzas por espacio de siglos. Pero en la Historia, como en la vida humana, el deplorar lo sucedido no hace retroceder el tiempo, y no bastan mil años para recuperar lo que se perdió en una sola hora" (Stefan Zweig)

Constantinopla era una ciudad prácticamente inexpugnable. Era la capital de un imperio de más de 1000 años, protegida por murallas triples con foso, y cerrado su puerto natural,

el Cuerno de Oro, con una enorme cadena de hierro. Además, sus navíos estaban equipados con un arma cuya fórmula aún hoy no se conoce del todo: el fuego griego. El fuego griego era una sustancia líquida que se lanzaba con cañones y que ardía en contacto con el agua, haciendo naufragar a las naves enemigas.

El asedio fue increíble, con artillería, con navíos transportados por tierra, con bombardeos de enormes cañones de bronce, con innumerables tropas, pero Constantinopla no cayó por todo esto.

Constantinopla se perdió por no detectar a tiempo un incidente: ¡la Kerkaporta noroeste se dejó entreabierta!

La kerkaporta era una pequeña puerta de servicio para tránsito de peatones y avituallamiento en tiempos de paz, que se dejó abierta por un descuido. Un pequeño número de jenízaros penetraron por ella, se situaron tras las filas de los defensores y proclamaron a voces que la ciudad estaba tomada. Esto provocó la desbandada de la soldadesca y la caída de la ciudad, que habría podido esperar un poco más a la escuadra veneciana que venía de camino en su auxilio, pero el incidente pasó desapercibido a los guardianes de las torres cercanas.

Y así, una ciudad que había resistido con éxito 22 asedios a lo largo de la Historia fue saqueada con saña. De haberse detectado a tiempo el incidente no habría ocurrido nada reseñable, pues esta puerta sólo permitía el paso de personas de una en una y el número de invasores que engañaron a los guardias fue, en realidad, muy reducido.

En esta unidad se revisarán los **procedimientos de notificación de incidentes**, interna y externamente, priorizando la notificación obligatoria por los cauces oficiales.

Estos procedimientos contendrán **indicaciones** relativas a la apertura del incidente, el detalle a informar acerca del mismo, las ventanas temporales de reporte, las entidades destinatarias de la información y, finalmente, las condiciones que se tendrán que dar para el cierre del incidente.

1.- Desarrollar Procedimientos de Actuación para la Notificación de Incidentes.

El Concepto de CSIRT

CSIRT. *Foro CSIRTs españoles* (CC0)

CSIRT. *Computer Security Incident Response Team*.

Un **Equipo de Respuesta a Incidentes de Seguridad** es una organización que es responsable de **recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.**

Estos procedimientos recopilan la información relativa a la notificación para enviarla a la autoridad competente o CSIRT de referencia, con objeto de que quede registrado el incidente de ciberseguridad.

Estos procedimientos deberán contemplar la secuencia de notificación, así como los criterios empleados y las tablas a consultar para asignar los niveles de peligrosidad e impacto correspondientes en cada caso.

Para saber más

El Consejo Nacional de Ciberseguridad edita y mantiene la **Guía Nacional de Notificación y Gestión de Ciberincidentes**, que contiene las pautas oficiales a seguir en cada caso.

Dichas pautas se resumen en este apartado, no obstante, se puede disponer del detalle completo de las mismas descargando la Guía desde el siguiente enlace:

https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

1.1.- 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** (según el *Esquema Nacional de Seguridad*) que haga aconsejable la **comunicación del incidente a la autoridad competente o CSIRT de referencia.**
En todo caso, cuando un determinado suceso pueda asociarse a más de un tipo de incidente contenido en la Tabla de Clasificación/Taxonomía de los ciberincidentes debido a sus características potenciales, éste se asociará a aquel que tenga un Nivel de peligrosidad superior de acuerdo con los criterios correspondientes.

1.1.1.- Nivel de Peligrosidad del Ciberincidente.

Nivel	Peligrosidad
1	BAJO
2	MEDIO
3	ALTO
4	MUY ALTO
5	CRÍTICO

CCN. *Nivel de Peligrosidad de un Incidente*
(CC0)

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.

En la Guía Oficial se incluye la **Tabla de Criterios de determinación del nivel de peligrosidad** de un ciberincidente. Mediante la consulta de esta tabla, las entidades notificadoras de información podrán asignar un determinado nivel de peligrosidad a un incidente.

A grandes rasgos, los **niveles de peligrosidad** son los siguientes:

- **Bajo**
  - Spam
  - Scanning o sniffing
- **Medio**
  - Discurso de odio
  - Ingeniería Social
  - Intrusión o Intento de Intrusión
  - Uso no autorizado de recursos
  - Fraude
  - Denegación de servicio
  - Revelación de información
- **Alto**
  - Pornografía infantil, contenido sexual, violencia
  - Infección por código dañino
  - Compromiso de aplicaciones y cuentas
  - Denegación de servicio distribuida
  - Compromiso de la información
  - Phishing
- **Muy Alto**
  - Distribución y configuración de malware
  - Robo y sabotaje
  - Interrupciones
- **Crítico**
  - Amenazas Persistentes Avanzadas

1.1.2.- Nivel de Impacto del Ciberincidente.

INCIBE. *Nivel de Impacto de un Incidente* (CC0)

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

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

- Impacto en la Seguridad Nacional o en la Seguridad Ciudadana.
- Efectos en la prestación de un servicio esencial o en una infraestructura crítica.
- Tipología de la información o sistemas afectados.
- Grado de afectación a las instalaciones de la organización.
- Posible interrupción en la prestación del servicio normal de la organización.
- Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
- Pérdidas económicas.
- Extensión geográfica afectada.
- Daños reputacionales asociados.

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

En la Guía Oficial se incluye la **Tabla de Criterios de determinación del nivel de impacto de un ciberincidente**. Mediante la consulta de esta tabla, las entidades notificadoras de información podrán asignar un determinado nivel de impacto a un incidente en concreto.

1.1.3.- Niveles con Notificación Obligatoria Asociada.

INCIBE. *Notificación de Incidentes* (CC0)

Los incidentes se asociarán a uno de los niveles de peligrosidad e impacto establecidos en la Guía Oficial, 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 con lo contemplado en dicha Guía, 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 la Guía.

Autoevaluación

De los siguientes criterios, marcar el que no se utiliza para la determinación del nivel de impacto asociado a un incidente:

- ○ Tipología de la información o sistemas afectados.
- ○ Grado de afectación a las instalaciones de la organización.
- ○ Nivel de impacto reglado para el malware documentado
- ○ Posible interrupción en la prestación del servicio normal de la organización.

INCORRECTO

No se utiliza el nivel de impacto reglado para el malware documentado

INCORRECTO

No se utiliza el nivel de impacto reglado para el malware documentado

¡ CORRECTO !

No existe esta tabla de niveles de impacto reglados

INCORRECTO

No se utiliza el nivel de impacto reglado para el malware documentado

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

1.2.- Interacción con el CSIRT de Referencia.

INCIBE. *Interacción con el CSIRT de Referencia* (CC0)

Los CSIRT de referencia disponen de herramientas de notificación y *ticketing* de incidentes para lograr una mejor gestión y seguimiento del incidente con los usuarios. Cada CSIRT puede proporcionar diversos métodos de interacción con estas herramientas para facilitar la interacción durante todo el ciclo de vida del incidente.
No obstante, en caso de no disponer de las herramientas proporcionadas por los CSIRT de referencia, se considera válido el uso de correo electrónico.

1.3.- Apertura del Incidente.

INCIBE. *Apertura del Incidente* (CC0)

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

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

Durante el registro de un ciberincidente, **el CSIRT asignará a cada caso un identificador único** que estará presente durante todas las comunicaciones relacionadas con el incidente. Si las comunicaciones se realizan por correo electrónico, este identificador aparecerá en el campo “asunto” y no deberá modificarse o eliminarse ya que esto ralentizaría la gestión y la resolución final del ciberincidente.

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

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

1.4.- Información a Notificar.

INCIBE. *Información a Notificar* (CC0)

Para una correcta gestión y tratamiento de incidente registrado, se hace necesario **disponer de datos e informaciones precisas** acerca del mismo.

La Guía Oficial incluye una **tabla que reseña la información a notificar en un ciberincidente**, a modo de orientación para la entidad afectada por el ciberincidente en su comunicación a la autoridad competente o CSIRT de referencia.

Todos aquellos sujetos obligados a los que les sea aplicable normativa específica de acuerdo con lo contemplado en la Guía Oficial, deberán **comunicar en tiempo y forma** toda aquella información relativa al incidente registrado que les sea exigible.

El sujeto obligado comunicará en la notificación inicial **todos aquellos campos de la tabla acerca de los que tenga conocimiento en ese momento**, siendo posteriormente perceptiva la cumplimentación del resto de los campos, que se resumen a continuación:

- Asunto
- Operador de Servicios Esenciales o Proveedor de Servicios Digitales
- Sector Estratégico
- Fecha y hora del incidente
- Fecha y hora de detección del incidente
- Descripción
- Recursos tecnológicos afectados
- Origen del incidente
- Taxonomía
- Nivel de peligrosidad
- Nivel de impacto
- Impacto transfronterizo
- Plan de acción y contramedidas
- Afectación
- Medios necesarios para la resolución
- Impacto económico estimado
- Extensión geográfica
- Daños reputacionales
- Adjuntos
- Regulación afectada
- Requerimiento de actuación de las Fuerzas y Cuerpos de Seguridad del Estado

Autoevaluación

¿Cuál de los siguientes campos pueden cumplimentarse a posteriori tras la notificación inicial?

- [ ] Fecha y hora del incidente
- [ ] Nivel de impacto
- [ ] Descripción
- [ ] Plan de acción y contramedidas

Mostrar retroalimentación

Solución

1. Correcto
2. Correcto
3. Correcto
4. Correcto

1.5.- Ventana Temporal de Reporte.

INCIBE. *Ventana Temporal de Reporte* (CC0)

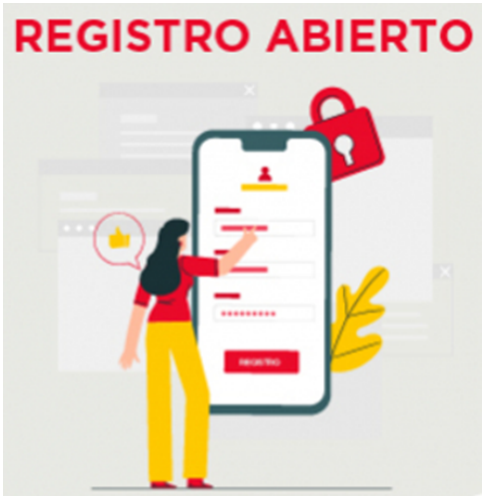
Todos aquellos sujetos obligados que se vean afectados por un incidente de notificación también obligatoria a la autoridad competente, a través del CSIRT de referencia, **remitirán, en tiempo y forma, aquellas notificaciones inicial, intermedia y final requeridas de acuerdo con la Tabla de Ventana temporal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

- La **notificación inicial** es una comunicación consistente en poner en conocimiento y alertar de la existencia de un incidente.
- La **notificación intermedia** es una comunicación mediante la que se actualizarán los datos disponibles en ese momento relativos al incidente comunicado.
- La **notificación final** es una comunicación final mediante la que se amplían y confirman los datos definitivos relativos al incidente comunicado.

Además, se aportarán todas aquellas **notificaciones adicionales intermedias o posteriores** que se consideren necesarias.

La comunicación se realizará siempre por escrito mediante el uso de correo electrónico o sistema proporcionado por el CSIRT de referencia del operador, enviando la Tabla de Información a notificar en un ciberincidente a la autoridad competente que figura en la Guía Oficial.

1.6.- Estados y Valores de Cierre.



INCIBE. *Incidente en Estado Abierto* (CC0)

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.

En la Guía Oficial se detalla la **Tabla de Estados de los ciberincidentes**, que muestra los diferentes estados que puede tener un ciberincidente en un instante dado, a saber:

- **Cerrado**.
  - Resuelto y con respuesta por parte del organismo afectado.
  - Resuelto y sin respuesta por parte del organismo afectado.
  - Sin impacto
  - Falso positivo
  - Sin Resolución y con respuesta por parte del organismo afectado.
  - Sin Resolución y sin respuesta por parte del organismo afectado.
- **Abierto**

En la Guía Oficial se indican asimismo los **días tras los que se cerrará un ciberincidente sin respuesta**, en función de su nivel de peligrosidad o impacto.

Autoevaluación

¿Cómo se efectuará la notificación al CSIRT de referencia?

- ○ Siempre por escrito, utilizando sólo correo electrónico
- ○ Siempre por escrito, utilizando sólo el sistema proporcionado por el CSIRT de referencia
- ○

Siempre por escrito, utilizando correo electrónico o el sistema proporcionado por el CSIRT de referencia

- ○ En caso de emergencia máxima, se puede notificar el incidente por teléfono

INCORRECTO

Se hará siempre por escrito, pero utilizando correo electrónico o el sistema proporcionado por el CSIRT de referencia

INCORRECTO

Se hará siempre por escrito, pero utilizando correo electrónico o el sistema proporcionado por el CSIRT de referencia

¡ CORRECTO !

INCORRECTO

Se hará siempre por escrito, pero utilizando correo electrónico o el sistema proporcionado por el CSIRT de referencia

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.- Notificación Interna de Incidentes.

Caso práctico

INCIBE. *Notificación Interna de Incidentes* (CC0)

Se denomina **Notificación Interna** de Incidentes al **conjunto de mecanismos, procedimientos, reglas y sistemas de Registro y Notificación** propios de cada **organización privada**.

Según esto, **no hay un estándar genérico** para estos mecanismos de notificación, no obstante, **sí que suele haber *estándares de facto*** internos a cada una de las organizaciones.

La definición del **flujo de notificación interna** tiene lugar en el ámbito de cada empresa, compañía o corporación empresarial, y tiene por objeto protocolizar el registro de datos del incidente con detalle suficiente y notificarlo de forma normalizada a la jerarquía de la empresa. A partir de dicha notificación, la organización tomará las medidas internas adecuadas, e incluso desencadenará las correspondientes notificaciones oficiales, en caso de que procedan.

Por lo general, **el flujo de notificación interna se implementa mediante un sistema *ad hoc***, que se basa en la información registrada automáticamente en un SIEM, complementada con los datos adicionales recogidos por los técnicos en el momento de detección del incidente.

Autoevaluación

¿Qué empresas deben tener un flujo de notificación interna de incidentes?

- ○ Las grandes corporaciones
- ○ Las PYMEs
- ○ Todas las empresas, sin distinción

INCORRECTO, no sólo las grandes corporaciones

INCORRECTO, no sólo las PYMEs

¡ CORRECTO !

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta

3.- Notificación de Incidentes a Quienes Corresponda.

Sistema de Ventanilla Única

INCIBE. *Ventanillas Únicas* (CC0)

Mediante el **sistema de ventanilla única** se informa de un incidente. La **información solicitada** en cada caso, en función de la naturaleza del afectado, **deberá ser remitida de acuerdo con el cauce establecido** por su autoridad competente o **CSIRT de referencia**.

Funcionamiento del sistema de ventanilla única:

Primero. **El sujeto afectado enviará un correo electrónico (o ticket) al CSIRT de referencia** (INCIBE-CERT o CCN-CERT) notificando el incidente.

Segundo. El **CSIRT** de referencia, dependiendo del incidente, **pondrá en conocimiento del mismo al organismo receptor implicado** o la autoridad nacional competente:

- Si afecta a la Defensa Nacional, al ESP-DEF-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:
  - **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.

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

Cuarto. **El sujeto afectado comunica los datos necesarios** al organismo receptor implicado o autoridad nacional competente.

Quinto. 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).

Autoevaluación

¿Cómo se actúa en la notificación urgente de incidentes a las autoridades competentes?

- ○ Se envía una notificación al CSIRT de referencia, INCIBE-CERT o CCN-CERT, que actúa como Ventanilla Única y lo remite a su vez al organismo receptor implicado en cada caso
- ○ Cuando se trata de una notificación realmente urgente, se puede obviar la comunicación a la Ventanilla Única y se puede acceder directamente al organismo receptor (ESP-DEF-CERT, CNPIC, AEPD, BDE)

¡ CORRECTO !

INCORRECTO, siempre se debe usar la Ventanilla Única

Solución

1. Opción correcta
2. Incorrecto

4.- Bibliografía.

Bibliografía (pdf - 51538 B)