Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
incibe cert_

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN

La S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) es una sociedad anónima estatal adscrita a la Secretaría de Estado de Digitalización e Inteligencia Artificiall y dependiente del Ministerio de Asuntos Económicos y Transformación digital 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 y proveedores de servicios digitales.

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[1] o CSIRT[2] Nacional competente en la prevención, mitigación y respuesta ante incidentes cibernéticos en España en el ámbito de las empresas privadas, ciudadanos e instituciones afiliadas a la Red Académica y de Investigación (RedIRIS) y proveedores de servicios digitales en el ámbito privado.

Adicionalmente, el INCIBE-CERT es operado conjuntamente por INCIBE y CNPIC[3] en todo lo que se refiere a la gestión de incidentes que afecten a operadores críticos.[4]

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

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

[3] Centro Nacional de Protección de Infraestructuras y Ciberseguridad.

[4] Artículo 11.2 del RD-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2 OBJETO

El presente documento deriva y está alineado con la **Guía nacional de notificación y gestión de ciberincidentes** y tiene por finalidad servir de apoyo en las tareas de gestión de ciberincidentes así como recoger los mecanismos, referencias y canales para su notificación al Centro de Respuesta a Incidentes de Seguridad de INCIBE (INCIBE-CERT), cuando así proceda.

El funcionamiento de dicho servicio de respuesta incluye la notificación a INCIBE-CERT según se recoge en la **Guía nacional de notificación y gestión de ciberincidentes,** así como las gestiones internas de INCIBE-CERT para llevar a cabo la resolución de los mismos y dar una respuesta a los afectados, aportando las recomendaciones oportunas que permitan reducir el riesgo para la seguridad que pudiera suponer dicho incidente.

Como tal, todos los ciberincidentes que afecten a los sistemas de información de cualquiera de los públicos objetivos a los que presta servicio INCIBE-CERT se pueden comunicar a este CSIRT, con independencia de que el afectado los resuelva por sus propios medios.

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 GESTIÓN DE INCIDENTES

Se conoce como gestión de incidentes de seguridad de la información 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.

Figura 1. Fases de la gestión de incidentes.

A continuación se describen en detalle las diferentes fases de la gestión de incidentes.

3.1. Preparación

Durante el estado previo a la declaración de un ciberincidente es necesario que toda entidad esté preparada para cualquier suceso que pudiera ocurrir. Una buena anticipación y entrenamiento previo pueden ser la diferencia entre una gestión eficaz de un incidente o un desastre absoluto, para lo que hace falta tener en cuenta tres pilares fundamentales: las **personas**, los **procedimientos** y la **tecnología**. El momento de declararse un incidente ya será tarde para comenzar a planificar.

Siempre se debe contar con un listado actualizado de contactos, tanto internos como externos a la organización, con los que puede ser necesario contactar (comité de crisis, proveedores, etc.) que cuenten con capacidades y entrenamiento en situaciones de presión y puedan reconducir un problema a un estado aceptable. Es necesario disponer de varios métodos de contacto para cada persona (teléfono, mensajería instantánea, correo electrónico…) por si alguna vía de contacto no estuviera disponible en el momento en que surja la necesidad. Para el caso de comunicaciones cifradas, resulta fundamental haber probado con anterioridad el sistema de envío y recepción y contar con los mecanismos de cifrado necesarios. No disponer de las claves públicas de un contacto o enviar un mensaje confidencial cifrado a un destinatario que no tiene capacidad acceder al mismo (problemas técnicos, falta de herramientas, personal no preparado…) obliga a dedicar recursos esenciales en labores no prioritarias.

En algunos casos será necesario recoger evidencias que serán posteriormente analizadas o utilizadas en algún proceso judicial. Para evitar contaminar estas evidencias, se debe disponer de medios extraíbles que hayan sido borrados previamente de forma segura. Esto evitará también que se tenga que proceder al borrado durante la gestión de un incidente con la pérdida de tiempo y recursos que ello implicaría.

También es el momento de preparar el resto de herramientas que puedan necesitarse durante la gestión del incidente, como una herramienta de *ticketing* en la cual registrar

la gestión de incidentes, u otras que puedan hacer falta durante las fases posteriores de la gestión de los mismos, como medios de almacenamiento, clonadoras, programas o herramientas, como destornilladores y alicates.

Los equipos de respuesta a incidentes, sobre todo si son externos a la organización, podrían no estar familiarizados con la arquitectura afectada; disponer de diagramas de red y un catálogo de activos actualizado (al menos con aquellos recursos más críticos) proporciona una visión global y ayuda a elaborar una estrategia para afrontar el problema.

Muy probablemente sea necesario disponer de dispositivos para realizar la recogida de evidencias, el análisis de las mismas o, incluso, la restauración de algún servicio crítico que se haya visto afectado. Deben tenerse en cuenta las posibles necesidades de este material adicional y asegurarse de que se encuentra preparado para la tarea que deban desarrollar (análisis de tráfico de red, duplicado de discos, extracción de evidencias, análisis forense, virtualización, análisis de programas maliciosos…) y que los pasos para realizarlos se hallen recogidos en los procedimientos y éstos estén actualizados.

Ante la necesidad de proceder a la restauración de un sistema afectado durante un incidente, se debe disponer de una imagen segura y funcional que permita volver a un estado previo y asegure la continuidad del proceso afectado. Estos procesos de restauración y recuperación deben haber sido probados y documentados previamente para asegurar que se desarrollen con las máximas garantías.

Las evidencias recogidas durante el proceso de gestión de un incidente, así como cualquier otro material sensible, podrían necesitar de una ubicación segura donde ser almacenados, por lo que en la fase de preparación ante incidentes también debe planificarse la localización y disponibilidad de este tipo de almacenamiento.

Dado que siempre existe la posibilidad de que ocurran los ciberincidentes, es necesario tratar de prevenirlos en la medida de lo posible y estar preparados por si estos se materializasen. Resulta especialmente importante prestar atención en algunos aspectos como:

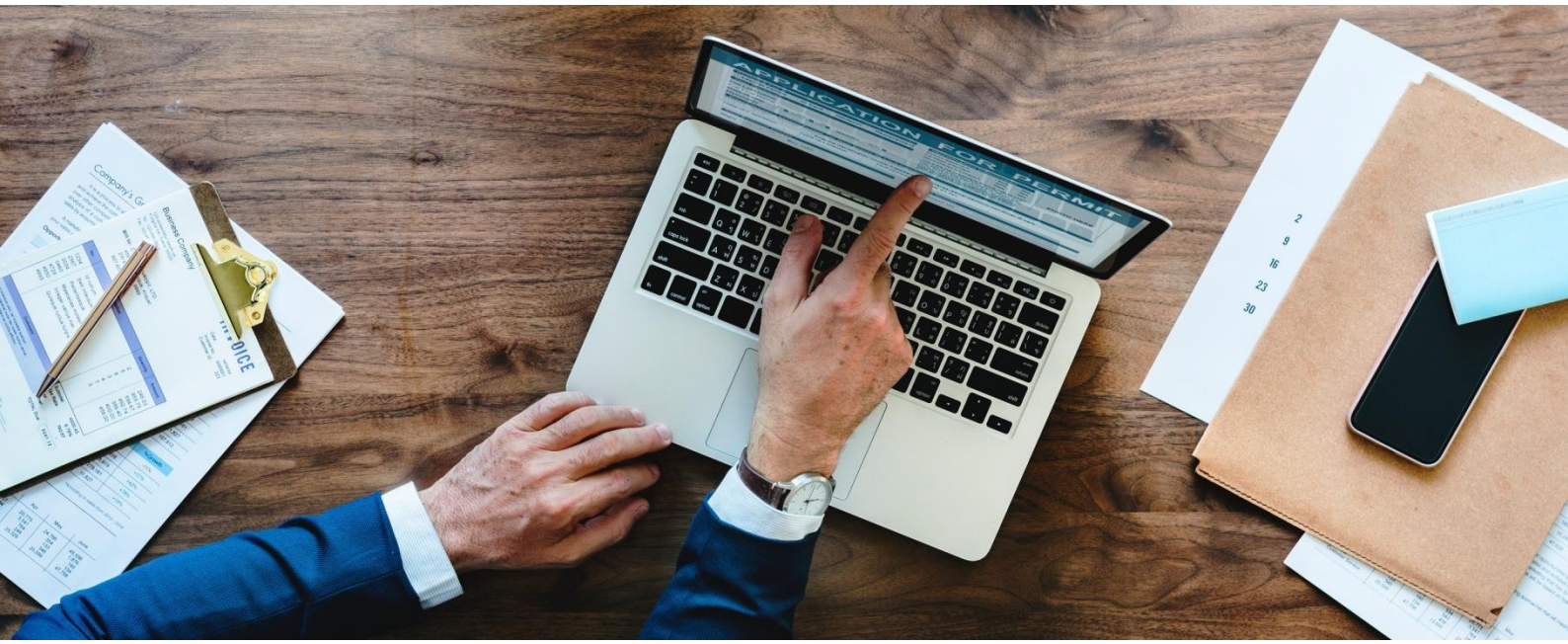
- **Formación del equipo humano:** El usuario siempre es el eslabón más débil cuando se habla de seguridad, por lo tanto, es necesario realizar labores de formación y concienciación para que los usuarios sean capaces de hacer un uso responsable de los sistemas y de la información que utilizan. Por ejemplo, los incidentes reales ocurridos en el pasado -a la propia entidad o a terceras- forman un excelente material para concienciar sobre las amenazas existentes y posibles consecuencias de un uso inapropiado de los activos.

- **Protección del puesto de trabajo:** El factor humano no tiene por qué ser siempre la causa de un posible ciberincidente, existen otras variables que se deben tener en cuenta, como pueden ser las posibles vulnerabilidades en programas o sistemas operativos, programas maliciosos, intrusiones o ataques a través de la red, etc. Es necesario conocer estas amenazas y aplicar las medidas preventivas adecuadas para evitar, en la medida de lo posible, que los ataques tengan éxito.

- **Análisis de riesgos:** Un correcto análisis de riesgos requiere identificar los activos que gestiona una entidad y las amenazas por las que podrían ser

afectados. Tras una asignación de probabilidad e impacto de las amenazas sobre los activos, se debe proceder a la gestión de los riesgos; un proceso que obliga a definir el umbral que determinará qué riesgos se consideran asumibles y cuáles no. A partir de aquí se debe definir un plan de tratamiento de riesgos que recoja qué acciones se van a realizar para controlar los riesgos previamente identificados durante el análisis, pudiendo ser mitigados, transferidos o aceptados.

La realización de ciberejercicios o entrenamientos de ciberdefensa es un excelente método de preparar al personal humano ante situaciones de crisis a través de situaciones simuladas que permite conocer las amenazas actuales que pueden afectar a los sistemas de información y los mecanismos existentes que pueden servir para combatir las amenazas. INCIBE ha publicado una taxonomía de ciberejercicios[5] y organiza periódicamente, desde el año 2013, los ciberejercicios CyberEx.[6]



3.2. Identificación

Cualquier organización debe conocer cuál es su estado normal de operación y qué sucesos forman parte de la operativa diaria, ya que solamente así será posible identificar aquellos casos que pueden ser considerados anormales y requieren un análisis en profundidad. Generalmente, solo una pequeña parte de todos los eventos que se procesan por los sistemas son motivo de análisis en detalle y considerados incidentes de seguridad.

Esta fase está muy relacionada con la fase de preparación, ya que existe un constante salto entre ambas. Cuando un evento requiere de un mayor análisis se podría decir que se pasa de la fase de preparación a la fase de identificación, sin embargo, si se descarta el evento, se volvería de nuevo a la fase de preparación hasta que un nuevo evento requiera de mayor atención.

[5] https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe_taxonomia_ciberejercicios.pdf

[6] https://www.cyberex.es

A partir del momento en que se inicia la fase de identificación se recomienda aplicar políticas de confidencialidad y considerar el principio de "necesidad de conocer", compartiendo la información solamente con aquellas personas implicadas que realmente necesiten conocerla. Las comunicaciones cifradas y el almacenamiento seguro de la información se deben tener en cuenta también a partir de este momento.

Resulta imposible disponer de procedimientos para gestionar todos los ciberincidentes que pueden llegar a materializarse, sin embargo, existen unos vectores de ataque comunes que ayudan a identificar un incidente de seguridad, determinar su alcance y los sistemas afectados. Algunos vectores habituales que merecen especial atención son:

- **Correo electrónico:** Los ataques de suplantación de identidad a través de correo electrónico (*spear phishing*) han resultado ser una técnica con un elevado porcentaje de éxito y son ampliamente utilizados. Este tipo de ataques puede contener enlaces o ficheros adjuntos maliciosos.
- **Vulnerabilidades conocidas:** Las vulnerabilidades en gestores de contenidos, componentes, módulos, dispositivos industriales, elementos de tipo IoT, aplicaciones web y software en general, incluido el propio sistema operativo, pueden suponer, además del acceso no autorizado a los sistemas, el robo de información sensible, credenciales u otra información que puede ser utilizada en combinación con alguna otra técnica para lograr un ataque exitoso.
- **Dispositivos de almacenamiento externo:** Los dispositivos de almacenamiento masivo que se conectan a través de USB son un vector de ataque que debe tenerse en cuenta durante la identificación de un ciberincidente.
- **Uso inapropiado de los activos:** La instalación de programas no autorizados, el acceso a páginas web de dudosa legalidad o los posibles descuidos al utilizar documentación confidencial son un origen común de numerosos ciberincidentes.
- **Pérdida o robo de activos:** La pérdida o robo de documentación o de dispositivos que no cuentan con las medidas de seguridad apropiadas como el borrado remoto o el cifrado de información.
- **Vectores externos:** Algunos ataques, como sabotajes o los ataques de fuerza bruta, son causa de problemas relacionados con la disponibilidad de los servicios.

Una vez que se han considerado los vectores del ataque, se pueden emplear diferentes fuentes de información que ayuden a identificar el origen de un posible ciberincidente y su alcance. Por ejemplo:

- A nivel de red:
  - Registros de conexiones realizadas a través de sistemas proxy.
  - Registros de conexiones autorizadas por los cortafuegos.
  - Registros de intentos de conexión que han sido bloqueadas en los cortafuegos.
  - Trazas de red que muestren conexiones a destinos, puertos o a través de protocolos no esperados, así como picos de tráfico anómalos o en horarios no habituales.

- Conexiones que tengan como origen o destino nodos de la red TOR o activos que aparezcan en listas de reputación como potencialmente maliciosos.
- Sistemas de correlación de eventos de seguridad (SIEM).
- Sistemas en red de detección/prevención de intrusos (NIDS/NIPS).
- Sistemas en red de prevención de fugas de información (NDLP).

- A nivel de equipo:
  - Registros de sistemas locales de detección/prevención de intrusos (HIDS/HIPS).
  - Cuentas de usuario inusuales en el sistema, especialmente aquellas con privilegios administrativos
  - Ficheros ocultos o con tamaños, nombres o ubicaciones sospechosas, pudiendo indicar los mismos algún tipo de fuga de información o almacenamiento por parte de algún *malware*.
  - Ficheros con permisos inusuales, con SUID o SGID en rutas no habituales, ficheros huérfanos y que pudieran determinar algún tipo de intrusión o *rootkit*.
  - Entradas sospechosas en el registro, principalmente en el caso de infecciones por malware en sistemas Windows, donde ésta es una de las técnicas habituales utilizadas por el malware para asegurar la persistencia en el sistema comprometido.
  - Registros de auditoría y accesos no autorizados.
  - Sistemas locales de prevención de fugas de información (DLP).
  - Procesos y servicios inusuales, no sólo servicios a la escucha, sino también conexiones establecidas a puertos o host extraños, poco habituales o incluidos en algún tipo de lista negra de servidores de Comando y Control (C&C) utilizados por *botnets*.
  - Una carga excesiva de disco o memoria puede estar producida por un incidente de seguridad como malware, denegaciones de servicio o intrusiones.
  - Sesiones abiertas en la máquina desde otros equipos, anomalías en las tablas ARP, carpetas compartidas inusuales o con permisos excesivos, o un elevado número de conexiones con algún *flag* TCP activado de manera anómala y que pudiera evidenciar un ataque.
  - En el caso de equipos de usuario o terminales móviles, pueden indicar algún tipo de infección en el sistema, entre otros: comportamiento anómalo de alguna aplicación, ventanas emergentes del navegador, conexiones muy lentas, reinicios o aplicaciones que se cierran sin motivo.
  - Tareas programadas o actividad sospechosa en los registros de auditoría y *logs* que indique un funcionamiento anormal del sistema o intentos de intrusión en algún servicio, por ejemplo mediante fuerza bruta.
  - Registros de consolas antivirus o de alguna herramienta habitualmente instalada en el sistema para la identificación de *rootkits*, de control de integridad de ficheros, firma de los binarios, etc.
  - Registros de consolas anti spam.
  - Anomalías o condiciones reportadas por otros usuarios.

- A nivel de aplicación:
  - Registros de auditoría y accesos no autorizados.
  - Registros o *logs* de aplicaciones que puedan recoger información de interés, como fechas, transacciones o actividad de los usuarios.

Existen otro tipo de fuentes externas que proporcionan información que debe ser considerada:

- Anomalías o condiciones reportadas por otros usuarios externos a la organización.
- Información sobre nuevos *exploits* o vulnerabilidades reportadas por fabricantes, proveedores de servicios u otros equipos de respuesta como INCIBE-CERT.[7]
- Información disponible públicamente a través de redes sociales, en muchos casos relativas a campañas de actividades hacktivistas.

Conviene comprobar siempre aquellos sistemas con configuraciones similares a los afectados, ya que un atacante podría utilizar una misma técnica de intrusión en diferentes equipos.

Como se ha mencionado con anterioridad, conocer cuál es el estado normal de operación ayudará a detectar anomalías que pueden requerir de un análisis en detalle. También es importante no caer en una falsa sensación de seguridad causada por la existencia de tecnologías de protección, ya que éstas no son infalibles.

3.3. Contención

Si un atacante ha logrado comprometer un dispositivo, se debe evitar que pueda comprometer un segundo; si ha logrado extraer un documento del servidor de archivos, la labor del equipo de respuesta, en este momento, es evitar que salga más información al exterior. La formación y experiencia del personal implicado en la gestión de incidentes será un factor determinante durante esta fase.

Cuando ocurre un ciberincidente, esta suele ser la fase en la que se toman las decisiones de forma más rápida ya que el tiempo es un factor determinante y la reputación o la continuidad del negocio están en jaque y hay que recordar que las decisiones precipitadas son buenas aunque no siempre son acertadas.

La documentación de cada paso que se tome o cada actividad que se observe durante esta fase resulta de gran importancia para incluir en la bitácora o la herramienta de gestión de incidentes. Las decisiones se toman rápidamente y resulta extremadamente sencillo realizar alguna acción indebida, o que requiera un posterior seguimiento, que podría no ser recordada y comprometer con ello la resolución del problema, sobre todo cuando no se siguen los procedimientos existentes sobre gestión de incidentes.

Una vez que se ha comenzado a estudiar la situación, se está en disposición de proceder a la clasificación del ciberincidente, lo que permitirá determinar cómo abordarlo y revelará algunas pautas para su resolución. Una taxonomía de ciberincidentes permite realizar una priorización en función del tipo de incidente y peligrosidad del mismo. El impacto producido por el ciberincidente es un tercer valor con carácter más dinámico que los anteriores y puede variar a lo largo del ciclo de vida del incidente ya que, lo que inicialmente puede parecer un problema simple relacionado con un correo electrónico podría resultar finalmente una crisis con robo de propiedad intelectual y daño de reputación.

[7] La web de INCIBE-CERT (https://www.incibe-cert.es/) ofrece tanto avisos de seguridad de alerta temprana y vulnerabilidades como una bitácora de Ciberseguridad y otros contenidos.

Una correcta clasificación de los ciberincidentes permite a los equipos de respuesta asignar la prioridad adecuada a cada problema, asegurando que se tratan en primer lugar o que se asignan más recursos a aquellos casos más graves. La taxonomía de ciberincidentes utilizada por INCIBE-CERT, basada en las mejores prácticas y siguiendo las recomendaciones de organismos internacionales relevantes en la materia, está disponible a través del enlace[8] al contenido actualizado por el grupo de trabajo.

Conviene registrar y documentar el ciberincidente con el apoyo de una herramienta de gestión de incidentes o *ticketing*, incluyendo la información obtenida durante la fase de identificación así como los valores de clasificación, peligrosidad e impacto inicial. También es el momento de considerar la necesidad de comunicar la existencia de un incidente de seguridad a un nivel superior en la estructura organizativa de la entidad (responsables de departamentos, CISO, CIO, Comité de crisis…) en función de cómo se haya definido en los procedimientos.

Si no ha ocurrido ya, es muy probable que las acciones que se tomen a partir de este momento puedan afectar a la prestación de algún servicio ofrecido por la organización. Dado que no es labor del equipo de respuesta, ni éste tiene el conocimiento necesario para estimar la pérdida que puede suponer para el negocio aislar un servidor que ofrece un servicio esencial para la organización, siempre se debe obtener la autorización del área de negocio antes de iniciar acciones de contención de gran impacto. Evite siempre que el remedio sea peor que la enfermedad.

Conocida la extensión del problema a través de diagramas de red, sistemas de detección, correladores de eventos y otras tecnologías, se pueden buscar características comunes entre los activos afectados y tomar medidas de aislamiento en función de los patrones identificados.

[8]https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md

Algunas de las acciones que se pueden tomar en primer lugar consisten en:

- Desconectar el equipo o segmento de red del resto de redes de la organización. Esto puede hacerse, si se trata de un equipo aislado, desconectando el cable de red o tirando el enlace inalámbrico si la conexión se realiza a través de Wi-Fi.
- En caso de tratarse de algún equipo que desempeña una función crítica para el negocio, es posible proceder a la colocación de un firewall intermedio entre el segmento afectado y el resto de la red que permita filtrar el tráfico y permitir únicamente aquello que sea estrictamente necesario para la prestación del servicio.
- Reubicación del recurso comprometido en una VLAN aislada.
- Considerar la aplicación de técnicas de DNS *sinkholing* para controlar tráfico malicioso.
- Si se conocen los detalles técnicos del tipo de ciberincidente se pueden aplicar medidas de contención más ajustadas a cada situación (bloqueo de determinados correos electrónicos, aplicación de reglas en los cortafuegos, bloqueo de acceso a unidades compartidas, etc.).
- Contactar con terceras entidades que pueden ofrecer ayuda en la contención. Los proveedores de servicio de Internet pueden aplicar filtros o activar medidas de protección e INCIBE-CERT puede ofrecer información adicional y coordinación a nivel nacional e internacional con otros posibles implicados en el incidente.

Una vez que se han tomado las medidas iniciales para contener el problema, cuidando de no destruir información valiosa, es momento de comenzar con los procedimientos de toma y preservación de evidencias. Este paso resulta importante, tanto por si finalmente es necesario judicializar el incidente, como para poder analizar correctamente el origen y determinar el impacto real del problema.

Los datos volátiles almacenados en la memoria del equipo pueden resultar muy importantes para el proceso de análisis en casos de programas maliciosos o de intrusiones y éstos se perderían si se apagara el equipo, por lo que en caso de considerarlo relevante se han de aplicar técnicas para su adquisición antes del apagado de los equipos. Para la adquisición de memoria volátil se pueden utilizar herramientas forenses (tanto hardware como software), procurando en todo momento no alterar el sistema ni los datos del mismo ya que podrían modificarse o perderse evidencias importantes. En sistemas virtualizados la memoria RAM está disponible como un fichero; en el caso de *VirtualBox* éste tiene la extensión ".sav" y ".vmem" en *VMWare*.

Una vez completado el proceso de adquisición de datos volátiles de la memoria ya se podría proceder al apagado del sistema. Para ello, y con el fin de evitar algún comportamiento desconocido de un posible programa malicioso presente en el equipo comprometido, lo más recomendable es proceder a un corte de energía repentino del sistema, desconectando el cable de corriente o retirando la batería del equipo.

Para los datos no volátiles se deben realizar copias exactas (bit a bit) de los datos originales. Esto se puede realizar a través de diferentes utilidades o herramientas, o mediante dispositivos físicos conocidos comúnmente con el nombre de *clonadoras*. Siempre que se realice una copia de un medio de almacenamiento conviene verificar que el medio original no sufrirá ninguna alteración, por lo que se recomienda emplear

elementos que bloqueen la escritura en ellos (*write-block*) mientras se realiza el clonado.

La información copiada se debe almacenar en dispositivos sobre los que se hayan aplicado previamente técnicas de borrado seguro para garantizar que no contengan ninguna información anterior que pudiera contaminar los nuevos datos. Conviene que los medios de destino tengan un tamaño ligeramente superior al medio de origen. Es posible que, en algunos casos, no sea posible realizar una copia completa del sistema ni de la memoria; en estos casos se pueden evaluar alternativas como realizar un análisis forense en vivo.

Una vez extraídos los datos se deben aplicar técnicas adicionales que garanticen la integridad de los mismos; esto se consigue a través de la aplicación de funciones criptográficas o *hash*. La mayoría de los sistemas actuales permiten realizar funciones de tipo MD5 y SHA1, en algunos casos también existirá la opción de aplicar funciones de la familia SHA2, siendo preferibles estas últimas. Estas funciones se deben aplicar tanto en los datos de origen como en los datos de destino, verificando que el valor obtenido en ambos casos es el mismo. Esto permite comprobar de forma sencilla que los datos copiados sean idénticos a los originales.

A partir de este momento se pueden comenzar las acciones de análisis de los datos copiados para tratar de obtener la máxima información sobre lo ocurrido y continuar con la fase de mitigación del incidente. Sin embargo, puede ocurrir que en este momento un equipo comprometido deba continuar prestando servicio por necesidades del negocio. En estos casos se deben aplicar medidas correctivas temporales hasta que el activo pueda ser reemplazado o retirado del servicio temporalmente para aplicar las medidas de mitigación de forma permanente. Sin ánimo de ser exhaustivos, algunas de estas medidas a considerar pueden ser:

- Eliminar procesos sospechosos.
- Eliminar cuentas de usuario que se hayan creado por parte de los posibles atacantes.
- Aplicar reglas de filtrado y medidas adicionales de seguridad en los sistemas de protección perimetrales.

3.4. Mitigación

La medida de mitigación más adecuada suele empezar por realizar un borrado seguro de los medios de almacenamiento comprometidos y una reinstalación del sistema pero desgraciadamente no siempre posible; en algunos casos porque no existe una copia de seguridad reciente de la información (si existe) y en otros casos porque volver a poner un sistema en producción sin conocer las causas del ciberincidente puede acarrear un nuevo e idéntico problema.

Las medidas de mitigación dependerán del tipo de ciberincidente, así, en casos de denegaciones de servicio distribuidas (DDoS) puede ser necesario solicitar asistencia de entidades externas, como proveedores de servicios de mitigación de este tipo de ataques o un CSIRT nacional como INCIBE-CERT, que puedan apoyar en el análisis y definición de la estrategia de mitigación.

Los fabricantes de productos antivirus ofrecen soluciones para eliminar amenazas de equipos comprometidos, sin embargo, es necesario que éstas hayan sido previamente

identificadas por el fabricante para que puedan ser detectadas y eliminadas automáticamente.

En algunos casos, la eliminación automática a través de herramientas no es posible, principalmente cuando se trata de algún tipo de *rootkit* o amenazas más avanzadas. En estos casos será necesario proceder a un borrado seguro del medio de almacenamiento y a una reinstalación completa del sistema operativo y aplicaciones. Si existen copias de seguridad y se conoce con exactitud la fecha de compromiso, es posible proceder a una restauración del sistema con una copia de seguridad anterior al comienzo del incidente.

Tanto si se realiza una instalación nueva, como si se restaura una copia de seguridad previa al ciberincidente, es necesario aplicar las medidas de seguridad necesarias en el sistema; esto incluye actualizaciones tanto del sistema operativo como del resto de aplicaciones. También es necesario realizar un análisis sobre el grado de exposición del activo, ya que en muchos casos el compromiso tiene su origen en servicios expuestos mal configurados que no deberían estar activos o que, si son necesarios, deberían haber estado correctamente protegidos (telnet, ssh, rdp, etc.).

Cuando no existan copias de seguridad disponibles y se haya realizado una reinstalación completa del sistema, la información debe ser extraída manualmente del equipo previamente comprometido y transferida al nuevo sistema, con la correspondiente cautela de no transmitir junto con ella la infección.

Aunque en algunos casos determinadas medidas pueden solaparse entre esta fase y la fase anterior, este puede ser el momento en el que se proceda a aplicar las últimas actualizaciones de los fabricantes, realizar el cambio de contraseñas de las cuentas de usuario o revisar las reglas de seguridad perimetral.

Antes de la puesta en producción del nuevo sistema, es recomendable realizar una auditoría de seguridad del mismo para garantizar que el nivel de protección del activo es aceptable y su puesta en producción se puede realizar de forma segura.

3.5. 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 como procesos extraños, cuentas de usuario no autorizadas, nuevas entradas en el registro, conexiones no identificadas, cualquier síntoma que pueda indicar que el problema está volviendo a ocurrir.

En los casos de sistemas críticos, conviene prestar especial atención a las instrucciones del fabricante del producto para su restauración o reinstalación, programando mantenimientos correctivos y paradas de sistemas necesarias para llevar a cabo la recuperación del ciberincidente.

Existe la posibilidad de que durante la puesta en producción del nuevo sistema se reproduzca el problema original o algún otro que tenga como objetivo alguno de los activos de nuestro dominio. En estos casos será necesario volver a aplicar las medidas de contención y erradicación que se explicaron en los apartados anteriores.

Es importante que los responsables no técnicos y los administradores del sistema verifiquen el correcto funcionamiento. Todo esto será mucho más fácil de realizar si la puesta en marcha se realiza en una franja horaria en la que la carga de trabajo del sistema sea menor.

3.6. 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 utilización de una herramienta de gestión de incidentes o una bitácora en la que se registre toda la información a medida que se ha ido recopilando ayudará en la elaboración de un informe post-incidente y evitará obviar información importante.

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. Esto ayudará también a evaluar los procedimientos de actuación, la cadena de mando, las políticas de seguridad y entrenará a los implicados para futuras situaciones de crisis.

Cada miembro del equipo implicado en la gestión del ciberincidente debe aportar sus anotaciones y todas deben ser recogidas en un informe general que puede ser revisado en una reunión. El informe post-incidente debe incluir un breve resumen ejecutivo y anexos técnicos para ser distribuido tanto a altos cargos de la organización como a personal técnico que desee ahondar en lo sucedido y analizar el proceso completo.

4 PROCEDIMIENTOS

La **Guía nacional de notificación y gestión de ciberincidentes** recoge el procedimiento y los mecanismos para la notificación de ciberincidentes al CSIRT de referencia.

La notificación de ciberincidentes puede realizarse desde la entidad afectada hacia INCIBE-CERT o viceversa. Como CSIRT o CERT de referencia a nivel nacional, INCIBE-CERT dispone de mecanismos propios y de colaboraciones con terceros para la detección de amenazas e informar a los afectados. Del mismo modo, cualquier ciudadano, pyme, entidad de derecho privado o institución afiliada a RedIRIS y proveedores de servicios digitales del ámbito privado puede comunicar un ciberincidente a INCIBE-CERT y beneficiarse del servicio de respuesta, independientemente de que finalmente resuelva el ciberincidente por sus propios medios.

Una vez realizada la notificación del ciberincidente se ponen en marcha los procedimientos internos del CSIRT para dar una respuesta efectiva y lograr una solución.

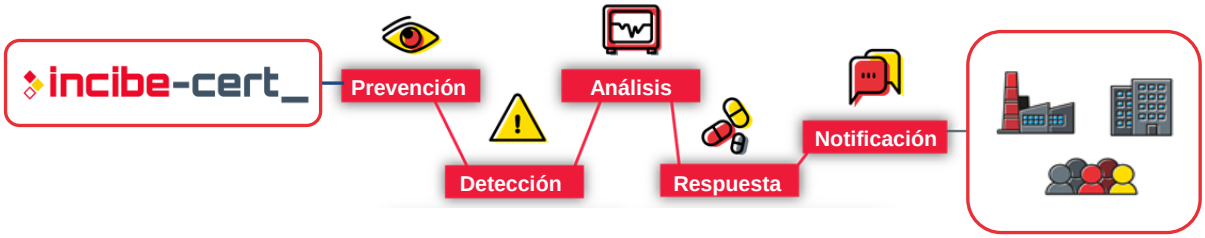


Figura 2. INCIBE-CERT, CSIRT nacional

4.1. Apertura del caso

Siempre que INCIBE-CERT 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 INCIBE-CERT. Si el remitente está fuera del ámbito de actuación o el caso reportado no puede ser clasificado en ninguna categoría de la taxonomía de INCIBE-CERT, se descartará la apertura de un nuevo ciberincidente, notificando al remitente cuando sea necesario.

Si aplica la gestión del ciberincidente por parte de INCIBE-CERT, se registrará la información reportada y se establecerá una prioridad al caso en función de su clasificación, iniciándose posteriormente las acciones necesarias para la resolución del ciberincidente.

Durante el registro de un ciberincidente, INCIBE-CERT asignará a cada caso un identificador único que estará presente durante todas las comunicaciones relacionadas con el incidente. En aquellos casos en los que la comunicación con el afectado u otras partes implicadas se realice por correo electrónico, este identificador aparecerá en el campo “asunto”. Este valor 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, INCIBE-CERT podrá comunicarse con el remitente o con terceras partes para solicitar o intercambiar información adicional que agilice la resolución del problema.

4.2. Priorización

A cada ciberincidente se le asignará una prioridad en función de la peligrosidad y del impacto potencial del mismo.

Como norma general, INCIBE-CERT realizará una comunicación inicial por correo electrónico con el responsable del activo implicado en el ciberincidente y, en caso de no obtener respuesta, volverá a intentarlo en otras dos ocasiones, esperando 7 días entre cada comunicación. De no obtener respuesta se procederá al cierre del incidente.

Figura 3. Seguimiento del incidente

Para aquellos ámbitos de actuación en los que se haya definido un procedimiento de escalado diferente, se procederá a notificar a los contactos alternativos a través de los medios establecidos antes de proceder al cierre del caso.

- **Prioridad Baja y Media**

Los incidentes se atienden por orden de llegada mientras no requiera atención uno de prioridad superior. En este caso, INCIBE-CERT esperará a que el afectado tome las acciones correctivas necesarias para la solución del problema, siguiendo el procedimiento descrito anteriormente.

- **Prioridad Alta**

Estos ciberincidentes requieren ser atendidos antes que otros, aunque sean detectados posteriormente. Cuando el volumen de incidentes sea elevado, no se gestionarán otros casos de prioridad inferior mientras que estos no hayan sido atendidos.

Procedimiento específico para las entidades afiliadas a RedIRIS:

Se intenta contactar con la institución responsable de la dirección IP implicada en el incidente para que tome las acciones correctivas oportunas tanto por correo como por teléfono. Primero con su responsable de seguridad de la institución y a continuación con el PER de la institución.

Figura 4. Incidentes de prioridad alta en RedIRIS

Si se trata de una institución conectada a una red regional o autonómica, se pone también en copia de todos los mensajes a los responsables de seguridad de la red autonómica.

Si al siguiente día laborable después de la última comunicación, y como máximo transcurridas 24 horas, el problema persiste, se solicita directamente a la red autonómica que proceda a tomar las acciones correctivas necesarias sobre la dirección IP atacante para atajar el problema. Para ello se enviará un mensaje solicitando dichas acciones a la red autonómica, poniendo en copia de dicho mensaje a los responsables de la institución, de forma que sean conscientes de las medidas que la red autonómica va a tomar sobre su dirección IP. Durante el transcurso de este lapso de tiempo se podrá contactar con ambas partes para conocer el estado de la implementación de la solución.

Si al siguiente día laborable desde el último mensaje, y como máximo transcurridas 24 horas, el problema persiste, se procederá a mitigar el problema directamente en el backbone. Las acciones implementadas por RedIRIS para solucionar el problema estarán vigentes hasta que la institución o la red autonómica acrediten que el problema ha quedado resuelto. Se quedará a la espera de recibir la información de la institución o la red autonómica, en la que debe consignarse el código del incidente (número de ticket) y la justificación que acredite que el problema se ha resuelto. Cuando se recibe la comunicación con la solución del problema dispondrá como máximo de 24 horas para analizar dicha información y proceder a la eliminación de las medidas correctivas aplicadas sobre la dirección IP.

- **Prioridad Crítica**

La gestión de estos ciberincidentes no admite demora y para su resolución se emplearán todos los recursos disponibles.

Procedimiento específico para las entidades afiliadas a RedIRIS:

Se toman las acciones correctivas del problema sobre el backbone de RedIRIS sin previa notificación a la institución afectada o a la red autonómica. De esta forma se protege la infraestructura de RedIRIS para garantizar su normal funcionamiento.

Figura 5. Incidentes de prioridad crítica en RedIRIS

Se intenta contactar con la institución responsable de la dirección IP implicada en el ciberincidente, tanto por correo como por teléfono. Primero con el responsable de seguridad de la institución y luego con el PER de la institución. Si se trata de una institución conectada a una Red Autonómica, se pone también en copia de todos los mensajes a los responsables de seguridad de la red autonómica

RedIRIS mantendrá las medidas correctivas aplicadas hasta que la institución o la red autonómica acrediten que el problema ha quedado resuelto. RedIRIS quedará a la espera de recibir la información de la institución o la red

autonómica, en la que debe consignarse el código del incidente (número de ticket) y la justificación que acredite que el problema se ha resuelto.

Cuando RedIRIS recibe la comunicación con la solución del problema dispondrá como máximo de 24 horas para analizar dicha información y proceder a la eliminación de las acciones correctivas aplicadas sobre la dirección IP.

4.3. Resolución

Una vez que se ha alcanzado una solución que implique el cierre del incidente, tanto por parte del afectado como por parte de INCIBE-CERT, ésta será comunicada a los actores implicados en el ciberincidente.

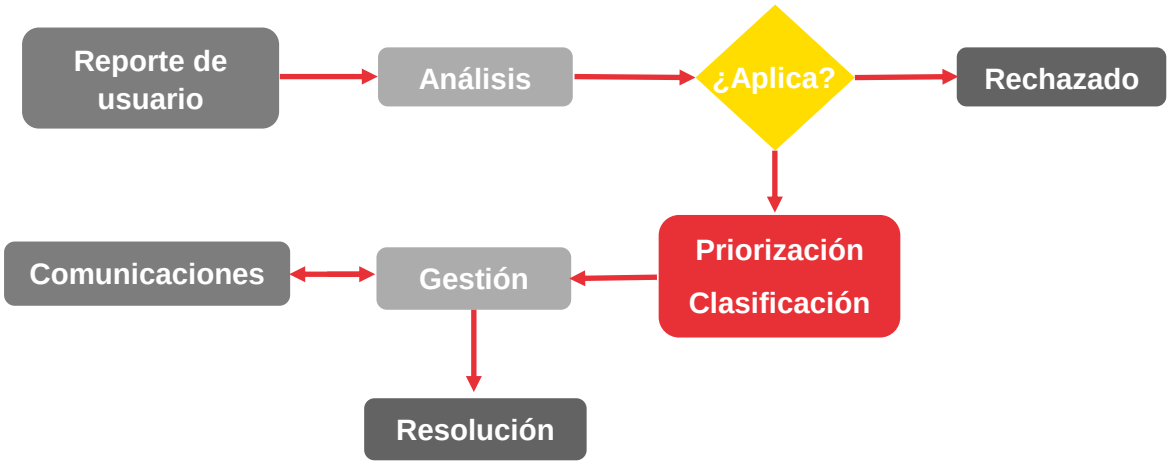


Figura 6. Flujo de gestión de ciberincidentes.

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.

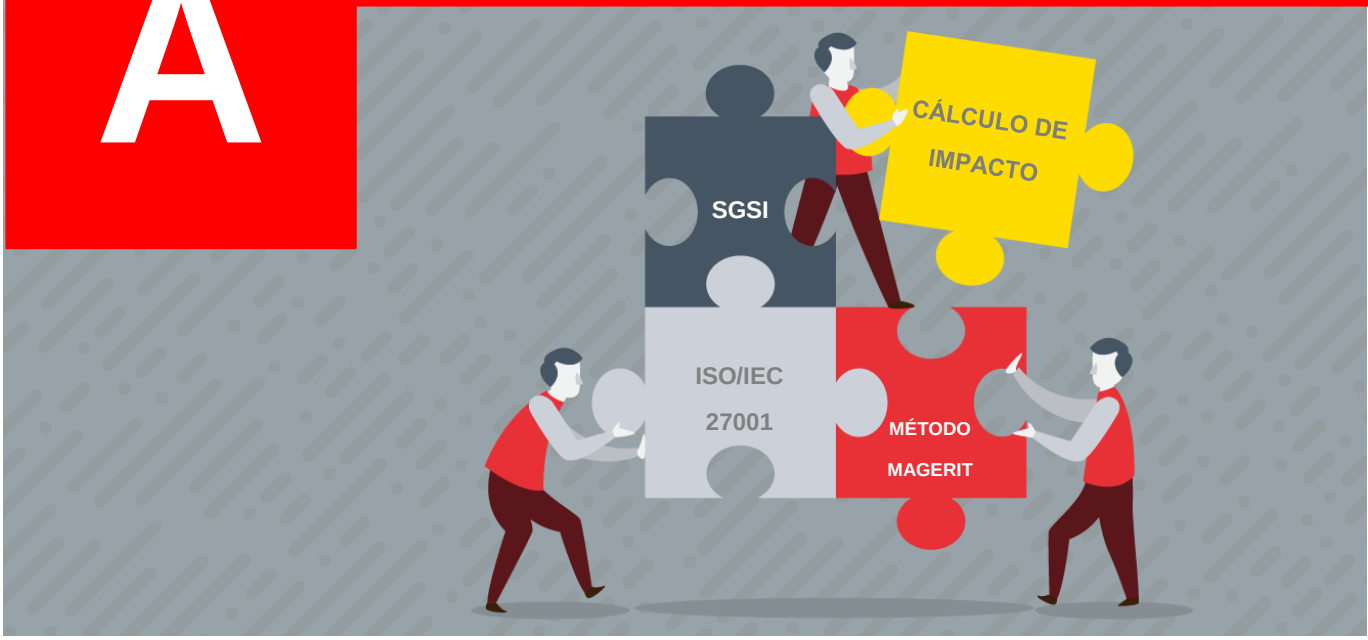
La comunicación de cierre de incidente se realizará a través del canal habitual de comunicación o mediante un correo electrónico informando del tipo de resolución alcanzado. En el caso de que el valor de resolución de un incidente no sea satisfactorio, el afectado puede solicitar su modificación respondiendo al mensaje de cierre del caso indicando con las causas del ataque así como las soluciones aportadas para su resolución.

El valor final asignado al impacto del ciberincidente deberá ser indicado por el afectado ya que, en caso contrario, el valor por defecto será “Impacto no declarado”.

Los valores de cierre adoptados por INCIBE-CERT, y que se detallan en la Guía nacional de notificación y gestión de ciberincidentes, no solo se enfocan en la descripción de la solución aportada por la institución afectada, sino que también tratan de mostrar el nivel de solución al que se ha podido llegar en cada uno de los incidentes.

Para las instituciones afiliadas a RedIRIS, el motivo fundamental se encuentra en que las labores de desinfección/reparación de los recursos afectados suelen ser una tarea interna de cada institución y trivial frente al conocimiento exhaustivo de sus causas. Tener una información detallada sobre las causas que han originado cierta actividad maliciosa permite, entre otras cosas, ayudar a otros afectados a resolver problemas similares, así como tener una fuente de conocimiento de la que toda la comunidad pueda sacar provecho.

A REFERENCIA: CÁLCULO DE IMPACTO



A continuación se muestran una serie de posibles consecuencias causadas por el ciberincidente asociadas a determinados niveles de impacto.

Los criterios para el cálculo del impacto se recogen en la **Guía nacional de notificación y gestión de ciberincidentes**. Con el ánimo de facilitar a ciudadanos, empresas y entidades afiliadas a RedIRIS las labores de cálculo de impacto de un incidente de seguridad se proponen, a modo orientativo, criterios adicionales a los incluidos en la **Guía nacional de notificación y gestión de ciberincidentes**, basados en escalas de análisis de riesgos de Sistemas de Gestión de la Seguridad de la Información (SGSI), buenas prácticas generalmente aceptadas y en la metodología Magerit v.3.0.

Esta tabla se expone a modo orientativo para apoyar las labores de cálculo de impacto de un incidente de seguridad.

NIVEL DE IMPACTO	IMPACTOS POTENCIALES DEL CIBERINCIDENTE	CRITERIOS / POSIBLES CONSECUENCIAS
CRÍTICO	**Imagen y reputación:** problemas en las relaciones con clientes, proveedores y otros stakeholders claves del sector e impacto negativo en medios de comunicación.	▪ El número de clientes, proveedores y otros *stakeholders* claves del sector que se ven afectados por la perturbación del servicio es extremadamente alto. ▪ Daños de reputación elevados y cobertura continua en medios de comunicación internacionales.
	Estrategia: poner en riesgo la consecución de uno o más objetivos de empresa.	▪ El alcance del impacto afecta a la consecución de más del 90% de los objetivos de la empresa.

	Cumplimiento legal: incumplimiento de legislación en materia de datos de carácter personal e incumplimiento de otras obligaciones legales (leyes y regulaciones específicas) que le sean de aplicación a la empresa.	▪ El ciberincidente probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.
	Gestión responsable y sostenibilidad: incumplimiento de compromisos de gestión responsable y sostenible asumidos voluntariamente por la empresa.	▪ El impacto deriva en un incumplimiento extremadamente grave de los compromisos adquiridos voluntariamente por la empresa con los distintos grupos de interés.
	Presupuesto y costes: causar elevados cambios en el presupuesto o pérdidas excepcionalmente elevadas de muy alto valor económico.	▪ El impacto deriva en un aumento del coste del servicio de más del 90%. ▪ El impacto genera una pérdida de beneficios de más del 90% respecto a los del año anterior.
	Operación: causar interrupciones en las actividades de la empresa pudiendo ocasionar impacto en terceros.	▪ El alcance del impacto afecta a más del 90% de los servicios prestados por la empresa. ▪ El impacto ocasiona una interrupción del/los servicio/s de más de 24 horas.
	Satisfacción: causar incumplimientos en plazos de entrega o prestación de servicios y quejas de los stakeholders que puedan derivar en pérdida de fidelización de la cartera de clientes o de proveedores.	▪ El impacto ocasiona un incumplimiento extremadamente grave de los plazos de entrega establecidos. ▪ El impacto ocasiona pérdidas de más del 90% de la cartera de clientes o de proveedores.
	Seguridad para las personas y/o instalaciones: causar daños y perjuicios a las personas o a las instalaciones corporativas.	▪ El ciberincidente probablemente afecte gravemente a un grupo de individuos. ▪ Las instalaciones corporativas se han visto afectadas de forma extremadamente grave.

	Seguridad para los sistemas: causar daños en los sistemas de información en los que están soportados los servicios prestados por la empresa o en los que se almacena información necesaria para la correcta operativa de los servicios.	▪ El impacto afecta a más del 90% de los sistemas de información de la empresa.
MUY ALTO	**Imagen y reputación:** problemas en las relaciones con clientes, proveedores y otros stakeholders claves del sector e impacto negativo en medios de comunicación.	▪ El número de clientes, proveedores y otros stakeholders claves del sector que se ven afectados por la perturbación del servicio es muy alto. ▪ El impacto negativo en medios de comunicación supondría una destrucción muy grave de la imagen de marca.
	Estrategia: poner en riesgo la consecución de uno o más objetivos de empresa.	▪ El alcance del impacto afecta a la consecución de entre el 76% y 90% de los objetivos de la empresa.
	Cumplimiento legal: incumplimiento de legislación en materia de datos de carácter personal e incumplimiento de otras obligaciones legales (leyes y regulaciones específicas) que le sean de aplicación a la empresa.	▪ El ciberincidente probablemente cause un incumplimiento grave de una ley o regulación.
	Gestión responsable y sostenibilidad: incumplimiento de compromisos de gestión responsable y sostenible asumidos voluntariamente por la empresa.	▪ El impacto deriva en un incumplimiento muy grave de los compromisos adquiridos voluntariamente por la empresa con los distintos grupos de interés.
	Presupuesto y costes: causar elevados cambios en el presupuesto o pérdidas excepcionalmente elevadas de muy alto valor económico.	▪ El impacto deriva en un aumento del coste del servicio de entre el 76% y el 90%. ▪ El impacto genera una pérdida de beneficios de entre el 76% y el 90% respecto a los del año anterior.

	Operación: causar interrupciones en las actividades de la empresa pudiendo ocasionar impacto en terceros.	▪ El alcance del impacto afecta entre el 75% y el 90% de los servicios prestados por la empresa. ▪ El impacto ocasiona una interrupción del/los servicio/s de más de 8 horas.
	Satisfacción: causar incumplimientos en plazos de entrega o prestación de servicios y quejas de los stakeholders que puedan derivar en pérdida de fidelización de la cartera de clientes o de proveedores.	▪ El impacto ocasiona un incumplimiento muy grave de los plazos de entrega establecidos. ▪ El impacto ocasiona pérdidas de entre el 75% y el 90% de la cartera de clientes o de proveedores.
	Seguridad para las personas y/o instalaciones: causar daños y perjuicios a las personas o a las instalaciones corporativas.	▪ El ciberincidente probablemente afecte gravemente a un individuo. ▪ Las instalaciones corporativas se han visto muy gravemente afectadas.
	Seguridad para los sistemas: causar daños en los sistemas de información en los que están soportados los servicios prestados por la empresa o en los que se almacena información necesaria para la correcta operativa de los servicios.	▪ El impacto afecta a más del 75% de los sistemas de información de la empresa.
ALTO	**Imagen y reputación:** problemas en las relaciones con clientes, proveedores y otros stakeholders claves del sector e impacto negativo en medios de comunicación.	▪ El número de clientes, proveedores y otros stakeholders claves del sector que se ven afectados por la perturbación del servicio es alto. ▪ Daños de reputación de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
	Estrategia: poner en riesgo la consecución de uno o más objetivos de empresa.	▪ El alcance del impacto afecta a la consecución de entre el 51% y el 75% de los objetivos de la empresa.

	Cumplimiento legal: incumplimiento de legislación en materia de datos de carácter personal e incumplimiento de otras obligaciones legales (leyes y regulaciones específicas) que le sean de aplicación a la empresa.	▪ El ciberincidente probablemente cause un incumplimiento grave de una ley o regulación.
	Gestión responsable y sostenibilidad: incumplimiento de compromisos de gestión responsable y sostenible asumidos voluntariamente por la empresa.	▪ El impacto deriva en un incumplimiento grave de los compromisos adquiridos voluntariamente por la empresa con los distintos grupos de interés.
	Presupuesto y costes: causar elevados cambios en el presupuesto o pérdidas excepcionalmente elevadas de muy alto valor económico.	▪ El impacto deriva en un aumento del coste del servicio de entre el 51% y el 75%. ▪ El impacto genera una pérdida de beneficios de entre el 51% y el 75% respecto a los del año anterior.
	Operación: causar interrupciones en las actividades de la empresa pudiendo ocasionar impacto en terceros.	▪ El alcance del impacto afecta entre el 51% y el 75% de los servicios prestados por la empresa. ▪
	Satisfacción: causar incumplimientos en plazos de entrega o prestación de servicios y quejas de los stakeholders que puedan derivar en pérdida de fidelización de la cartera de clientes o de proveedores.	▪ El impacto ocasiona un incumplimiento grave de los plazos de entrega establecidos. ▪ El impacto ocasiona pérdidas de entre el 51% y el 75% de la cartera de clientes o de proveedores.
	Seguridad para las personas y/o instalaciones: causar daños y perjuicios a las personas o a las instalaciones corporativas.	▪ El ciberincidente probablemente afecte a un grupo de individuos. ▪ Las instalaciones corporativas se han visto gravemente afectadas.
	Seguridad para los sistemas: causar daños en los sistemas de información en los que están soportados los servicios prestados por la empresa o en los que se almacena información necesaria para la correcta operativa de los servicios.	▪ El impacto afecta a más del 50% de los sistemas de información de la empresa.

MEDIO	**Imagen y reputación:** problemas en las relaciones con clientes, proveedores y otros stakeholders claves del sector e impacto negativo en medios de comunicación.	▪ El número de clientes, proveedores y otros stakeholders claves del sector afectados por la perturbación del servicio es importante. ▪ Daños de reputación apreciables, con eco mediático (amplia cobertura en medios de comunicación).
	Estrategia: poner en riesgo la consecución de uno o más objetivos de empresa	▪ El alcance del impacto afecta a la consecución de entre el 21% y el 50% de los objetivos de la empresa.
	Cumplimiento legal: incumplimiento de legislación en materia de datos de carácter personal e incumplimiento de otras obligaciones legales (leyes y regulaciones específicas) que le sean de aplicación a la empresa.	▪ El ciberincidente probablemente sea causa de incumplimiento leve o técnico de una ley o regulación.
	Gestión responsable y sostenibilidad: incumplimiento de compromisos de gestión responsable y sostenible asumidos voluntariamente por la empresa.	▪ El impacto deriva en un incumplimiento importante de los compromisos adquiridos voluntariamente por la empresa con los distintos grupos de interés.
	Presupuesto y costes: causar elevados cambios en el presupuesto o pérdidas excepcionalmente elevadas de muy alto valor económico.	▪ El impacto deriva en un aumento del coste del servicio de entre el 21% y el 50%. ▪ El impacto genera una pérdida de beneficios de entre el 21% y el 50% respecto a los del año anterior.
	Operación: causar interrupciones en las actividades de la empresa pudiendo ocasionar impacto en terceros.	▪ El alcance del impacto afecta entre el 21% y el 50% de los servicios prestados por la empresa. ▪
	Satisfacción: causar incumplimientos en plazos de entrega o prestación de servicios y quejas de los stakeholders que puedan derivar en pérdida de fidelización de la cartera de clientes o de proveedores.	▪ El impacto ocasiona un incumplimiento alto de los plazos de entrega establecidos. ▪ El impacto ocasiona pérdidas de entre el 21% y el 50% de la cartera de clientes o de proveedores.

	Seguridad para las personas y/o instalaciones: causar daños y perjuicios a las personas o a las instalaciones corporativas.	▪ El ciberincidente probablemente afecte a un individuo. ▪ Las instalaciones corporativas se han visto afectadas de forma importante.
	Seguridad para los sistemas: causar daños en los sistemas de información en los que están soportados los servicios prestados por la empresa o en los que se almacena información necesaria para la correcta operativa de los servicios.	▪ El impacto afecta entre el 21% y el 50% de los sistemas de información de la empresa.
BAJO	**Imagen y reputación:** problemas en las relaciones con clientes, proveedores y otros stakeholders claves del sector e impacto negativo en medios de comunicación.	▪ El número de clientes, proveedores y otros stakeholders claves del sector que se ven afectados por la perturbación del servicio es mínimo. ▪ Daños de reputación puntuales, sin eco mediático.
	Estrategia: poner en riesgo la consecución de uno o más objetivos de empresa.	▪ El alcance del impacto afecta a la consecución de hasta un 20% de los objetivos de la empresa.
	Cumplimiento legal: incumplimiento de legislación en materia de datos de carácter personal e incumplimiento de otras obligaciones legales (leyes y regulaciones específicas) que le sean de aplicación a la empresa.	▪ El ciberincidente pudiera causar el incumplimiento leve o técnico de una ley o regulación.
	Gestión responsable y sostenibilidad: incumplimiento de compromisos de gestión responsable y sostenible asumidos voluntariamente por la empresa.	▪ El impacto deriva en un incumplimiento menor de los compromisos adquiridos voluntariamente por la empresa con los distintos grupos de interés.
	Presupuesto y costes: causar elevados cambios en el presupuesto o pérdidas excepcionalmente elevadas de muy alto valor económico.	▪ El impacto deriva en un aumento del coste del servicio de hasta un 20%. ▪ El impacto genera una pérdida de beneficios de hasta el 20% respecto a los del año anterior.

	Operación: causar interrupciones en las actividades de la empresa pudiendo ocasionar impacto en terceros.	▪ El alcance del impacto afecta hasta el 20% de los servicios prestados por la empresa. ▪
	Satisfacción: causar incumplimientos en plazos de entrega o prestación de servicios y quejas de los stakeholders que puedan derivar en pérdida de fidelización de la cartera de clientes o de proveedores.	▪ El impacto ocasiona un incumplimiento leve de los plazos de entrega establecidos. ▪ El impacto ocasiona pérdidas de hasta el 20% de la cartera de clientes o de proveedores.
	Seguridad para las personas y/o instalaciones: causar daños y perjuicios a las personas o a las instalaciones corporativas.	▪ El ciberincidente pudiera causar molestias a un individuo. ▪ Las instalaciones corporativas se han visto afectadas de forma leve.
	Seguridad para los sistemas: causar daños en los sistemas de información en los que están soportados los servicios prestados por la empresa o en los que se almacena información necesaria para la correcta operativa de los servicios.	▪ El impacto afecta hasta un 20% de los sistemas de información de la empresa.
NULO / SIN IMPACTO	No existe impacto	

Tabla 1. Cálculo de impacto.

La relación entre criterios cualitativos y cuantitativos está basado en la siguiente relación:

Criterio cualitativo	Criterio cuantitativo
Excepcionalmente grave	> 90%
Muy grave	76% – 90%
Grave	51% – 75%
Importante	21% – 50%
Leve / menor	< 20%

Tabla 2. Criterios cualitativos y cuantitativos.

B REFERENCIA: BIBLIOGRAFÍA

- Boletín Oficial del Estado (BOE). *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*. Recuperado de https://www.boe.es/eli/es/rdl/2018/09/07/12/con
- European Union Agency for Network and Information Security (ENISA). *Reference Incident Classification Taxonomy.* Recuperado de https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
- Europol. *Common Taxonomy for Law Enforcement and CSIRTS.* Recuperado de https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts
- Instituto Nacional de Ciberseguridad de España (INCIBE). *Glosario de términos de seguridad. Una guía de aproximación para el empresario.* Recuperado de https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario
- Instituto Nacional de Ciberseguridad de España (INCIBE). *Guía nacional de notificación y gestión de ciberincidentes*. Recuperado de https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes
- Ministerio de Hacienda y Administraciones Públicas. *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Libro II - Catálogo de Elementos. Recuperado de https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf
- National Institute of Standards and Technologies (NIST). *Computer Security Incident Handling Guide*. Recuperado de https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- Reference Security Incident Taxonomy Working Group. *Reference Security Incident Classification Taxonomy*. Recuperado de https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md

incibe cert_

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 AYUDA EN CIBERSEGURIDAD