CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

INTECO (cert)

IDENTIFICACIÓN Y REPORTE DE INCIDENTES DE SEGURIDAD PARA OPERADORES ESTRATÉGICOS

Guía básica de protección de Infraestructuras Críticas

INTECO Instituto Nacional de Tecnologías de la Comunicación

www.inteco.es
@intecocert

Diciembre 2013

INDICE

Autores

Jesús Díaz Vico

Daniel Fírvida Pereira

Marco Antonio Lozano Merino

Coordinación

Elena García Díez

1 OBJETIVO DE LA GUÍA

Esta guía básica de protección de Infraestructuras Críticas relativa a la Identificación y Reporte de incidentes de seguridad para operadores estratégicos tiene como finalidad servir de manual de actuación para el reporte y gestión de incidentes relacionados con las Infraestructuras Críticas (IICC) y los Operadores Estratégicos, a través del Centro de Respuesta a Incidentes de Seguridad de INTECO (INTECO-CERT).

Destacar que la respuesta a incidentes en IICC se realiza desde INTECO en estrecha colaboración con el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) a través del CERT de Seguridad e Industria.

El funcionamiento de dicho servicio de respuesta incluye el reporte a INTECO-CERT y CNPIC de los propios incidentes de seguridad, su análisis y el escalado necesario para poder gestionar su resolución y dar una respuesta por parte de INTECO-CERT a los operadores con las recomendaciones oportunas que permitan reducir el riesgo para la seguridad que suponga dicho incidente.

Para facilitar una gestión más adecuada, en este documento se definen también las pautas y actuaciones que pueden adoptar los operadores que puedan estar sufriendo un incidente, así como las categorías y niveles de criticidad del mismo. Esta información se incluirá al tratar cada incidente en el sistema de gestión de incidentes (en adelante RTIR, de *Request Tracker Incident Response*).

Como guía de identificación y reporte de incidentes de seguridad, aunque se incluyen cuestiones específicas que pueden ser sólo de aplicación al caso concreto que se desarrolla, los criterios generales que aquí se exponen 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.

Esta publicación técnica se enmarca en las acciones específicas del CERT de Seguridad e Industria en su línea de trabajo de protección de Infraestructuras Críticas definida en el convenio suscrito en octubre de 2012 por la Secretaria de Estado de Seguridad (SES), dependiente del Ministerio del Interior, y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), dependiente del Ministerio de Industria, Energía y Turismo, para la cooperación efectiva en materia de ciberseguridad entre CNPIC, FCSE e INTECO.

2 ACTUACIONES ANTE UN INCIDENTE

Ante un incidente de seguridad, el objetivo principal es **recuperar el nivel habitual de funcionamiento de los sistemas o servicios** en cuanto a su calidad y disponibilidad, minimizando las pérdidas todo lo posible.

El proceso para conseguir recuperar dicho nivel habitual, así como las acciones para mitigar las posibles consecuencias del incidente, o el proceso de adquisición y análisis de evidencias, conforman el conjunto de actuaciones que deben afrontarse ante un incidente de seguridad.

A continuación se describen las actuaciones para la mitigar los efectos de incidentes de seguridad y recuperar los sistemas afectados, incluyendo un flujograma de las mismas.

RESPUESTA

Las fases principales de respuesta ante un incidente, mostradas en la Imagen 1, pueden resumirse en: **identificación**, **contención y mitigación**, **preservación de evidencias** y **consideraciones legales**, **recuperación** y **documentación**[1].

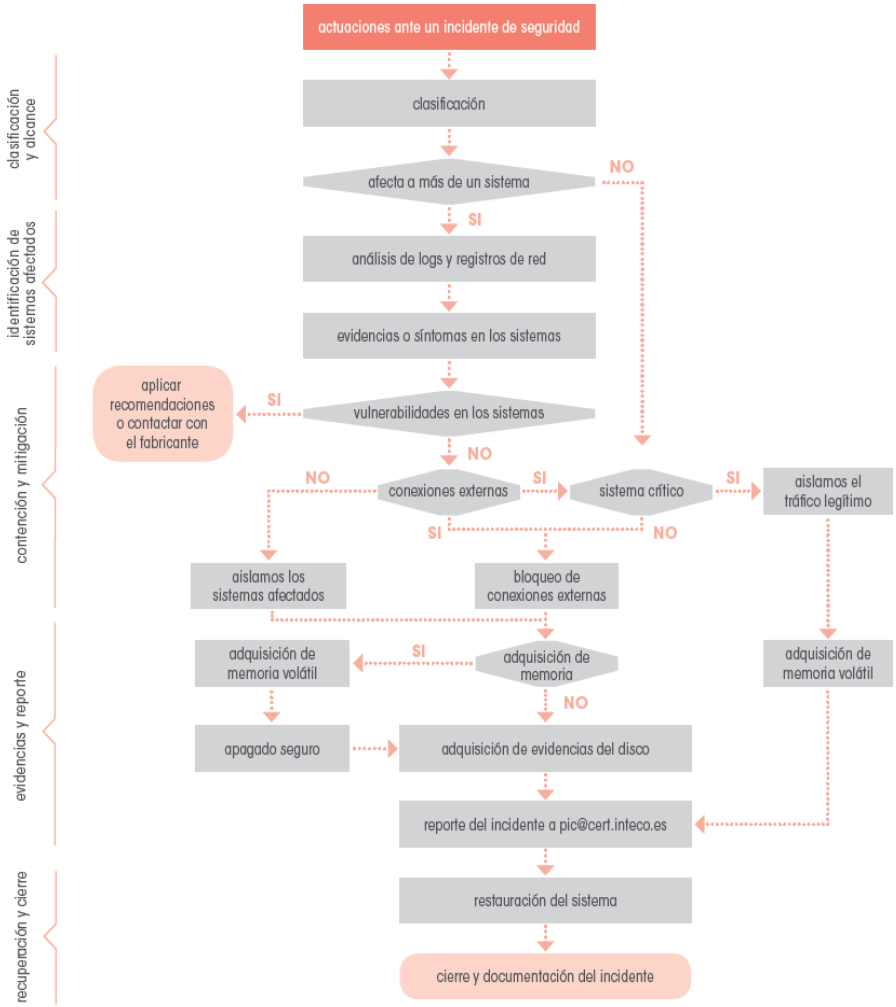

Imagen 1. Flujograma de actuación ante un incidente de seguridad

[1] http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

IDENTIFICACIÓN

Para identificar un incidente de seguridad, determinar su alcance y los sistemas afectados por el mismo, se pueden obtener indicios de múltiples maneras en función de la naturaleza y tipo de incidente. Uno de los principales mecanismos es el análisis de *logs,* registros y fuentes de información para detectar anomalías. Sin ánimo de exhaustividad, fuentes de información a considerar en este punto son:

- Consolas de antivirus.
- Sistemas de Detección / Prevención de Intrusión (IDS/IPS).
- Alertas de sistemas de correlación de eventos de seguridad o SIEM.
- Registros de auditoría para detectar intentos de acceso no autorizados.
- Registro de conexiones bloqueadas en los cortafuegos.
- Registro de conexiones realizadas a través de proxys corporativos.
- Registros en herramientas DLP (Data Loss Prevention).
- Bloqueo de cuentas de usuario u otras anomalías reportadas en masa al CAU o que impliquen algún riesgo como pérdidas de USBs o equipos portátiles.
- Consumos excesivos y repentinos de memoria o disco en servidores.
- Anomalías de tráfico como picos de consumo a horas no habituales.
- Volcados de red, mediante port mirroring por ejemplo, que permitan confirmar alguna sospecha de incidente.

La detección de este tipo de anomalías permite identificar un posible incidente de seguridad, así como la naturaleza o el alcance del mismo. En el caso de que alguno de estos registros presentase alguna anomalía, sería necesario su análisis detallado para determinar si realmente existe un incidente.

Este análisis se puede realizar, por ejemplo, mediante la detección de tráfico de red malicioso, identificando la infraestructura afectada, las direcciones de origen y destino, valores de puertos utilizados, TTL, protocolos, etc.

Estas acciones ayudarán a determinar si realmente hay un incidente de seguridad y su naturaleza.

A nivel de sistema, algunos ejemplos para conocer si está siendo afectado por un incidente son:

- Cuentas de usuario inusuales en el sistema o especialmente privilegiadas.
- Ficheros ocultos o con tamaños, nombres o ubicaciones sospechosas, pudiendo indicar los mismos algún tipo de fuga de información o registro por parte de algún malware.
- Ficheros con permisos inusuales, con *SUID* o *GUID* 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 principales técnicas que el malware utiliza para asegurar su persistencia en el sistema infectado.
- Procesos y servicios inusuales, no sólo servicios a la escucha, si no con 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 las *botnets*.
- Cargas excesivas de disco o memoria pueden estar producidas 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 un elevado número de conexiones con algún *flag* TCP activado de manera anómala y que pudiera evidenciar un ataque de denegación de servicio.

- 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 mediante por ejemplo fuerza bruta.
- Reporte del antivirus corporativo o de alguna herramienta habitualmente instalada en el sistema de identificación de *rootkits*, de control de integridad de ficheros, firma de los binarios, etc. No es recomendable instalar *ad hoc* estas herramientas en un sistema sospechoso ya que pueden alterar las fechas de acceso de los sistemas y suponer una pérdida de evidencias.

Aunque en la organización se contemplen todas estas medidas para identificar un incidente de seguridad y el equipo o equipos afectados, no es descartable que la identificación del incidente se produzca a través de una fuente de información externa, un reporte de un CERT o de otro organismo, de un usuario externo a la organización, etc.

CONTENCIÓN Y MITIGACIÓN

Identificado el incidente, hay que contenerlo y mitigar sus efectos usando la información obtenida anteriormente. Para ello es esencial definir la extensión, el tipo de equipos afectados y buscar las características comunes para poder aislar el incidente en función de esos patrones.

De igual manera, es muy importante el nivel de preparación del que se disponga. Herramientas como un inventario de activos actualizado, un mapa de la arquitectura de red, detectores de intrusos IDS/IPS, correladores de eventos (SIEM) o cortafuegos ayudarán a determinar con más precisión la naturaleza del incidente y cómo contenerlo.

Detectado el incidente, es clave definir la extensión del mismo, si se trata de una infección, así como el tipo de equipos a los que afecta, buscando las características comunes (plataforma de sistema operativo, tipo concreto de puestos de trabajo, solo servidores, etc.) para determinar la extensión de la infección y poder tomar medidas de aislamiento en función de los patrones identificados.

Las principales recomendaciones para la contención y mitigación de un incidente de seguridad y que pueden aplicarse en esta fase son:

- Desconectar el equipo o segmento de red del resto de redes de la organización. Esto puede hacerse si se trata de un equipo aislado directamente desconectando el cable de red del mismo o aislando un segmento de red en una VLAN o similar.
- En caso de tratarse de algún equipo crítico puede aislarse únicamente el tráfico estrictamente necesario mediante la colocación de algún firewall entre ese elemento y el resto de la red, permitiendo solamente el tráfico crítico para el funcionamiento del sistema.
- Si el tipo de incidente ha sido identificado y se conocen tanto detalles técnicos del mismo como los vectores de propagación de un malware, el patrón de comportamiento de una denegación de

servicio, o las características de un intento de intrusión mediante fuerza bruta, es posible aplicar medidas de contención más ajustadas a cada circunstancia. Por ejemplo, bloqueando determinados emails, el acceso a unidades compartidas, conexiones salientes, o cualquier vector de infección mediante malware a través de políticas o reglas en cortafuegos. De igual manera, en el IDS/IPS es posible programar reglas de filtrado para denegaciones de servicio o intentos de intrusión.

- En el caso de una vulnerabilidad que permita alguna intrusión o algún tipo de denegación de servicio se deben aplicar todas las recomendaciones de mitigación proporcionadas por el fabricante del producto, e instalar los parches recomendados. Si se trata de un sistema crítico en el que por algún motivo no sea posible aplicar el parche o las recomendaciones de mitigación, lo correcto es ponerse en contacto con el fabricante para valorar y obtener soluciones alternativas.

FUGAS DE INFORMACIÓN Y ADQUISICIÓN DE EVIDENCIAS

Para evitar fugas de información es clave identificar cuál es el vector de la fuga y, sobre él, adoptar las medidas técnicas adecuadas que limiten su explotación, ya sea restringir el acceso a carpetas compartidas, deshabilitar sistemas de almacenamiento portátil como USBs, bloqueo de URLs o de emails, etc.

Además de esta contención, se deben cuantificar las repercusiones de esa fuga de información. Podría darse el caso de que la fuga de información hiciese referencia a las credenciales de acceso de un usuario a algún sistema de la organización y que hubiesen sido expuestas públicamente. En estos casos es necesario contemplar la implicación del equipo legal, de RRHH y de comunicación de la empresa para trazar una estrategia global ante dicha fuga de información.

Una vez que se ha identificado un incidente de seguridad, los equipos afectados y se han aislado los mismos del resto de la red, se debe tener en cuenta, dentro de la estrategia de contención, la preservación de evidencias para el análisis forense del incidente y, dentro de dicha preservación, deben extraerse los datos volátiles de la memoria antes de proceder al apagado del sistema.

La información almacenada en la memoria del equipo puede resultar muy importante para el proceso de análisis en casos de malware o de intrusiones y, si se apaga el sistema, se perderían, por lo que en la medida de lo posible se han de aplicar técnicas forenses para su adquisición antes de apagarlo.

Para realizar esta adquisición es posible utilizar herramientas forenses destinadas a este fin, procurando en todo momento no alterar el sistema ni los datos del mismo, ya que puede corromperse información importante como fechas de acceso a ficheros, o incluso eliminar evidencias.

Adquiridos los datos, es importante añadir mecanismos para la preservación de su integridad, mediante la aplicación de funciones hash criptográficas apropiadas. En este aspecto, hay varios criterios a tener en cuenta.

Por un lado, la mayoría de las herramientas de análisis forense soportan las funciones MD5 y SHA1, mientras que funciones más avanzadas, como las de la familia SHA2 no tienen un soporte tan amplio. Por otra parte, MD5 y SHA1 conllevan un coste computacional menor, a cambio de una seguridad criptográfica algo menor también, mientras que las funciones SHA2 son más robustas ante colisiones a costa de una carga computacional mayor. Esto es efectivamente un factor importante, ya que los volcados de memoria típicamente serán de al menos 512 MB. Por lo tanto, la decisión final dependerá de los recursos disponibles (herramientas y capacidad de cómputo),

siendo inevitable realizar un balance entre coste y seguridad. Una solución que probablemente ofrezca una robustez y costes aceptables en la mayoría de los casos podría ser obtener tanto el hash MD5 como el hash SHA1 de los datos a respaldar.

Las principales herramientas para la adquisición de los datos volátiles de la memoria y que se pueden utilizar son:

- En sistemas UNIX/Linux, la herramienta LiME desde un dispositivo USB conectado al sistema comprometido, teniendo en cuenta que la herramienta debe estar compilada con el mismo *kernel* que el sistema comprometido y que deben incluirse en el USB las librerías necesarias.
- También en sistemas UNIX/Linux, está disponible la herramienta Volatility. Como la anterior, también se puede utilizar desde un dispositivo USB con una versión compilada para la misma versión del *kernel* que el del sistema e incluirse en el USB las librerías necesarias.
- En sistemas Windows, herramientas como FTK Imager, DumpIT, Memory DD o Memoryze para realizar un volcado de la memoria del sistema, de los ficheros de paginación, o de los procesos. También, con la herramienta Volatility, es posible realizar un análisis de los datos extraídos.
- En sistemas virtualizados, la memoria RAM se encuentra en ficheros *.sav* en el caso de VirtualBox y en ficheros *.vmen* en el caso de VMWare.

Una vez completado este proceso de adquisición de datos volátiles de la memoria ya se puede proceder a apagar el sistema. Para ello, y con el fin de evitar algún comportamiento desconocido del malware o del posible *rootkit* utilizado por el intruso durante el apagado, lo más recomendable es proceder a un corte de energía repentino del sistema, desenchufando directamente el cable de energía.

RECUPERACIÓN

Habiendo garantizado la preservación de evidencias y reportado el incidente, hay que proceder a la recuperación de los sistemas afectados.

En caso de incidentes de seguridad provocados por una intrusión o malware en sistema que no resultan críticos, una vez detectado el vector de infección o de intrusión en el sistema y establecidas las medidas correctivas oportunas para evitar que el incidente se reproduzca nuevamente, se puede proceder a restaurar el sistema afectado por el incidente mediante un *backup* que haya sido realizado anteriormente a la infección.

En sistemas críticos sobre los que no exista alta disponibilidad, habrá que valorar añadir al plan de continuidad del negocio la realización de copias periódicas de todo el sistema, no sólo de los datos. Esto puede permitir recuperar la actividad normal en caso de incidentes como los ocasionados por

[2] LiME: http://code.google.com/p/lime-forensics/

[3] Volatility: http://code.google.com/p/volatility/

[4] FTK Imager: http://www.accessdata.com/support/product-downloads/ftk-download-page

[5] DumpIT: http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7

[6] Memory DD: http://sourceforge.net/projects/mdd/

[7] Memoryze: http://www.mandiant.com/resources/download/memoryze/

un malware o una intrusión, teniendo en cuenta que se debe evitar o bloquear el vector de ataque o de infección que afectó al sistema original.

En cualquier caso, en sistemas críticos siempre se deben seguir las instrucciones del fabricante del producto para su restauración o reinstalación, programando los mantenimientos correctivos y paradas de sistemas necesarias para llevar a cabo la recuperación del incidente.

De igual manera, en incidentes relacionados con vulnerabilidades siempre habrán de seguirse las recomendaciones del fabricante para mitigar o solucionar la vulnerabilidad, aplicando los parches oficiales liberados por el desarrollador.

DOCUMENTACIÓN

En la gestión de incidentes de seguridad resulta de gran importancia documentar todo lo aprendido en incidentes anteriores. Esas lecciones aprendidas pueden resultar vitales para evitar futuros incidentes de seguridad o solucionar nuevos incidentes con similares características.

Es importante que esta documentación resulte muy detallada, permitiendo conocer qué herramientas se utilizaron y cómo, las investigaciones realizadas y sus resultados, las colaboraciones que se necesitaron, la documentación utilizada para resolver el incidente, la línea temporal de las acciones seguidas, etc.

Esto sirve para conocer con exactitud la naturaleza y tipo de incidente, las características del mismo y los vectores de infección con malware o intrusión para parametrizar los sistemas de seguridad de manera adecuada. Pero también para iniciar campañas de sensibilización adaptadas a la organización, conocer sus puntos más débiles y saber cómo protegerlos.

También permite conocer a los atacantes, sus estrategias y sus patrones en las denegaciones de servicio. Las nuevas vulnerabilidades que afectan los sistemas más críticos de la organización también ayudarán en gran medida a prevenir y solucionar los posibles incidentes de seguridad.

Todas estas acciones técnicas y procedimentales de la organización deben tener siempre en cuenta las consideraciones legales que apliquen a la organización por su sector o ámbito, pero también otras como los principios del secreto de las comunicaciones y privacidad de las personas, el código penal, etc. y que requieran ser tenidas en cuenta durante el proceso de resolución de un incidente, en especial en la toma y adquisición de evidencias que se deriven en un caso de análisis forense.

3 REPORTE DE INCIDENTES

Una de las tareas de INTECO-CERT y CNPIC es la respuesta a incidentes de seguridad en IICC reportados por los usuarios de este servicio siendo necesario que toda la información relativa a los mismos se almacene en RTIR.

Para ello se detalla en los siguientes puntos la información necesaria para realizar un correcto reporte de información por parte de los operadores así como facilitar las comunicaciones entre INTECO-CERT, CNPIC y dichos operadores siguiendo el esquema mostrado en la Imagen 2.

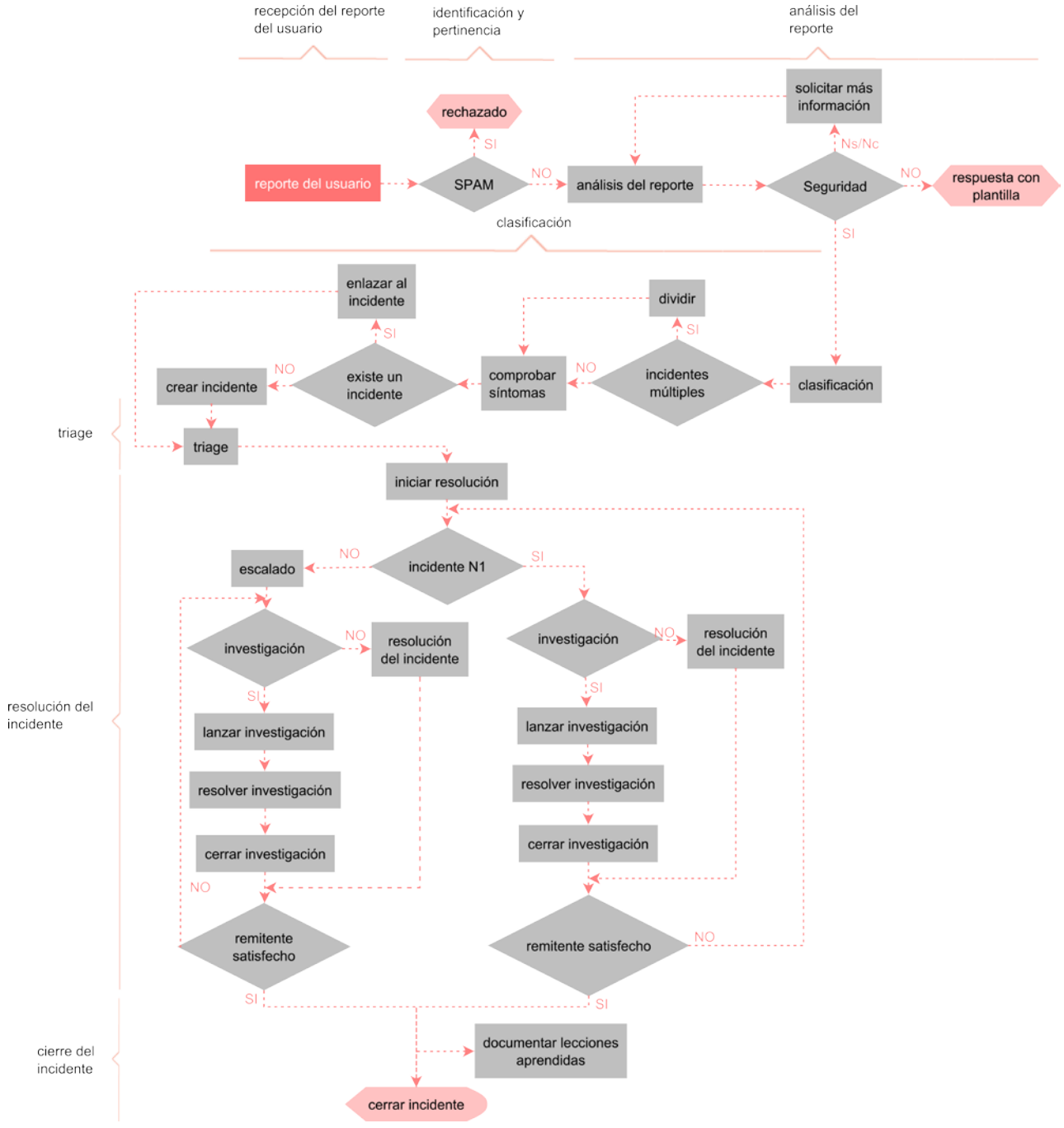

Imagen 2. Pasos para reportar un incidente

CÓMO REPORTAR

Los incidentes de seguridad se reportan a través del usuario que, identificado como punto de contacto de la organización, y en representación de la misma, accede al servicio de respuesta a incidentes a través de un correo al buzón pic@cert.inteco.es. Con ésta información se generará un Reporte de Incidente en RTIR.

Todos los intercambios de información con el usuario se realizan por correo electrónico desde RTIR, desde la dirección pic@cert.inteco.es y con un campo estándar en el asunto [INTECO-CERT/CNPIC #***]. Siendo *** el número del reporte creado por el usuario. De esta forma, todos los correos intercambiados se almacenarán en el mismo reporte, para tener un seguimiento completo del mismo.

Como excepción, se podrá contactar con determinados usuarios a través de teléfono en caso de necesidad, si se considera que el incidente es suficientemente relevante, que será complementaria al tratamiento general detallado a continuación.

Todos los correos enviados desde la cuenta pic@cert.inteco.es serán firmados digitalmente con la clave privada perteneciente a dicha cuenta. Además, cuando la información intercambiada sea confidencial (envío de logs con credenciales, datos confidenciales o personales, etc.), dichos correos también deberán ser cifrados por el técnico de INTECO-CERT que realiza la notificación.

INFORMACIÓN NECESARIA

La información que debe incluir un reporte de un incidente de seguridad para la generación del mismo en la herramienta RTIR por parte del técnico de INTECO-CERT debe incluir toda la información que el usuario considere necesaria para la resolución del mismo. Por ejemplo, la descripción del mismo, los elementos implicados, versiones de software, naturaleza o tipo de incidente si el usuario lo sabe, los datos de IPs/hosts implicados, etc.

Con esta información, el moderador de la cola de incidentes de RTIR que ha recibido y registrado el reporte creará un incidente nuevo desde el reporte del usuario. En este incidente se incluyen los siguientes datos:

- **Asunto:** Frase que describe de forma general el incidente. Este campo lo heredarán todas las investigaciones que se abran asociadas a ese incidente.

  Por defecto, aparece el campo asunto del reporte a partir del que se ha creado, por lo que se puede mantener o cambiar por un nombre más explicativo con el siguiente formato:

  - ***[Nombre de la empresa]* Texto descriptivo de la incidencia***

    - ** Sólo si es identificada*

- **Descripción:** Es una breve descripción del incidente. El moderador de la cola utilizará este campo para aportar comentarios importantes sobre el incidente.

- **Función:** Consulta o Incidente. Por defecto Incidente.

- **Clasificación:** Define el tipo de incidente de acuerdo a las categorías definidas en el apartado de Tipos de Incidentes de este documento.

- **Nivel:** Seleccionando el nivel de soporte que tratará el incidente, según los niveles definidos en el apartado de Escalado de Incidentes de este documento. Por defecto será el nivel 1.

- **Mensaje:** Por defecto se hereda el cuerpo del mensaje del reporte del usuario. El moderador aportará comentarios en caso de necesidad y eliminará los campos del formulario que el usuario ha dejado en blanco.

  Este mensaje también incluirá toda la información que haya podido extraer el personal del operador estratégico durante la identificación del incidente, incluyendo ficheros, volcados de memoria y cualquier información que aplique al incidente.

- **Prioridad:** Marca el nivel de prioridad del incidente, según la clasificación del mismo estará enmarcado en uno u otro. Los niveles de prioridad están definidos en el apartado de Clasificación y Priorización de este documento.

CLASIFICACIÓN Y PRIORIZACIÓN

Para proporcionar desde INTECO-CERT respuestas/soluciones consistentes y oportunas al usuario y asegurar que la información sensible se maneje de manera apropiada, se debe realizar una correcta clasificación y priorización de los incidentes desde el momento que se registran en RTIR. No obstante, por parte de INTECO-CERT pueden modificarse las tipologías y prioridades de incidentes de seguridad durante la resolución del incidente, quedando registrado en RTIR los valores contemplados.

Según la prioridad de los incidentes, los diferentes niveles contemplados son los siguientes:

- **Alta** Incidentes que afectan a sistemas o información críticos para el operador y que puedan potencialmente tener impacto en el negocio.

Estos incidentes son típicamente malware destructivo, denegación de servicios o sistema comprometido, y ciertos incidentes de *hacking* y violación de políticas que afecten a sistemas críticos.

- **Media:** Incidentes que afectan a sistemas o información no críticos para el operador o cuyo impacto no repercute directamente en el devenir del negocio.

En esta categoría se incluyen la mayoría de incidentes de *hacking* y *phishing*. También se incluirán ciertos casos de violación de políticas y otras consultas.

- **Baja:** Son posibles incidentes en sistemas no críticos para el operador, investigaciones que impliquen análisis forenses que se alarguen en el tiempo o consultas genéricas sobre seguridad.

Este nivel incluye la mayoría de consultas y ataques de invasión, además de algún incidente de cualquier otro tipo que afecte a sistemas con poco nivel de importancia o bajo impacto en el negocio. Las diferentes categorías de incidentes contempladas son las introducidas en el apartado de Tipos de Incidentes.

ESCALADO DE INCIDENTES

A continuación se describe una metodología de niveles de escalado para dar soporte a la gestión de incidentes de seguridad en INTECO-CERT.

- **Nivel 1:** Los operadores de seguridad de primer nivel realizarán las actividades de atención primaria a los reportes y consultas que lleguen a INTECO-CERT y actuarán ante los incidentes más triviales (que no requieran un nivel experto de seguridad).

  Realizan el seguimiento de todos los reportes e incidentes abiertos y generan toda la documentación necesaria.

  Responden y aportan solución inmediata a ataques o incidencias de seguridad tales como:

  - Respuesta a solicitudes de información (consultas).
  - Ataques conocidos o de identificación inmediata.
  - Monitorización y respuesta ante vulnerabilidad públicas.
  - Identificación de defectos y riesgos en la topología de red o sistemas de seguridad.
  - Identificación de defectos e incidencias en procedimientos y políticas de seguridad internos (sistemas, desarrollo, seguridad,...).

Las incidencias que requieran un conocimiento elevado en seguridad se derivarán al segundo nivel.

- **Nivel 2:** Es un equipo experto que responde ante incidentes que requieren un conocimiento elevado en seguridad, siempre escalados desde el equipo de primer nivel.

  Analizan y responden ante ataques o incidencias de seguridad tales como:

  - Ataques no conocidos o de difícil identificación
  - Análisis de vulnerabilidades sospechosas o incidencias que requieren un nivel de conocimiento propio de un experto.
  - Soporte y consultoría sobre la topología de red existente o configuración adecuada de los dispositivos de seguridad.
  - Identificación de la relación de la incidencia con defectos en los procedimientos o políticas de seguridad y soporte.
  - Evaluación del riesgo e impacto de vulnerabilidades y ataques.
  - Pruebas de Intrusión.
  - Análisis de impacto y riesgo real de vulnerabilidad existentes.

- **CNPIC:** Adicionalmente, el Servicio de Seguridad Lógica del CNPIC estará informado a través de correo electrónico, y puede verse implicado en la gestión del incidente aportando su experiencia específica en alguno de los principales temas relacionados con la protección de las infraestructuras críticas, como pueden ser:

  - Experiencia previa en sistemas de control industrial.
  - Aportando contactos con otros centros u operadores que faciliten una mejor gestión de los incidentes.
  - Realizando notificaciones a contactos de personas dentro de las organizaciones, con las que ya exista relación previa, en caso de necesidad.
  - Legislación aplicable a las PIC en España.

4 TIPOS DE INCIDENTES

Las características del incidente determinan qué acciones habrá que llevar a cabo para resolverlo. En general, se puede considerar los siguientes tipos de incidentes:

- **Denegación de servicio:** Incidentes relacionados con ataques de denegación de servicios (*DoS*) o denegación de servicios distribuida (*DDoS*). Son muy peligrosos, ya que pueden afectar a la disponibilidad de sistemas críticos de los Operadores Estratégicos.
- **Infección por malware:** Incidentes provocados por malware (virus, gusanos, troyanos, bombas lógicas, spyware, *rootkits*, etc.). La gravedad varía según el malware, pudiendo afectar a robos de información, o a la disponibilidad de los sistemas. Lo más complicado es la detección e identificación del mismo debido a la incorporación de *rootkits*.
- **Compromiso del sistema:** Cualquier sistema informático, hardware o software, que está siendo o ha sido atacado con éxito. Por ejemplo: robo de información confidencial, alteración de la configuración del sistema, etc.
- ***Hacking*:** Cualquier actividad o tráfico sospechosos que puedan alterar el funcionamiento del sistema y estén relacionadas con un intento de intrusión. Por ejemplo, tentativas de acceso no autorizado al sistema o escaneo de servicios.
- **Distribución de malware:** Incidentes en los que un servidor público de la organización es utilizado para distribuir malware. Estos incidentes ponen en riesgo la seguridad de terceros.
- **Violación de políticas:** Usos inadecuados de algún activo informático, como escalada desautorizada de privilegios o intentos de evadir los controles de acceso en un sistema.
- **Ataques de invasión:** Cualquier tipo de ataque contra las autorizaciones, autenticaciones, permisos, derechos sobre los archivos o interceptación de correo electrónico.
- **Vulnerabilidad:** Cualquier tipo de incidente provocado por la explotación de una vulnerabilidad en un sistema.

Además de estas tipologías que se podrían considerar comunes, la evolución de las tecnologías y la complejidad de los ataques hace inevitable contemplar la posibilidad de que ocurran otros tipos de incidentes.

5 CONCLUSIONES

En esta guía se han estudiado las acciones que se han de tomar para la identificación y gestión de incidentes de seguridad. En concreto, las actuaciones a tomar ante un incidente comprenden su identificación, contención y mitigación, preservación de evidencias y consideraciones legales, recuperación y documentación.

También se ha detallado el proceso a seguir para reportar los incidentes, utilizando como medio de comunicación principal el **buzón de correo** pic@cert.inteco.es, que se comunica con el sistema RTIR (*Request Tracker Incident Response*). El usuario que reporte el incidente incluirá en dicho email toda la información que considere necesaria que será utilizada por un moderador de la cola de incidentes RTIR para crear un nuevo incidente. Los pasos generales que seguirá el proceso desde que se reporta hasta que se resuelve, son: **recepción** del reporte del usuario**, identificación y pertinencia, análisis** del reporte**, clasificación, triage, resolución del incidente** y **cierre** del incidente.

Además, para facilitar la gestión y reporte de los mismos, se ha proporcionado una clasificación general, dependiendo de las principales características que puedan presentar los posibles incidentes de seguridad. En concreto, se han definido incidentes de denegación de servicio, infecciones por malware, compromisos del sistema, *hacking*, *d*istribución de malware, violación de políticas, ataques de invasión, vulnerabilidades y otros.

Como guía de identificación y reporte de incidentes de seguridad, aunque se han tratado cuestiones específicas que pueden ser sólo de aplicación al caso concreto que se desarrolla, los criterios generales expuestos 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.