

6

RESPUESTA AL **INCIDENTE**



CONTENIDO

- Contención del incidente
- Erradicación del incidente
- Etapa de recuperación
- Recopilación y análisis de evidencias
- Recursos materiales
- Estrategia de comunicación

En esta fase, se continúa con la investigación del incidente, siendo necesario en ocasiones llevar a cabo una recopilación y análisis de evidencias en profundidad (análisis forense, reversing de una pieza de malware...) para ampliar información de la que dispone de forma que las decisiones que se tomen en esta etapa sean las más adecuadas, proporcionadas y ágiles.

A más rapidez de actuación, menor impacto tendrá el incidente, así que en esta etapa el equipo debe estar completamente coordinado y la comunicación entre todos los involucrados debe ser muy fluida.

Esa fase pasa por las siguientes subetapas, que se verán a continuación:

- a. Contención del incidente
- b. Erradicación del incidente
- c. Recuperación tras el incidente

1. CONTENCIÓN DEL INCIDENTE

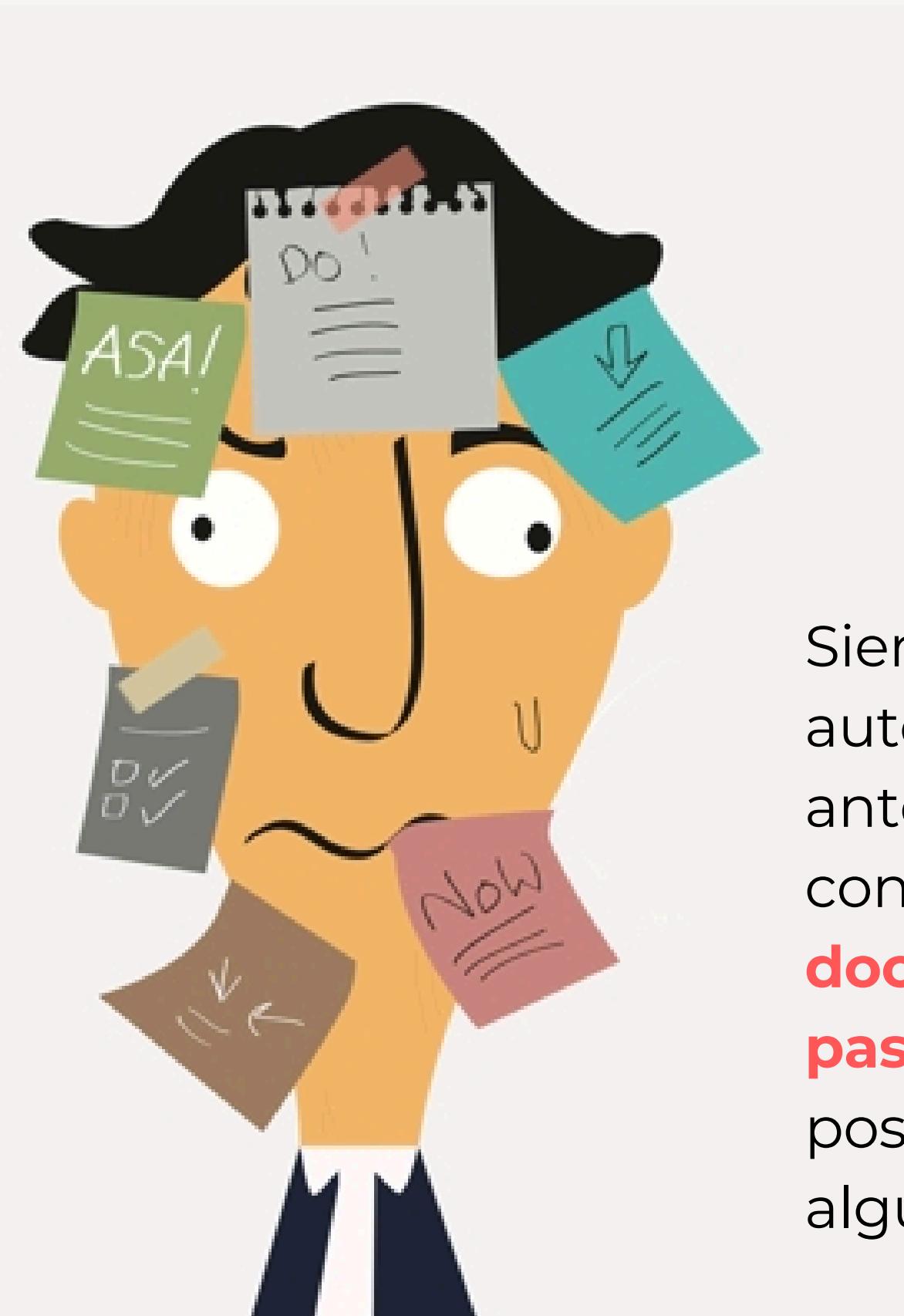
Una vez el plan de respuesta se ha activado, se han valorado de forma adecuada a los datos recopilados y se ha compartido la información con el personal clave, es necesario comenzar a aplicar las medidas de contención necesarias para mitigar el impacto del incidente.

La mayor parte de las medidas de contención son temporales y se eliminarán tras haberse vuelto a la normalidad una vez erradicado el incidente.



Las medidas de contención deben ser proporcionales y ágiles con el objetivo de ganar tiempo y mitigar el impacto del incidente. Además, la experiencia y el conocimiento del equipo implicado en la gestión del incidente será un factor clave durante esa fase.

Es posible que haya que tomar medidas de contención muy drásticas y es por ello que siempre hay que evaluar la situación y consensuar con la dirección las decisiones más importantes



Siempre se debe obtener la autorización de la Dirección antes de iniciar acciones de contención de gran impacto y **documentar en detalle cada paso que se dé**, ya que es posible que haya que revertir algún paso.

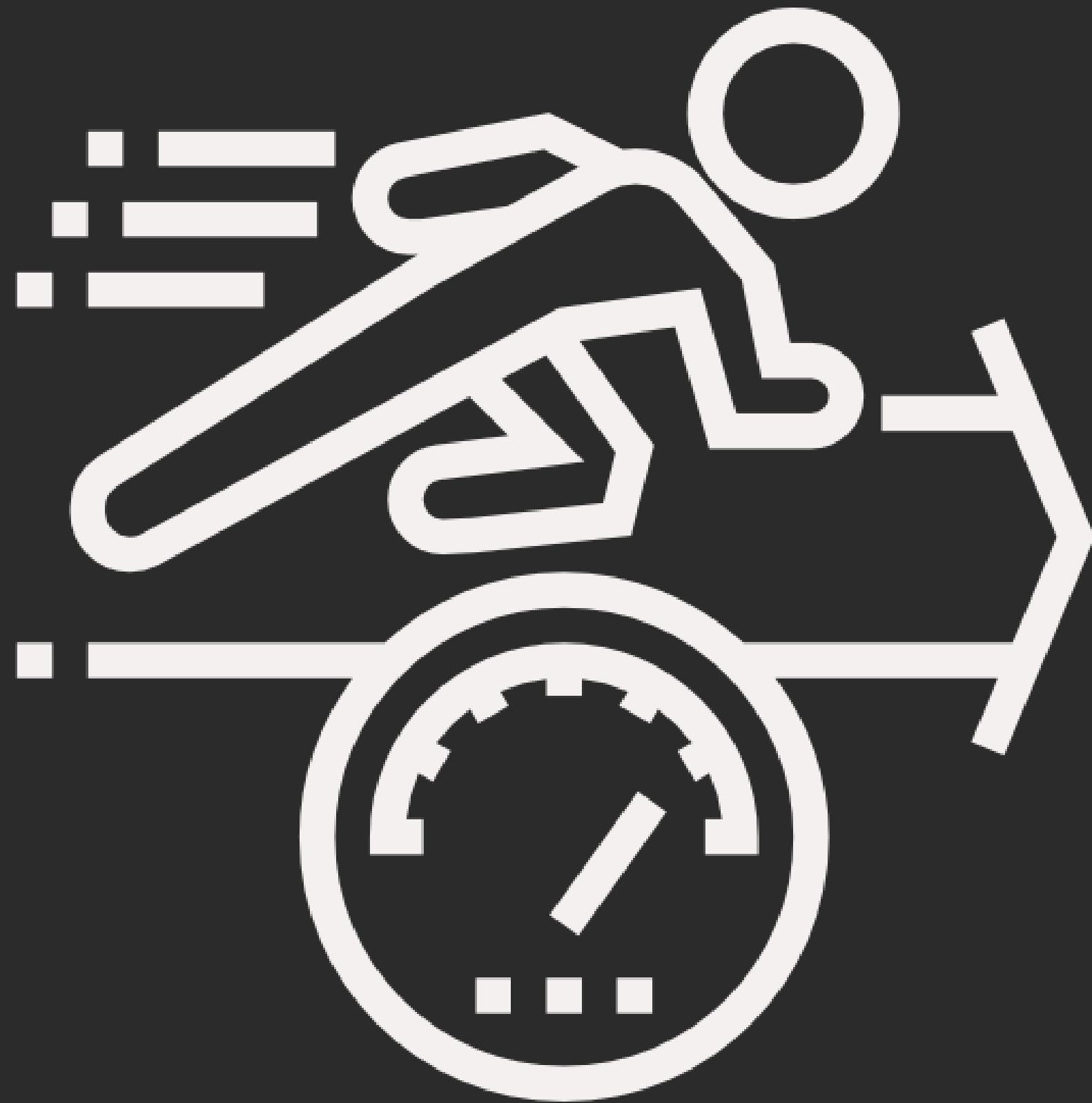
Junior: ¿Dónde está la documentación?



Senior: ¡YO SOY LA DOCUMENTACIÓN!

Ayudándonos de la tecnología que tenemos a nuestra disposición el primer punto para contener el incidente es aislar el problema. Algunas acciones que se podrían tomar, según el escenario en el que nos encontremos podrían ser:

- Cambios en los dispositivos de red (switches, routers, Firewalls) como por ejemplo desconectar un equipo o varios de la red. O en el caso que sea necesario algún segmento de red específico.
- Aislar unidades organizativas en el Directorio Activo
- Considerar técnicas de DNS sinkholding para controlar el tráfico malicioso.
- Bloqueo de determinados correos electronicos
- Bloqueo de determinados dominios o IP externas
- Bloqueo de unidades compartidas
- Bloquear usuarios



La etapa de contención debe durar el mínimo tiempo posible, sobre todo si las medidas adoptadas no permiten un funcionamiento normal de los sistemas TI de la organización.

2. ERRADICACIÓN DEL INCIDENTE

Tras la contención del incidente se procede a tomar paso de las medidas de erradicación. Para ello, y según el tipo de ciberincidente en el que nos encontremos se pueden tomar medidas como:

- Eliminación de cuentas de usuario que hayan podido crear los atacantes.
- Eliminación de ficheros sospechosos
- Ejecutar escaneos a medida por parte del antivirus si el fabricante ha proporcionado reglas para mitigar la situación
- Borrado seguro de los sistemas comprometido si es posible
- Contactar con proveedores externos para mitigación de ataques DDoS
- Realizar cambios de contraseñas de los usuarios afectados
- Aplicar actualizaciones de seguridad pendientes
- Cambios de contraseñas para usuarios, administradores locales, servicios ...

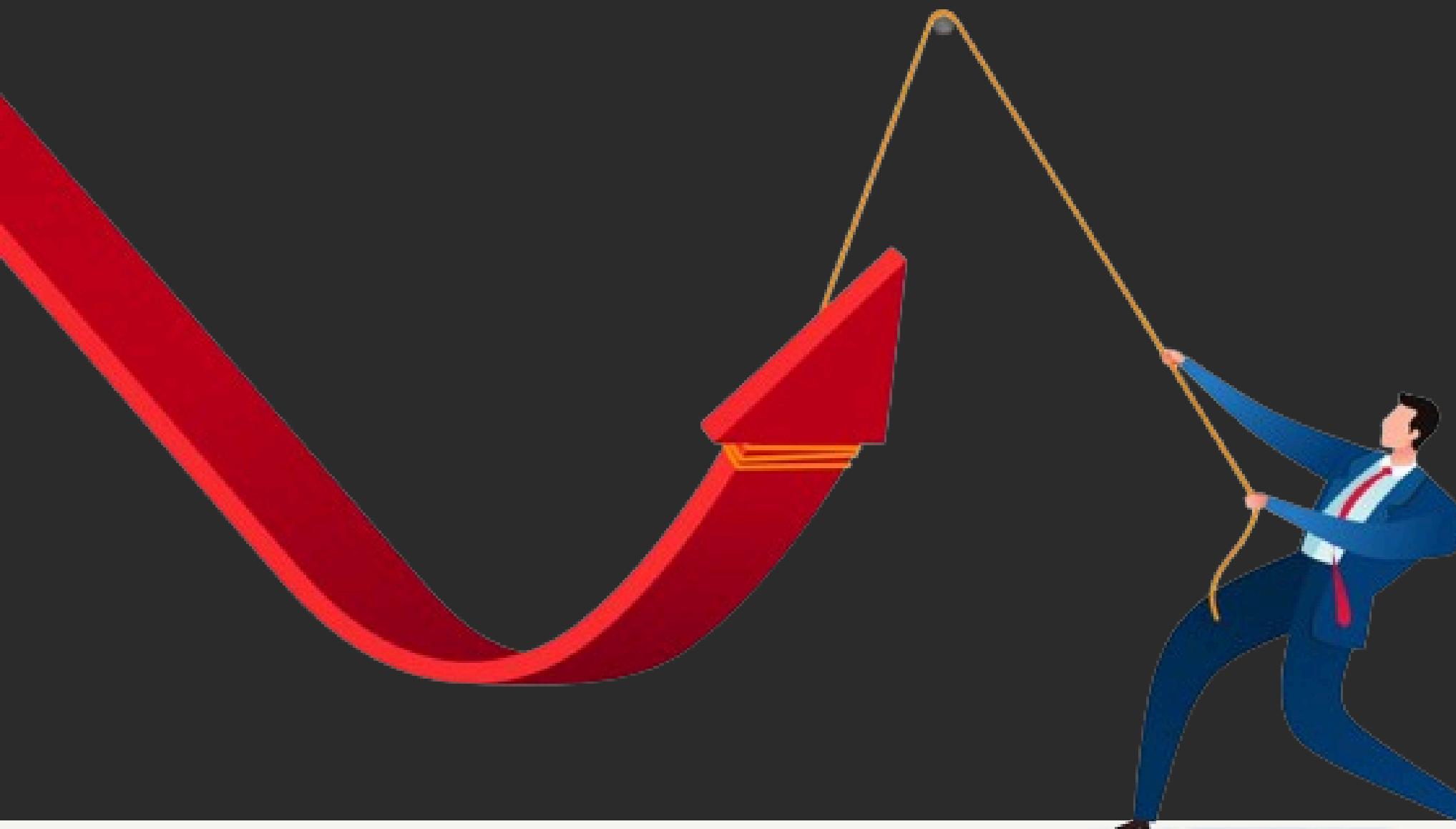
2. ERRADICACIÓN DEL INCIDENTE

Tras la contención del incidente se procede a tomar paso de las medidas de erradicación. Para ello, y según el tipo de ciberincidente en el que nos encontremos se pueden tomar medidas como:

- Eliminación de cuentas de usuario que hayan podido crear los atacantes.
- Eliminación de ficheros sospechosos
- Ejecutar escaneos a medida por parte del antivirus si el fabricante ha proporcionado reglas para mitigar la situación
- Borrado seguro de los sistemas comprometido si es posible
- Contactar con proveedores externos para mitigación de ataques DDoS
- Realizar cambios de contraseñas de los usuarios afectados
- Aplicar actualizaciones de seguridad pendientes
- Cambios de contraseñas para usuarios, administradores locales, servicios ...

3. ETAPA DE RECUPERACIÓN

Una vez se ha dado por erradicada la amenaza la fase siguiente es devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas, si las hay, pueden retomar su actividad.



En esta fase será la dirección, apoyada por el equipo de continuidad de negocio, la responsable de tomar las decisiones marcando las prioridades.

Es recomendable que las organizaciones tengan previsto un Plan de Recuperación ante Desastres y un Plan de Continuidad del Negocio, de vital importancia en esta etapa.



PLAN DE RECUPERACIÓN



PLAN DE CONTINUIDAD DEL NEGOCIO

El proceso debe ser paulatino y bien planificado y antes de comenzar con el mismo, se recomienda realizar una **auditoría exhaustiva** de los sistemas que fueron afectados.

Una vez iniciemos el proceso de recuperación se debe incrementar al máximo la monitorización en busca de cualquier síntoma que pueda indicar que el problema está volviendo a ocurrir; significaría que no se ha hecho correctamente la fase anterior o los atacantes han encontrado un nuevo vector de entrada. (En ese caso, volveríamos a la etapa anterior)



En ocasiones, volver a la normalidad requiere reinstalar los sistemas. Algunas acciones que se podrían tomar serían las siguientes:

- Restauración de datos a través de backups en los sistemas comprometidos y posteriormente desinfectados. En este caso se debe verificar que la copia a restaurar no está contaminada por la amenaza.
- Eliminación de salvaguardas temporales asociadas a la fase de contención
- Reinstalación de sistemas comprometidos o de cuya integridad exista una duda razonable
- Bastionado de los sistemas basándose en códigos de buenas prácticas comúnmente aceptados.



En sistemas OT la restauración o nuevo despliegue de aplicaciones es posible que requiera del apoyo de los fabricantes para la restauración o reinstalación de los sistemas o recuperación de copias de seguridad.



¿QUE ES UN SISTEMA OT?





La tecnología OT se puede integrar con dispositivos ICS (Sistema de control industrial) e IoT (Internet of things), por lo que los pormenores de su ciberseguridad aún pueden resultar poco comunes, y no todos los profesionales en seguridad los han atendido de cerca

En la puesta en marcha podemos establecer 3 escenarios:

RED SUCIA

Se parte de que la organización está totalmente afecta. Por ejemplo, por un ransomware.

RED GRIS

Escenario temporal en el que se pongan en funcionamiento servicios urgentes necesarios para la continuidad del negocio. Esta red deberá ser lo más aislada y completamente monitorizada.

RED LIMPIA

En este escenario final la red deberá ser bastionada, monitorizada y será la red que adoptará permanentemente la organización una vez se ha dado por cerrado el incidente.

4. RECOPILACIÓN Y ANÁLISIS DE EVIDENCIAS

En ocasiones es necesario llevar a cabo un análisis forense de los activos comprometidos. Existen diferentes metodologías, aun así se basan en el mismo concepto del propio incidente que es la recolección de información y su análisis.

El dispositivo a analizar contiene las evidencias digitales que permitirán al investigador forense digital determinar cuándo y cómo tuvo lugar el ataque. Adicionalmente, podrían obtenerse evidencias que demostrarán quién, qué, dónde y por qué realizó el ataque.

Existen dos formas de adquisición de evidencias:



DISPOSITIVOS APAGADOS

Tiene lugar cuando el dispositivo del que se quiere obtener la evidencia está ejecutando el sistema operativo instalado en él.

Los datos volátiles almacenados en la memoria del equipo pueden resultar muy importantes para el proceso de análisis en casos de código dañino o de intrusiones y estos se perderían si se apagara el equipo, por lo que se debe hacer la recogida de evidencias en vivo.

Pasos eficaces para realizar un análisis forense en dispositivos apagados:

- Antes de comenzar el proceso de clonado forense de la evidencia, el soporte de almacenamiento destino debe ser sometido a un proceso de **borrado seguro**.
- Utilizar **write blockers**, evitando que se puedan producir modificaciones en ella durante el proceso de clonado forense.
- Efectuar un **resumen digital (hash)** de la información contenida en el soporte de almacenamiento original de forma simultánea al proceso de clonado u obtención de la imagen a bajo nivel.
- Efectuar el **cálculo del valor del hash** de la información contenida en el soporte destino donde se realizó el clonado forense utilizando los mismos algoritmos de resumen empleados con la evidencia original.
- **Comprobar que los valores de los hashes obtenidos de la evidencia original y de la copia forense coinciden**, lo cual garantiza la integridad de los datos almacenados en la copia forense.

DISPOSITIVOS ENCENDIDOS

Tiene lugar cuando para llevar a cabo la obtención de evidencias del dispositivo objeto de la investigación se utiliza un sistema operativo modo live ubicado en una unidad externa.

En este caso se puede acceder al almacenamiento persistente del dispositivo, pero no se puede acceder a la información volátil.

El orden de la adquisición de evidencias viene determinado por el orden de volatilidad, que es el inverso de persistencia:

- Registros y caché del procesador
- Memoria RAM
- Red (tablas de enrutamiento, cache ARP,...)
- Tabla de procesos den ejecuación
- Tráfico de red
- Archivos temporales del sistema de ficheros
- Sistema de ficheros del almacenamiento del dispositivo
- Configuración física de una red
- Cintas, disquetes, memoria USB, soportes ópticos.

Los analistas deberán trabajar en todo momento trabajar con —salvo casos muy excepcionales— con copias de las evidencias y jamás sobre las originales, puesto que serían alteradas y, por tanto, invalidadas. En cualquier caso, la copia debe ser exacta, bit a bit, es por ello que de la copia segura se debe obtener un valor hash de ambas evidencias para poder compararlas.

Es importante preservar la cadena de custodia de los datos a analizar; una cadena de custodia es un registro documental de quien estaba en posesión y control de una determinada evidencia en cada momento, **hasta que dicha evidencia es presentada ante un tribunal.**

ANÁLISIS DE LA EVIDENCIA DIGITAL

Una clasificación habitual de las diferentes formas en las que un analista forense puede analizar una evidencia digital es la siguiente:

- **Análisis temporal:** Determina la actividad a nivel de archivo ocurrida en el dispositivo de una determinada horquilla temporal, examinando diferentes archivos de eventos del sistema para relacionar las actividades del sistema de ficheros con otras actividades.
- **Análisis de información oculta:** Busca información oculta ya sea en el sistema de ficheros o en partes de disco normalmente inaccesibles al acceso estándar del sistema de ficheros.

- **Análisis de aplicaciones y archivos:** Busca el contenido de archivos, relaciona archivos con aplicaciones y actividad de aplicaciones con la creación y eliminación de archivos.
- **Análisis de propiedad y posesión:** Ayuda a identificar actividades relacionadas con la actividad de una determinada cuenta de usuario.

INTRODUCCIÓN AL ANÁLISIS DEL MALWARE

Se considera malware cualquier tipo de software dañino contra el normal funcionamiento de un dispositivo, aplicación o red.

El análisis de malware es el arte de diseccionar un software malicioso para comprender su funcionamiento, caracterizarlo y obtener indicadores de compromiso para su identificación en otros sistemas o determinar el método de eliminación de un dispositivo comprometido.

INTRODUCCIÓN AL ANÁLISIS DEL MALWARE

Existen diversas técnicas para llevar a cabo el análisis de una determinada muestra de malware. Estas técnicas, ordenadas de menor a mayor complejidad, se pueden resumir en:

- **Análisis estático del malware:** Se trata de una primera aproximación a un fichero sospechoso. Abarca las investigaciones realizadas sobre el objeto que contiene el código dañino sin ejecutarlo o desensamblarlo. Consiste en examinar las propiedades estáticas de dicho archivo como cadenas de texto, hash, posibles recursos embebidos ...
- **Análisis dinámico o comportamental del malware:** El analista debe utilizar un entorno de pruebas aislado que le permita infectar un sistema (generalmente máquina virtual) con el malware objeto de estudio para observar su comportamiento como si se tratase de un sistema en producción. Se podrá analizar cómo el software malicioso interactúa con el entorno o qué comunicaciones externas genera.

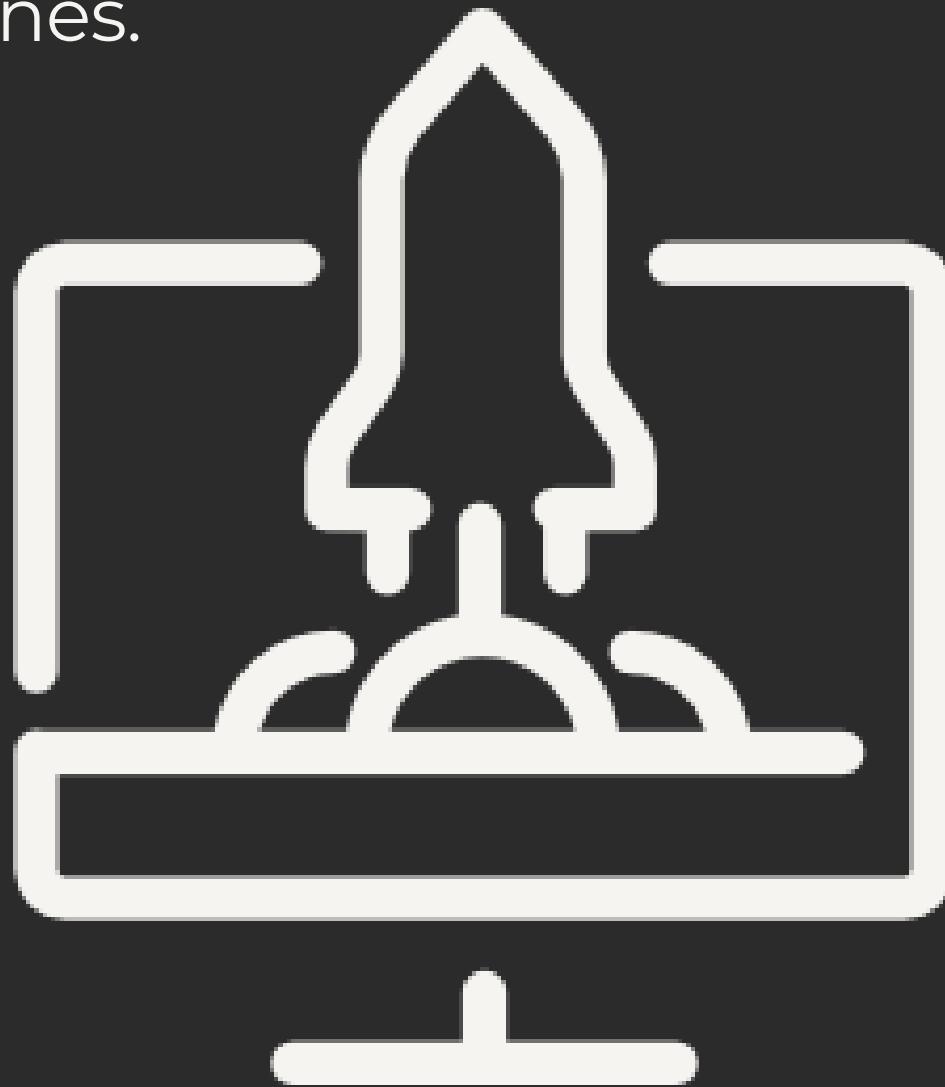
INTRODUCCIÓN AL ANÁLISIS DEL MALWARE

- **Reversing del código del malware:** Realizar la ingeniería del código de la muestra malware puede aportar un conocimiento adicional muy valioso a la información ya obtenida en el análisis dinámico.

Este tipo de análisis implica la utilización de un desensamblador y un depurador, además de una amplia variedad de plugins y herramientas específicas para automatizar algunos aspectos del análisis. El análisis forense de memoria RAM también suele resultar de ayuda en esta fase de análisis de malware.

5. RECURSOS MATERIALES

Los equipos de respuesta ante incidentes deben disponer de los medios adecuados para llevar a cabo un análisis forense. Es por ello que los equipos deben ser de altas prestaciones.



En otros muchos casos el propio equipo pues debido a la complejidad del incidente debe de desplazarse *in situ*. Para ello deben de disponer de medios como portátiles seguros, dispositivos de gran almacenamiento, S.O. externos, checklist impresas, cámaras de fotos...

6. ESTRATEGIA DE COMUNICACIÓN

Como ya se ha mencionado en el anterior tema, es muy importante abordar la gestión de cada incidente desde una perspectiva operativa y de respuesta técnica, pero también desde una perspectiva organizativa y estratégica.

En los incidentes más críticos es fundamental establecer la estrategia de comunicación en función del tiempo o prioridad y grupo al que va dirigida.

¿qué tipo de información se va a ofrecer? ¿Cuáles son los mensajes clave? ¿Qué formato se utilizara para la difusión de la comunicación? ¿Qué canales o medios se usarán?

Es importante que la organización sea proactiva y ágil a la hora de comunicar la situación, ya que hay que tener en cuenta posibles filtraciones de información (voluntarias o no) por parte de empleados, proveedores, clientes, ... Sobre lo que está sucediendo, corriendo el riesgo de que sea información incompleta, a destiempo, o errónea maximizando así el impacto del propio incidente de la organización.

Los mensajes a comunicar deberían tener las siguientes características:

- Ofrecer un discurso unificado y a ser posible por una única fuente oficial de información
- Transparencia, empatía y asunción de responsabilidades. Nunca se debe mentir y ofrecer la información de forma precisa. Para proteger la reputación de la organización debe evitarse cualquier tipo de incertidumbre, pero también tener en cuenta que la información que se ofrezca debe ser la correcta.
- Es importante transmitir confianza, actuar con serenidad, firmeza y profesionalidad
- Demostrar atención y respeto hacia todos los involucrados
- Puesta en valor de las acciones adoptadas. Cualquier situación de crisis representa una oportunidad para demostrar la capacidad de la organización para solventar una situación compleja, mostrando que la gestión del evento disruptivo está siendo la adecuada.

Kaspersky Lab investigates hacker attack on its own network

Kaspersky Lab has discovered an advanced attack on its own internal network and is sharing its investigation results. TL;DR – Customers are safe; neither products nor services have been compromised.

Lejos de centrarse en el compromiso en sí y en su parte negativa, se focalizaron en como habían sido capaces de detectar en detalle una amenaza tan avanzada como Duqu 2.0.

IMF

05 Respuesta ante incidentes



| Escuela de Ciberse...

SGG
Share

05.

Respuesta ante Incidentes

IMF x Deloitte.

Smart Education

Watch on

