

Implantación de Medidas de Ciberseguridad.

Aumento de Incidentes debido a la Transformación Digital



INCIBE. *Medidas de Ciberseguridad* (CC0)

La Transformación Digital que se está generalizando está produciendo una proliferación masiva de Incidentes de Ciberseguridad, pues **no sólo se están digitalizando los particulares y las empresas, sino también los malintencionados y los delincuentes.**

Para protegerse frente a esta plaga, se deberán efectuar labores **preventivas**, labores **operativas** en caso de la manifestación de un incidente, así como labores de **registro y documentación** de las lecciones aprendidas, de cara a futuros ataques similares o derivados del detectado.

En esta unidad se darán **indicaciones para implementar e implantar las Medidas de Ciberseguridad** que permitan prevenir y combatir adecuadamente los incidentes.

Estas medidas estarán compuestas por **procedimientos, capacidades, flujos de toma de decisión y mecanismos de restablecimiento** de los servicios afectados en cada caso.

1.- Procedimientos de Actuación para Dar Respuesta, Mitigar, Eliminar o Contener Incidentes.

A más desconcierto, más afectación



[INCIBE. Procedimientos de Respuesta a Incidentes \(CC0\)](#)

En los momentos iniciales de afectación por un incidente o de detección temprana del mismo, suele existir un cierto desconcierto en lo relativo a las medidas que se deben tomar, por parte de quién y en qué orden.

La afectación de los incidentes es directamente proporcional a dicho desconcierto, por lo que la mejor forma de preverlo y evitarlo es desarrollando Procedimientos de Actuación adecuados.

A pesar de que las medidas de mitigación dependen del tipo de ciberincidente y la afectación que haya tenido, algunas recomendaciones en esta fase son:

- ✓ **Determinar las causas y los síntomas del ciberincidente para determinar las medidas de mitigación más eficaces.** La identificación de la causa raíz suele constituir el 80% del trabajo posterior de análisis del incidente, puesto que en la mayoría de los casos una causa suele llevar aparejado un motivo para el ataque (malicia, burla, hurto, perjuicio para la actividad). Por lo que respecta a los síntomas, también es muy importante detallar todo aquello que se pueda detectar por observación directa o indirecta, puesto que estas trazas casi siempre estarán conectadas con el modus operandi, lo cual aportará también información muy valiosa para el análisis.
- ✓ **Identificar y eliminar todo el software utilizado por los atacantes.** Esta recomendación está ligada a la Filosofía Lean, esto es, pulcritud y orden en todos los escenarios, máxime cuando se trata de malware, cuya funcionalidad no se acaba nunca de conocer del todo y cuyos restos pueden propiciar la reproducción del problema antes o después, bien porque escondan aún más capacidades de ataque, bien porque dejen abiertos canales de entrada desde el exterior. En esta recomendación conviene ser radical, esto es, si se tiene la más mínima sospecha de que pueda quedar algún resto de malware en el sistema, o que pueda haber quedado abierta alguna vía de infección posterior, se deberá recuperar una imagen de respaldo anterior que esté limpia, o bien, se deberá plataformar totalmente la máquina, aunque ello conlleve la pérdida de los últimos movimientos o transacciones efectuadas.
- ✓ **Recuperación de la última copia de seguridad limpia.** Esta recomendación conecta con la anterior, no obstante, figura expresamente por separado porque muchas veces es muy difícil garantizar que una imagen de respaldo anterior no haya respaldado también el malware que ha ocasionado el ataque, o bien, otro malware que pueda estar dormido en su interior, por lo que se deberá disponer de herramientas de análisis de información de respaldo que sean capaces de detectar el máximo número de amenazas potenciales.
- ✓ **Identificar los servicios utilizados durante el ataque, ya que en ocasiones los atacantes utilizan servicios legítimos de los sistemas atacados.** En este sentido, las estadísticas son claras, puesto que el número de ataques que se efectúan utilizando brechas de los sistemas es sensiblemente menor que aquellos ataques que se efectúan a través de **servicios legítimos** no suficientemente protegidos, o bien, a los que se accede tras un robo de credenciales o usando Fuerza Bruta.
- ✓ **Por último, se realizará un informe del ciberincidente que deberá detallar su causa y su coste** (especialmente, en términos de compromiso de información o de impacto en los servicios prestados), así como las medidas que la organización deberá tomar para prevenir futuros ciberincidentes de naturaleza similar. La euforia derivada de vencer o superar un ataque junto con la premura de restaurar los servicios productivos, hace que muchas veces no se detalle adecuadamente la información necesaria para el futuro, o bien, no se estime el impacto en costes o prestación de servicios. La consecuencia inmediata suele ser lamentable, pues muchos ataques exitosos se deben a una repetición de un ataque anterior que no se ha preventido a pesar de tener la información suficiente. Además, muchos ataques son toscos y se efectúan mediante branches de algún malware anterior que haya tenido éxito en sus propósitos. Este problema se refuerza si no se calcula el coste del ataque, puesto que ante un coste desconocido no se suelen tomar medidas inmediatamente, lo cual provoca que el siguiente ataque similar se efectúe a corto plazo, mientras que si se observa un elevado coste sí que se tomarán medidas adecuadas de prevención cuanto antes.

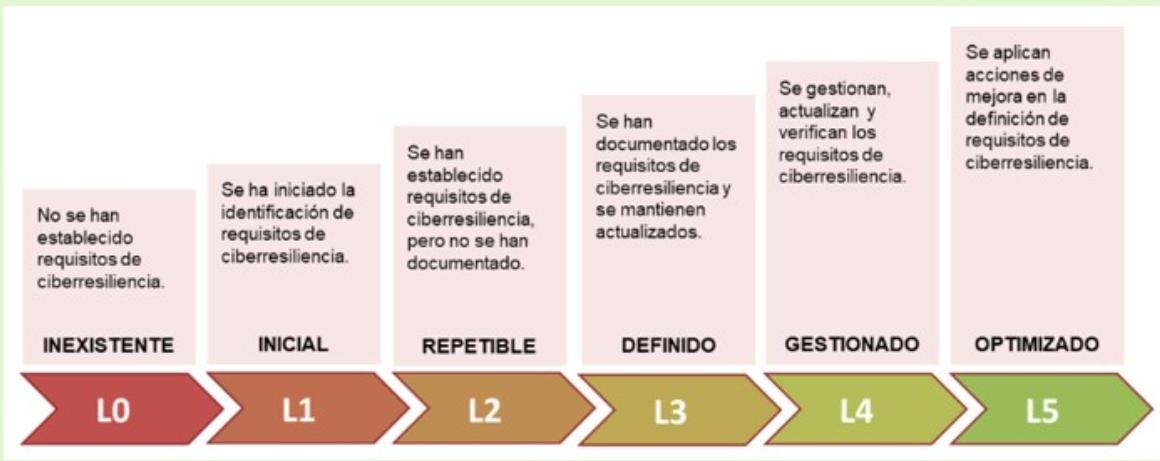
Autoevaluación

¿Qué consecuencias tiene no detallar adecuadamente la información de un incidente?

- La contaminación de los respaldos con el malware atacante
- La persistencia del malware dentro del software legítimo
- La repetición de un ataque anterior que no se ha prevenido, de forma directa o mediante un *branch* del malware

2.- Implantar Capacidades de Ciberresiliencia.

El Concepto de Ciberresiliencia



La ciberresiliencia, es la **capacidad para resistir, proteger y defender el uso del ciberespacio frente a los atacantes**.

Por lo general se suele establecer, desarrollar y medir con base en una escala de niveles.

En general, la mayoría de las **empresas** están **poco preparadas para resistir frente a los ciberataques**, debido principalmente a:

- ✓ Falta de medidas técnicas para mitigarlos.
- ✓ Poca preparación de los sistemas para detener este tipo de ataques.
- ✓ Falta de formación o de recursos para hacerles frente.
- ✓ Falta de pruebas para evaluar la capacidad real de la organización ante cualquier tipo de ataque externo.

Las organizaciones, deben estar preparadas para dar respuestas rápidas a este tipo de ataques, permitiendo que los servicios que prestan no se vean interrumpidos, y fortaleciendo sus capacidades de identificación, detección, prevención, contención, recuperación, cooperación y mejora continua contra las ciberamenazas.

Durante mucho tiempo, la política de combate de los incidentes de ciberseguridad ha sido completamente reactiva, esto es, sólo se ha combatido de forma puntual los ataques y sólo se han tomado medidas *ad hoc* para cada variedad de malware.

Afortunadamente, **en la actualidad quedan pocas dudas de que haya que tomar medidas preventivas de ciberseguridad** y de que la política de combate deba ser proactiva, como reza la antigua sentencia del escritor romano Flavio Vegecio: "si vis pacem, para bellum" (si quieres la paz, prepárate para la guerra). En línea con esto, en la mayoría de las empresas existen directivos y políticas específicas para la prevención de incidentes, junto con su correspondiente presupuesto en el plan estratégico.

Autoevaluación

¿Cuál es la política más recomendable para el combate efectivo contra los incidentes de ciberseguridad?

- Reaccionar de forma rápida y puntual a cada ataque
- Tomar medidas preventivas de ciberseguridad
- La combinación de las dos anteriores

3.- Establecer Flujos de Toma de Decisiones y Escalado Interno y/o Externo Adecuados.

La Estrategia de Contención de Incidentes



[INCIBE. Toma de Decisión y Escalado \(CC0\)](#)

El **conjunto de flujos de decisión y escalado** constituyen la denominada **Estrategia de Contención de Incidentes** de Ciberseguridad.

En este marco estratégico se debe contemplar toda la tipología de incidentes, relacionándola adecuadamente con el **conjunto de criterios a tener en cuenta para la toma de decisión** en cada caso.

Los **criterios** generales para **guiar la toma de decisión** podrán ser los siguientes:

- ✓ Cuestiones forenses.
- ✓ Daño potencial a la organización.
- ✓ Hurto de activos y detalle de su valor.
- ✓ Premisas para preservar las evidencias, de cara a una investigación posterior.
- ✓ Disponibilidad del servicio afectado y tiempo necesario para restablecerlo.
- ✓ Tiempo y recursos requeridos para la implementación del marco estratégico.
- ✓ Efectividad de la estrategia para la contención total o parcial del incidente.
- ✓ Vigencia de la solución aplicada.
- ✓ Etc.

Para el diseño de estos flujos es importante tomar como referencia toda la información que sea posible, sin centrarse sólamente en los incidentes acaecidos en la empresa o en empresas próximas o relacionadas. En ese sentido, es fundamental la adhesión a las comunidades del ámbito de la ciberseguridad, sobre todo en lo relativo a la prevención de incidentes.

Lo que suele dar mejor resultado en esta cuestión es abrir un capítulo de Hacking Ético y conectarse con las comunidades relacionadas con el mismo, pues suelen ser muy activas y procuran tener actualizados sus procedimientos y su software en línea con todas las amenazas conocidas a nivel global. Si no es posible contemplar este tema de forma orgánica, creando un área al efecto en la empresa, lo mejor es hacerlo de forma inorgánica, esto es, contratando los servicios de una empresa de Pentesting y Hacking Ético.

La iniciativa más popular en este sentido a nivel global es la de **Offensive Security** y su distribución **Kali Linux**, que contiene cientos de paquetes software de código abierto, especializados en ataques muy variados y actualizados a diario.

Así pues, conjugando todas las amenazas conocidas y sus medidas de contención, con las particularidades de cada empresa y su organización, se podrá diseñar flujos coherentes de toma de decisión en lo tocante a la contención de incidentes de ciberseguridad.

Autoevaluación

¿Cuál es la mejor estrategia para establecer Flujos de Toma de Decisión y Escalado?

- Abrir un capítulo de Hacking Ético y conectarse con las comunidades relacionadas con el mismo
- Contratar los servicios de una empresa de Pentesting y Hacking Ético
- Cualquiera de las anteriores, en función de los recursos de la empresa

4.- Tareas para Restablecer los Servicios Afectados por Incidentes.

La Recuperación frente a un Incidente



[INCIBE](#). Contingencia y Continuidad del Negocio (CCO)

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 cuanto antes. Es importante no precipitarse en la puesta en producción de sistemas que se hayan visto implicados en ciberincidentes.

La recuperación de la actividad normal no siempre es posible de forma completa e inmediata. Por ello, es conveniente definir y detallar los niveles de operación de la empresa en su escenario de trabajo habitual, de forma que se sepa cómo actuar para llegar a cada uno de dichos niveles, y qué características del servicio se verán deterioradas total o parcialmente por no estar en el nivel más alto de operación. Esta actividad de definición y caracterización de los niveles de operación también deberá estar recogida en la estrategia de ciberseguridad de la empresa, pues la implementación de dichos niveles puede que no sea estrictamente organizativa y precise desarrollos o configuraciones ad hoc en los sistemas involucrados en la prestación de los servicios.

Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un período de tiempo con medidas adicionales de monitorización. Por lo general, la prisa existente tras un incidente para recuperar el nivel de operación requerido provoca que, en ocasiones, no se tomen todas las precauciones necesarias ni se mantengan las cuarentenas requeridas, a lo cual hay que sumar la dotación de planes de respuesta de emergencia a aplicar en caso de reproducción a corto plazo de un incidente ya identificado y contenido.

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**, que se basan en la documentación del incidente, como se verá en el apartado siguiente.

Autoevaluación

¿Cuál es el proceso que menos se prioriza durante el restablecimiento de servicios afectados por un incidente?

- La recuperación de la actividad normal
- La búsqueda de signos de actividad sospechosa tras la recuperación de la actividad normal
- Las lecciones aprendidas

5.- Documentación de los Incidentes.

La Necesaria Reflexión tras un Incidente



[INCIBE. Documentación de Incidentes \(CC0\)](#)

Tras un incidente, 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 finalidad de este proceso es aprender de lo ocurrido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda repetir, además de mejorar los procedimientos.

La **última tarea del proceso** de gestión de incidentes consistirá en **documentar adecuadamente el ciberincidente** detallando lo siguiente:

- ✓ Su causa.
- ✓ Su coste, por compromiso de información o por impacto en los servicios que se hayan visto afectados.
- ✓ Las medidas a tomar para prevenir futuros ciberincidentes similares.

La creación de políticas de Lecciones Aprendidas no es una opción en el campo de la ciberseguridad. Esta recomendación *Lean* ha probado ya su eficiencia sobradamente cuando se trata de producción, fabricación o prestación de servicio, todos ellos ámbitos acotados en cierta medida. Así pues, dado que en el caso de la ciberseguridad el ámbito no es acotado de ninguna manera, toda la información que se recoja será de utilidad para documentar adecuadamente el problema y evitar su reproducción. Se debe trabajar intensamente en esta cuestión para evitar tropezar dos veces en la misma piedra, pues en algunas ocasiones el coste de estos tropiezos inducidos puede ser muy alto y puede tener incluso responsabilidades disciplinarias por dejación de funciones, omisión de deberes o inacción en general.

Autoevaluación

¿Qué se debe detallar durante el proceso de documentación de un incidente?

- Sólo los datos del malware atacante
- Sólo las consecuencias del ataque
- Su causa, su coste y las medidas a tomar para el futuro

6.- Seguimiento de Incidentes para Evitar una Situación Similar.

La Cuarentena tras un Incidente



[INCIBE. Seguimiento de Incidentes \(CCO\)](#)

Conviene prestar especial atención a los sistemas atacados durante la nueva puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un periodo de tiempo con medidas adicionales de monitorización, normalmente denominado cuarentena.

Para efectuar este seguimiento, la empresa se deberá servir de todos los medios a su alcance, tanto humanos (analistas de ciberseguridad) como técnicos (detección de intrusiones), lo cual equivale en la mayoría de los casos a disponer de un Centro de Operaciones de Seguridad.

En las empresas en que se disponga de un SOC, toda la actividad de ciberseguridad de la empresa estará centralizada, tanto en lo relativo a la detección y combate, como en lo relativo al almacenamiento de datos y a su análisis posterior, máxime si éstos se efectúan durante el período de cuarentena de un sistema tras un ataque ya expurgado.

Como se comentó al principio del módulo, en las dos últimas unidades del mismo se implementará un **SOC** real fundamental, a partir del cual se podrá trabajar para construir el conocimiento de ciberseguridad de cualquier empresa, escalando el sistema tanto en recursos físicos como en recursos lógicos a medida que se vayan detectando y combatiendo incidentes.

Autoevaluación

¿Cuál es la mejor forma de supervisar un sistema recuperado, durante su período de cuarentena?

- Disponer de un Sistema de Detección de Intrusiones
- Disponer de un SOC
- Disponer de Mecanismos de Respuesta Rápida

7.- Bibliografía

[Bibliografía](#) (pdf - 53803 B)

Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.



MINISTERIO
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL



Antes de cualquier uso leer detenidamente el siguiente [Aviso legal](#)

Historial de actualizaciones

Versión: 01.00.01

Fecha de actualización: 08/11/23

Actualización de materiales y correcciones menores.

Versión: 01.00.00

Fecha de actualización: 04/07/23

Versión inicial de los materiales.