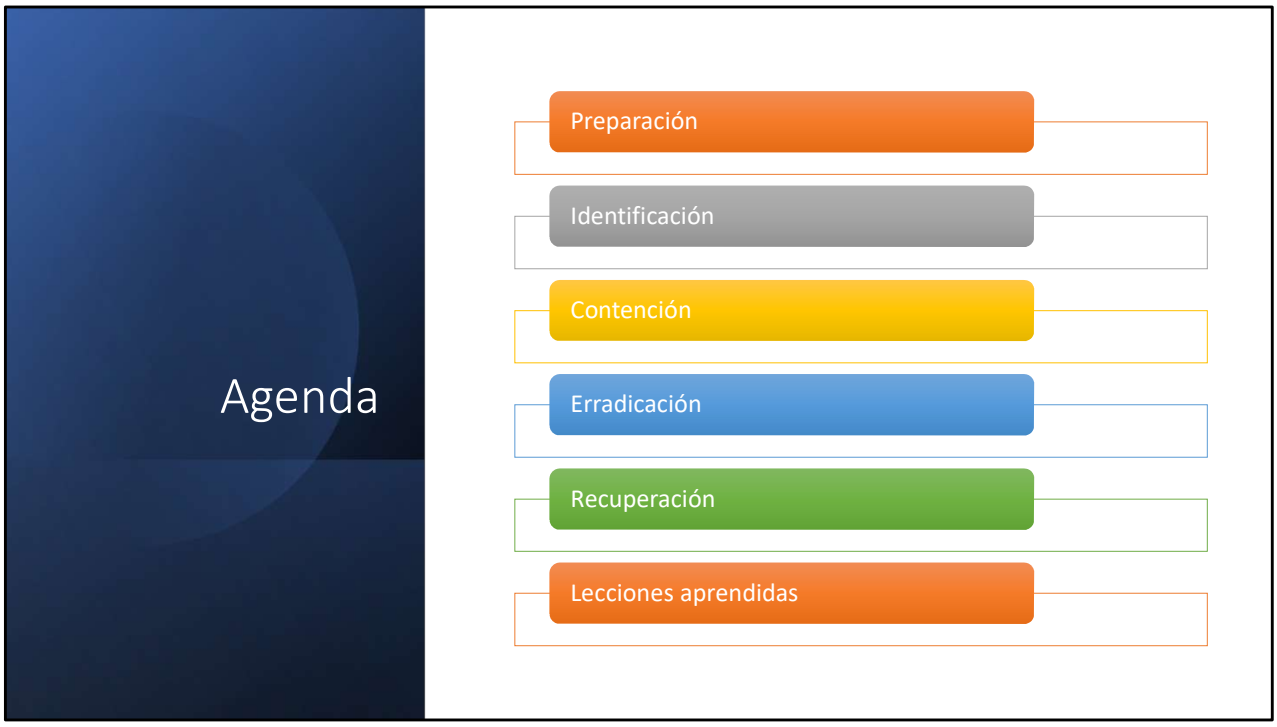
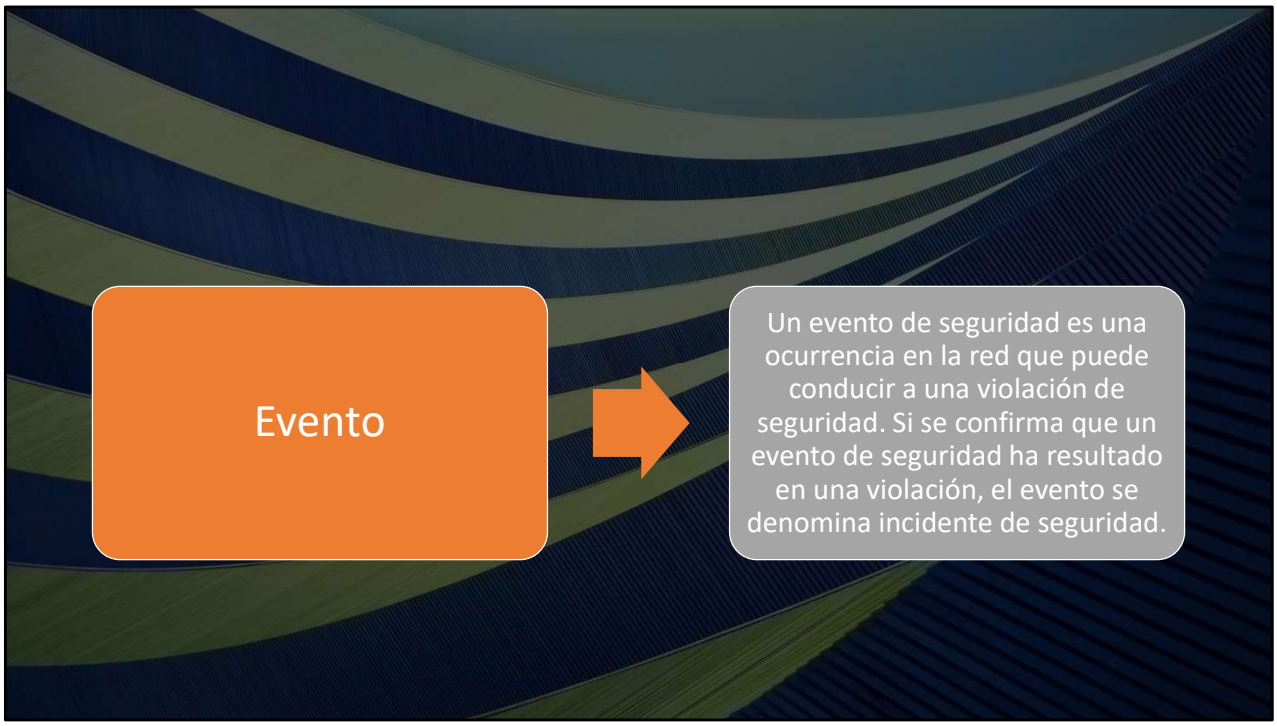
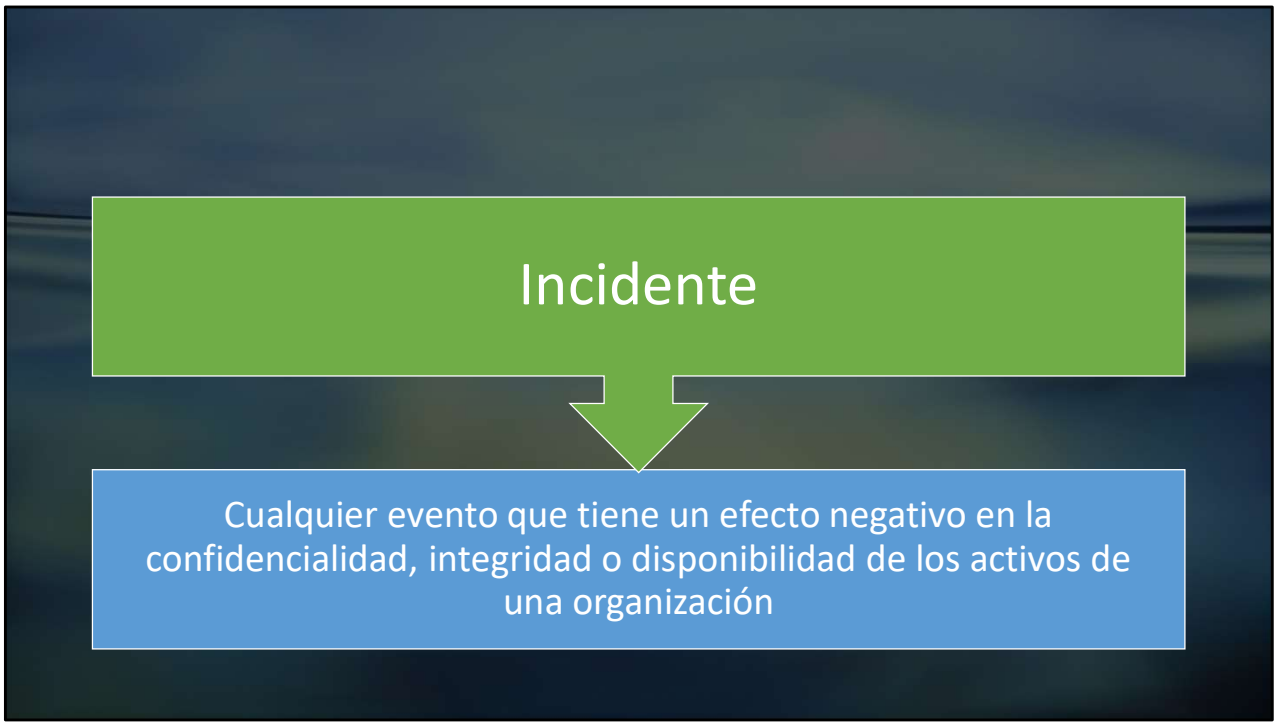
La respuesta a incidentes es un proceso que permite a las organizaciones identificar, priorizar, contener y erradicar los ciberataques. El objetivo de la respuesta a incidentes es garantizar que las organizaciones estén al tanto de los incidentes de seguridad significativos y actúen rápidamente para detener al atacante, minimizar el daño causado y evitar ataques posteriores o incidentes similares en el futuro.


Agenda
Preparación
Identificación
Contención
Erradicación
Recuperación
Lecciones aprendidas

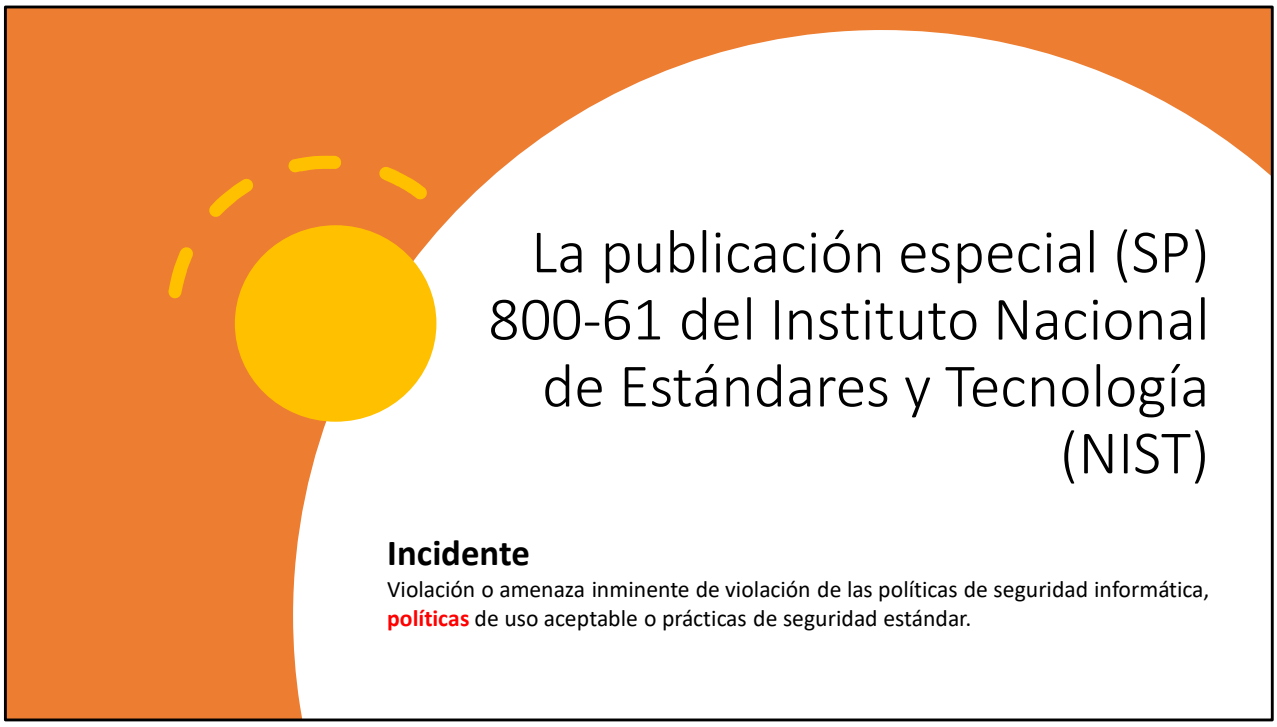

Evento
Un evento de seguridad es una ocurrencia en la red que puede conducir a una violación de seguridad. Si se confirma que un evento de seguridad ha resultado en una violación, el evento se denomina incidente de seguridad.



Antes de profundizar en la gestión de incidentes, es importante comprender la definición de un incidente. Aunque eso puede parecer simple, encontrará que diferentes fuentes tienen definiciones ligeramente diferentes.

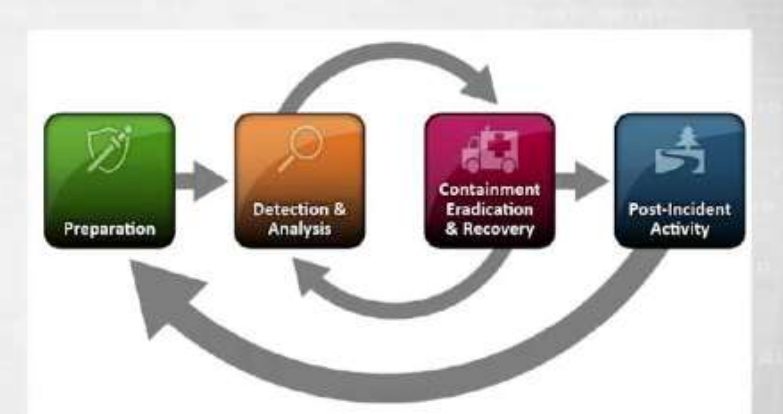
En general, un incidente es cualquier evento que tiene un efecto negativo en la confidencialidad, integridad o disponibilidad de los activos de una organización. Tenga en cuenta que esta definición abarca eventos tan diversos como ataques directos, sucesos naturales como un huracán o un terremoto, e incluso accidentes, como alguien que corta accidentalmente cables para una red en vivo.

En contraste, un incidente de seguridad informática (a veces llamado solo incidente de seguridad) comúnmente se refiere a un incidente que es el resultado de un ataque o el resultado de acciones maliciosas o intencionales por parte de los usuarios.

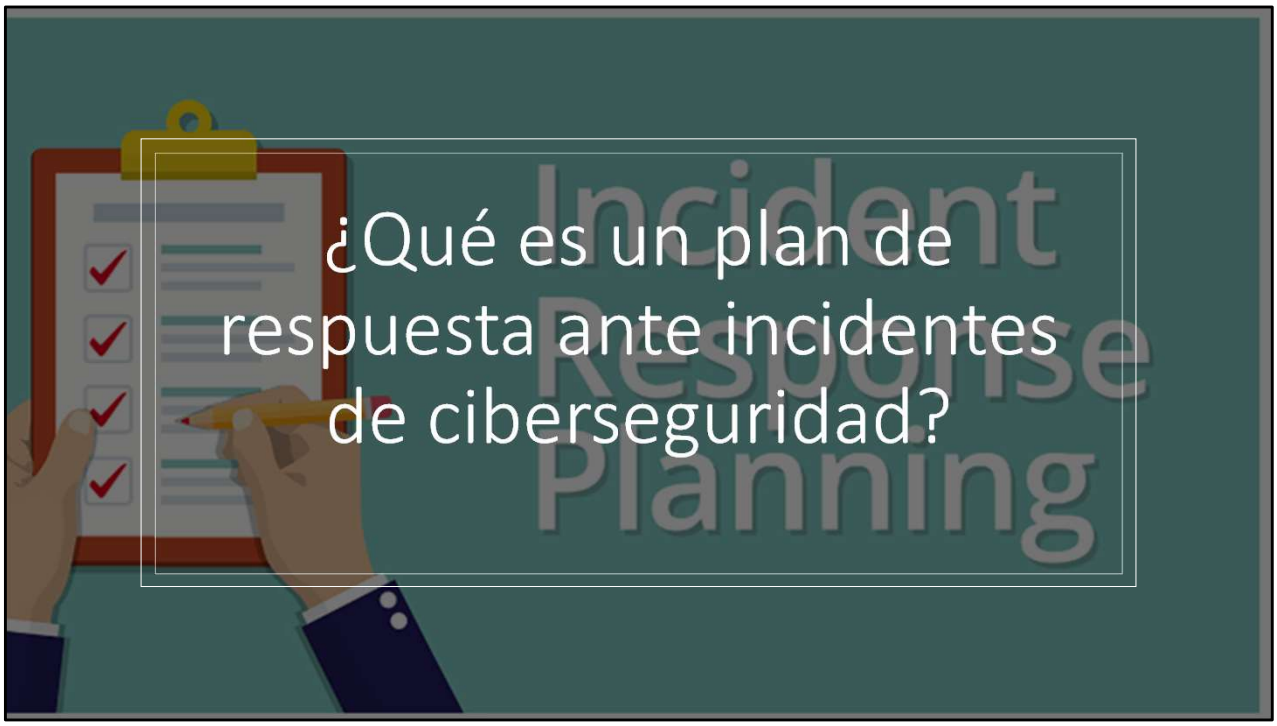


La publicación especial (SP) 800-61 del Instituto Nacional de Estándares y Tecnología (NIST), Guía de manejo de incidentes de seguridad informática, define un incidente de seguridad informática como "una violación o amenaza inminente de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas de seguridad estándar".

Estos son los pasos según NIST



Estos son los pasos según NIST, pero en esta presentación usare como referencias los 6 pasos que SANS sugiere.



La respuesta a incidentes es un proceso que permite a las organizaciones identificar, priorizar, contener y erradicar los ciberataques. El objetivo de la respuesta a incidentes es garantizar que las organizaciones estén al tanto de los incidentes de seguridad significativos y actúen rápidamente para detener al atacante, minimizar el daño causado y evitar ataques posteriores o incidentes similares en el futuro

Paso 1: Preparación

El objetivo de la etapa de preparación es garantizar que la organización pueda responder de manera integral a un incidente en cualquier momento.

Lista de Prevención

- Barrera humana
- Gestión de identidades sólidas
- Gestión de Vulnerabilidades
- Reducir errores de configuración
- Copias de seguridad seguras y confiables
- Higiene cibernética
- Logging Centralizado y suficiente
- Automatización (SOAR, XDR)

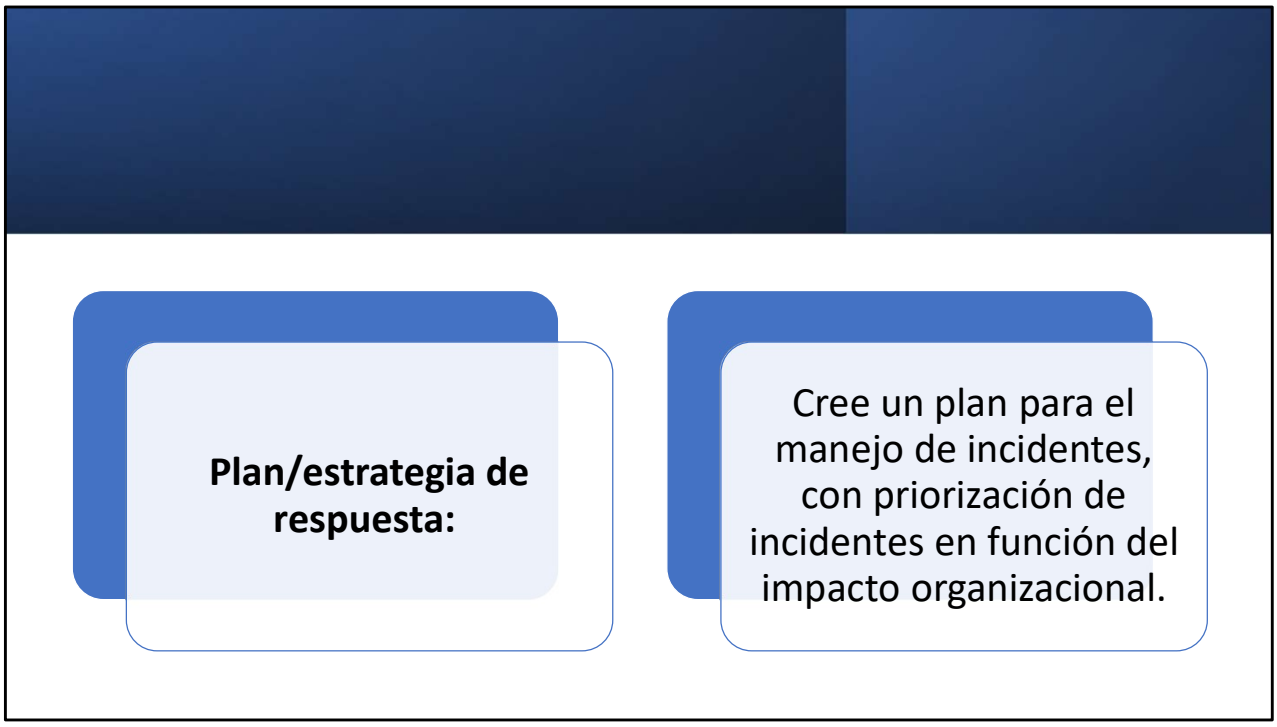
Política : defina principios, reglas y prácticas para guiar los procesos de seguridad. Asegúrese de que la política sea muy visible tanto para los empleados como para los usuarios, por ejemplo, mostrando un banner de inicio de sesión que indique que se supervisarán todas las actividades y que indique claramente las actividades no autorizadas y las sanciones asociadas.

Plan/estrategia de respuesta: cree un plan para el manejo de incidentes, con priorización de incidentes en función del impacto organizacional. Por ejemplo, el impacto organizacional es mayor cuanto más empleados se ven afectados dentro de la organización, más probable es que un evento afecte los ingresos o más datos confidenciales están involucrados, como salarios, datos financieros o de clientes privados.

Política

defina principios, reglas y prácticas para guiar los procesos de seguridad.

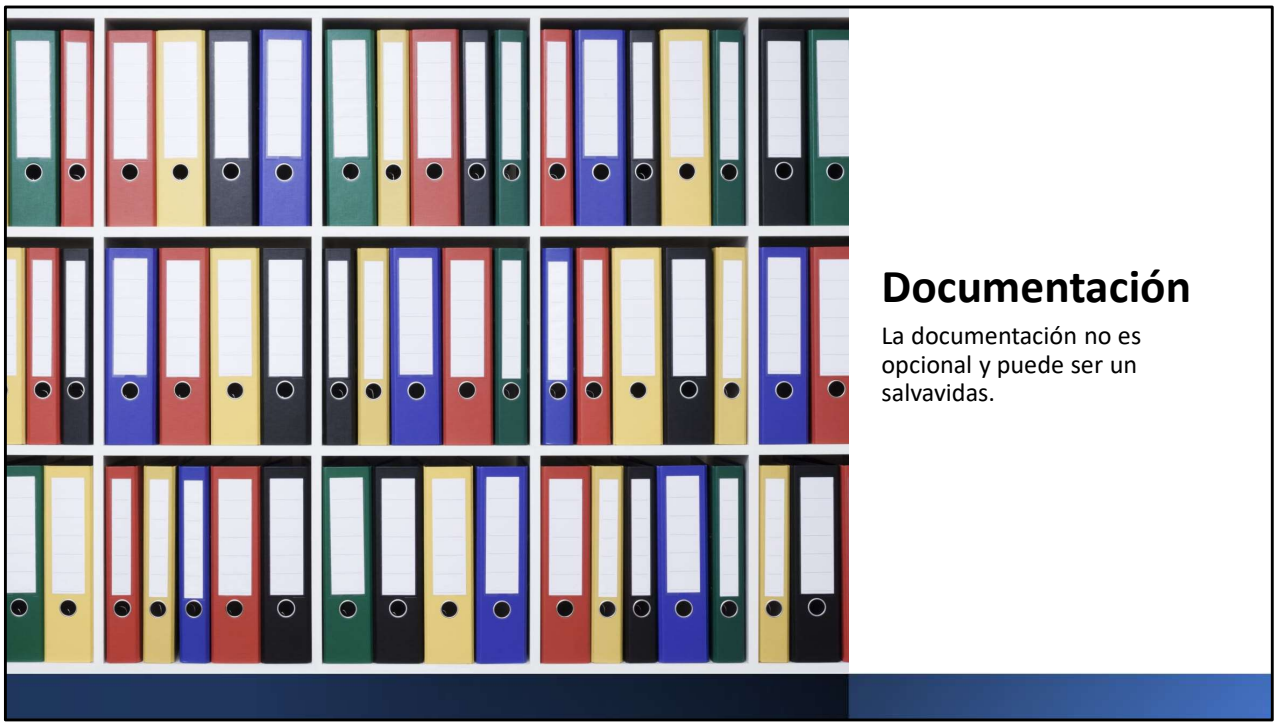
Asegúrese de que la política sea muy visible tanto para los empleados como para los usuarios, por ejemplo, mostrando un banner de inicio de sesión que indique que se supervisarán todas las actividades y que indique claramente las actividades no autorizadas y las sanciones asociadas.



Por ejemplo, el impacto organizacional es mayor cuanto más empleados se ven afectados dentro de la organización. El impacto también depende de si datos confidenciales han sido afectados.

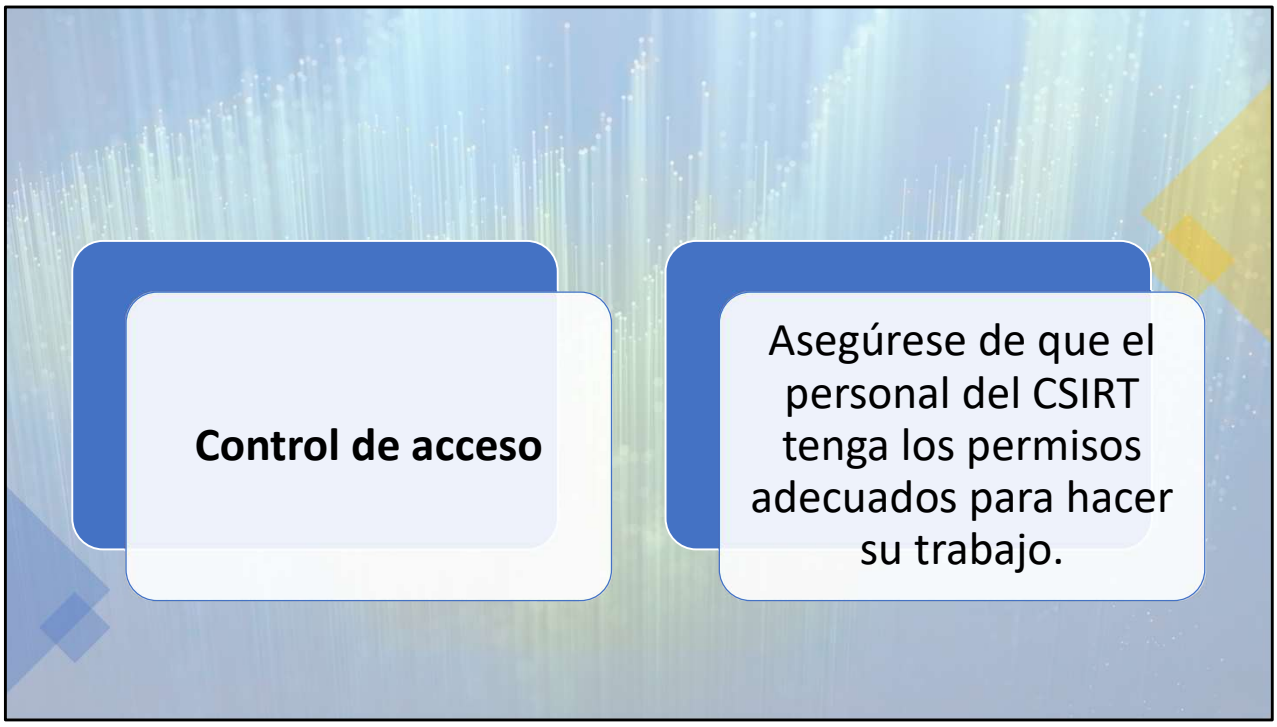
Comunicación

Cree un plan de comunicación que establezca qué miembros del CSIRT deben ser contactados durante un incidente, por qué razones y cuándo pueden ser contactados.

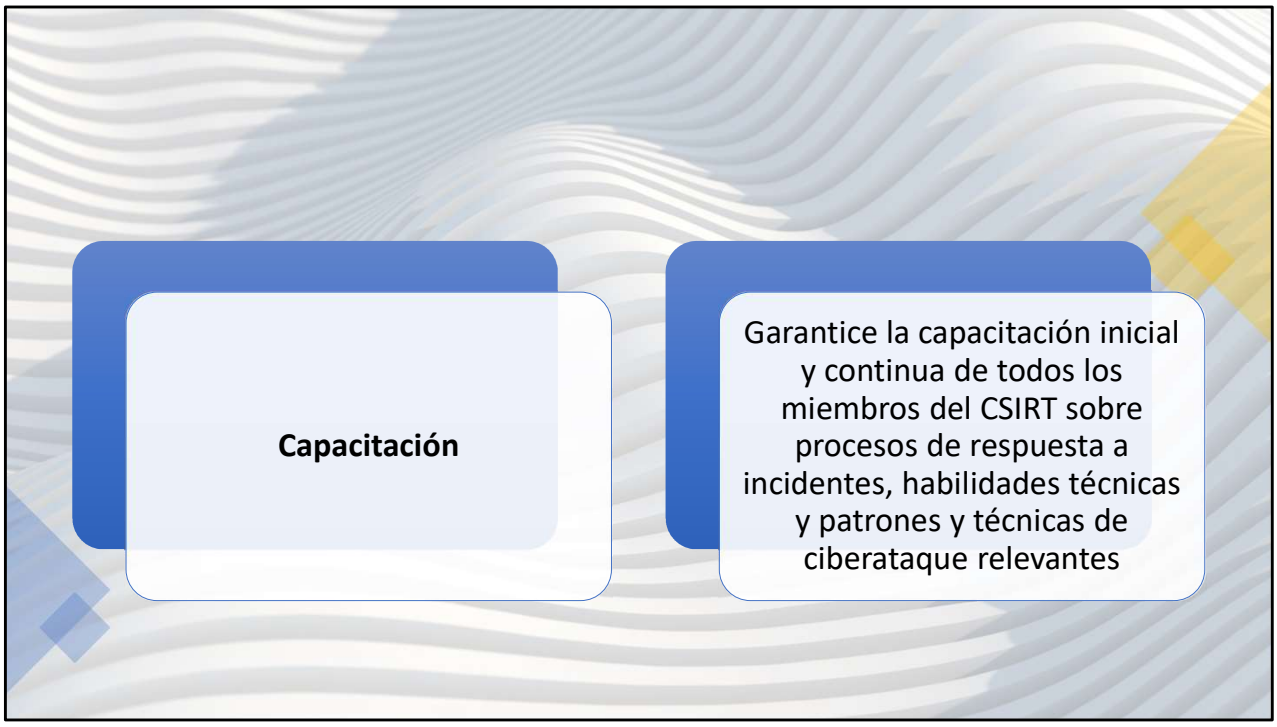


Si el incidente se considera un acto delictivo, su documentación se utilizará para presentar cargos contra los sospechosos. Cualquier información que recopile sobre el incidente también puede usarse para lecciones aprendidas y para mejorar su proceso de respuesta a incidentes. La documentación debe responder a las preguntas: ¿Quién, qué, cuándo, dónde, por qué y cómo?.

Incluya personas con experiencia en seguridad, pero también en operaciones de TI, legales, recursos humanos y relaciones públicas, todos los cuales pueden ser fundamentales para enfrentar y mitigar un ataque.



Es una buena idea que, como parte del plan de respuesta a incidentes, los administradores de red agreguen permisos a las cuentas de los miembros del CSIRT y luego los eliminen cuando finalice el incidente.



Realice simulacros a intervalos regulares para asegurarse de que todos en el CSIRT sepan lo que deben hacer y puedan desempeñar sus funciones durante un incidente real.

Herramientas

Evalúe, seleccione e implemente software y hardware que puedan ayudar a responder a un incidente de manera más efectiva.

Todas las herramientas deben empaquetarse en una “bolsa auxiliar” (jump bag) a la que los miembros del CSIRT puedan acceder rápidamente cuando ocurra un incidente.

La realidad es que muchas organizaciones pequeñas y medianas no tienen los recursos necesarios para tener un equipo de seguridad capaz de enfrentarse a un gran ataque. Tenga listo un contrato con una compañía que brinde servicios de respuesta a incidentes. No espere que sea demasiado tarde.


Paso 2: Identificación

El procedimiento de identificación de respuesta a incidentes de incluye los siguientes elementos:

- Configuración de monitoreo
- Análisis de eventos
- Identificar un incidente
- Notificar a los miembros del CSIRT
- Documentación
- Capacidades de prevención y detección de amenazas

Este paso implica detectar desviaciones de las operaciones normales en la organización, comprender si una desviación representa un incidente de seguridad y determinar qué tan importante es el incidente.

Detección


Los sistemas de detección y prevención de intrusiones


El software antimalware


Herramientas automatizadas (EDR y XDR)


Los usuarios finales

Los entornos de TI incluyen múltiples métodos para detectar posibles incidentes.

- Los sistemas de detección y prevención de intrusiones envían alertas a los administradores cuando detectan un posible incidente.
- El software antimalware a menudo mostrará una ventana emergente para indicar cuándo detecta malware.
- Muchas herramientas automatizadas escanean regularmente los registros de auditoría en busca de eventos predefinidos, como el uso de privilegios especiales. Cuando detectan eventos específicos, normalmente envían una alerta a los administradores.
- Los usuarios finales a veces detectan actividad irregular y se ponen en contacto con técnicos o administradores para obtener ayuda. Cuando los usuarios informan de eventos, como la imposibilidad de acceder a un recurso de red o actualizar un sistema, alerta al personal de TI sobre un posible incidente.

Solo porque un profesional de TI reciba una alerta de una herramienta automatizada o una queja del usuario, esto no siempre significa que haya ocurrido un incidente

Tenga en cuenta que solo porque un profesional de TI reciba una alerta de una herramienta automatizada o una queja del usuario, esto no siempre significa que haya ocurrido un incidente. Los sistemas de detección y prevención de intrusiones a menudo dan falsas alarmas, y los usuarios finales son propensos a errores simples del usuario. El personal de TI investiga estos eventos para determinar si son incidentes.

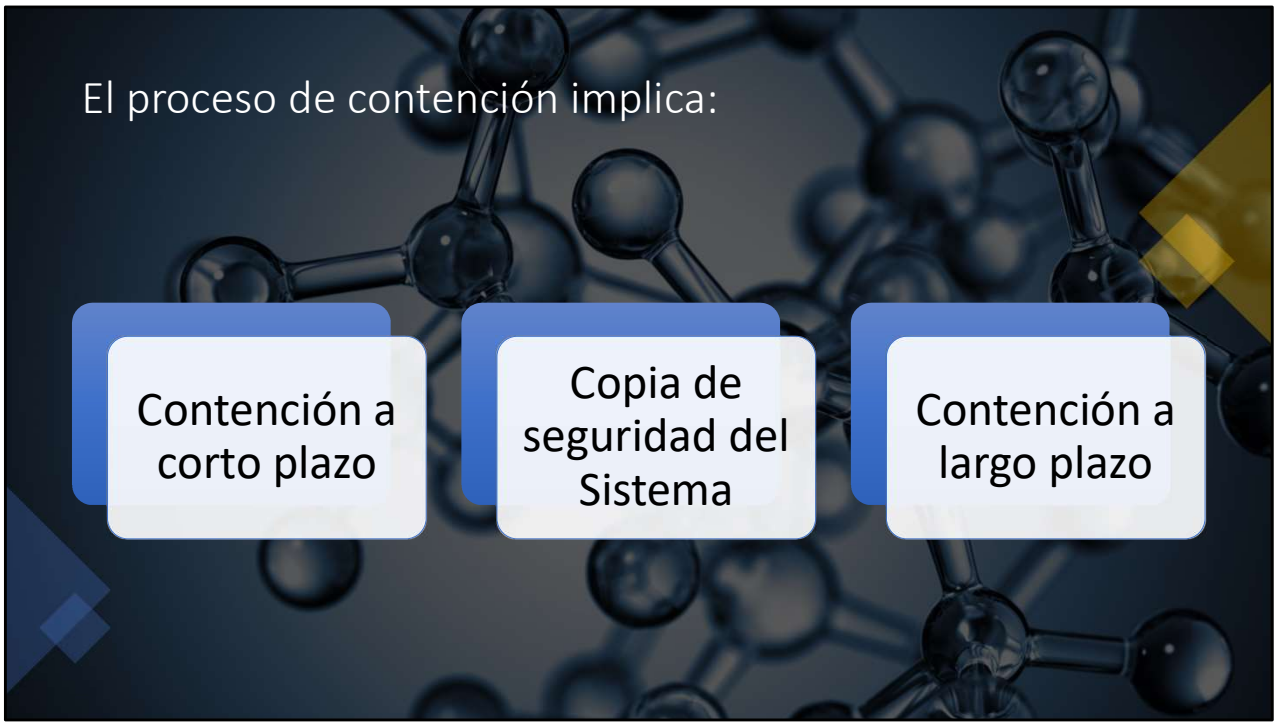
Muchos profesionales de TI se clasifican como primeros respondedores de incidentes. Son los primeros en la escena y saben cómo diferenciar los problemas típicos de TI de los incidentes de seguridad.

Son similares a los socorristas médicos, que tienen habilidades y habilidades sobresalientes para proporcionar asistencia médica en las escenas del accidente y ayudar a llevar a los pacientes a las instalaciones médicas cuando sea necesario.

Los socorristas médicos tienen capacitación específica para ayudarlos a determinar la diferencia entre lesiones menores y mayores. Además, saben qué hacer cuando se encuentran con una lesión importante. Del mismo modo, los profesionales de TI necesitan capacitación específica para determinar la diferencia entre un problema típico que necesita solución de problemas y un incidente de seguridad que necesitan escalar.

Paso 3: Contención

El objetivo de la contención es limitar los daños del incidente de seguridad actual y evitar daños mayores. Son necesarios varios pasos para mitigar completamente el incidente, al mismo tiempo que se previene la destrucción de pruebas que pueden ser necesarias para el enjuiciamiento, si el caso llega a las cortes.



El proceso de contención implica:

•**Contención a corto plazo:** limitar el daño antes de que el incidente empeore, generalmente aislando segmentos de red, eliminando el servidor de producción hackeado.

•**Copia de seguridad del sistema** : tomar una imagen forense de los sistemas afectados con herramientas como Forensic Tool Kit (FTK) o EnCase, y solo luego borrar y volver a crear una imagen de los sistemas. Esto preservará la evidencia del ataque que se puede usar en la corte, y también para una mayor investigación del incidente y las lecciones aprendidas.

•**Contención a largo plazo:** aplicar arreglos temporales para hacer posible que los sistemas de producción vuelvan a funcionar. El enfoque principal es eliminar cuentas o puertas traseras dejadas por los atacantes en los sistemas y abordar la causa raíz, por ejemplo, arreglar un mecanismo de autenticación roto o parchear una vulnerabilidad que condujo al ataque.

El tiempo: Aliado o Enemigo

Cuanto más rápido una organización pueda responder a un incidente, más posibilidades tendrá de limitar el daño. Si un incidente continúa durante horas o días, es probable que el daño sea mayor. Por ejemplo, un atacante puede estar intentando acceder a una base de datos de clientes. Una respuesta rápida puede evitar que el atacante obtenga datos significativos. Sin embargo, si se le da acceso continuo sin obstáculos a la base de datos durante varias horas o días, el atacante puede obtener una copia de toda la base de datos.

Paso 4: Erradicación

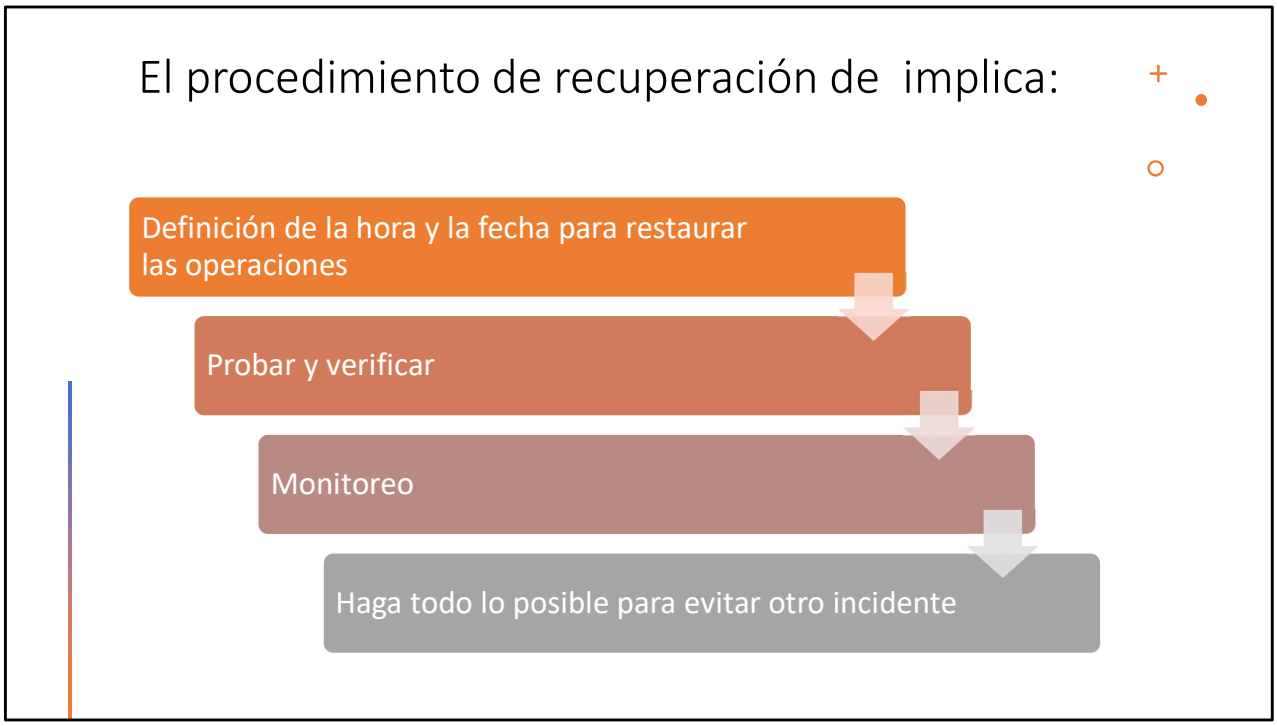
La erradicación tiene como objetivo eliminar el malware u otros artefactos introducidos por los ataques y restaurar completamente todos los sistemas afectados.

El proceso de erradicación de implica:

•**Recreación** de imágenes: limpieza completa y nueva imagen de los discos duros del sistema afectado para garantizar que se elimine cualquier contenido malicioso.
•**Prevención de la causa raíz** : comprensión de la causa del incidente, prevención de compromisos futuros, por ejemplo, parcheando una vulnerabilidad explotada por el atacante.
•**Aplicar las mejores prácticas básicas de seguridad** , por ejemplo, actualizar versiones de software antiguas y deshabilitar servicios no utilizados.
•**Escanee en busca de malware** : use software antimalware o Antivirus de próxima generación (NGAV), si está disponible, para escanear los sistemas afectados y asegurarse de que se elimine todo el contenido malicioso.

Paso 5: Recuperación

El objetivo de la recuperación es hacer que todos los sistemas vuelvan a funcionar por completo, después de verificar que estén limpios y que se elimine la amenaza.

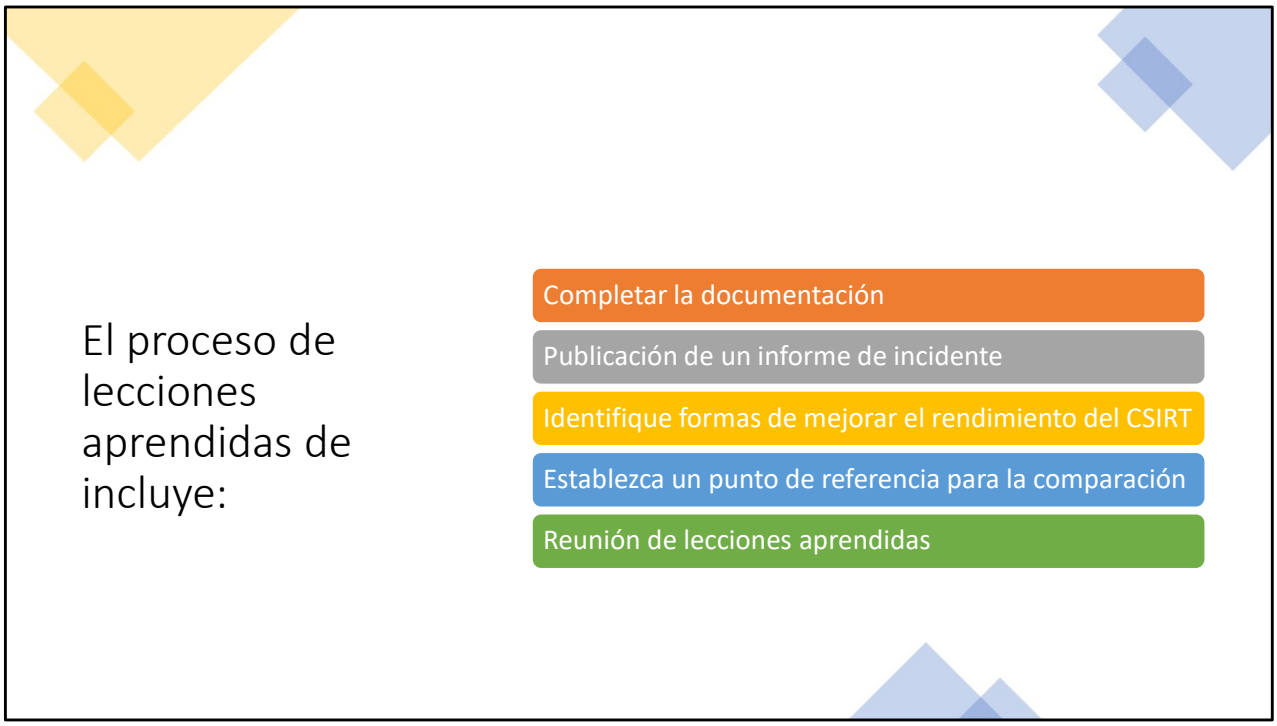


El procedimiento de recuperación de implica:

•**Definición de la hora y la fecha para restaurar las operaciones** : los propietarios del sistema deben tomar la decisión final sobre cuándo restaurar los servicios, según la información del CSIRT.
•**Probar y verificar** : garantizar que los sistemas estén limpios y completamente funcionales a medida que se ponen en marcha.
•**Monitoreo** : monitoreo continuo durante algún tiempo después del incidente para observar las operaciones y verificar comportamientos anormales.
•**Haga todo lo posible para evitar otro incidente** , teniendo en cuenta lo que se puede hacer en los sistemas restaurados para protegerlos de la recurrencia del mismo incidente.

Paso 6: Lecciones Aprendidas

A más tardar dos semanas después del final del incidente, el CSIRT debe compilar toda la información relevante sobre el incidente y extraer lecciones que puedan ayudar con la futura actividad de respuesta a incidentes.



•**Completar la documentación** : nunca es posible documentar todos los aspectos de un incidente mientras está ocurriendo, y lograr una documentación completa es muy importante para identificar lecciones para la próxima vez.
•**Publicación de un informe de incidente:** el informe debe proporcionar una revisión detallada de todo el incidente y responder a las preguntas quién, qué, dónde, por qué y cómo.
•**Identifique formas de mejorar el rendimiento del CSIRT** : extraiga los elementos del informe de incidentes que no se manejaron correctamente y se pueden mejorar para la próxima vez.
•**Establezca un punto de referencia para la comparación** : obtenga métricas del informe de incidentes que pueda usar para guiarse en futuros incidentes.
•**Reunión de lecciones aprendidas** : lleve a cabo una reunión con el equipo del CSIRT y otras partes interesadas para analizar el incidente y cimentar las lecciones aprendidas que se pueden implementar de inmediato.

El equipo de respuesta a incidentes estará involucrado en esta etapa, pero también participarán otros empleados que estén bien informados sobre el incidente.

Durante la etapa de lecciones aprendidas, el personal examina el incidente y la respuesta para ver si hay alguna lección que aprender. El equipo de respuesta a incidentes estará involucrado en esta etapa, pero también participarán otros empleados que estén bien informados sobre el incidente.

Al examinar la respuesta al incidente, el personal busca cualquier área en la que pueda mejorar su respuesta. Por ejemplo, si el equipo de respuesta tardó mucho tiempo en contener el incidente, el examen intenta determinar por qué. Puede ser que el personal no tenga la capacitación adecuada y no tenga el conocimiento y la experiencia para responder de manera efectiva. Es posible que no hayan reconocido el incidente cuando recibieron la primera notificación, lo que permite que un ataque continúe más tiempo del necesario. Es posible que los socorristas no hayan reconocido la necesidad de proteger la evidencia y la hayan corrompido inadvertidamente durante la respuesta.

Recuerde, la salida de esta etapa se puede retroalimentar a la etapa de detección de la gestión de incidentes. Por ejemplo, los administradores pueden darse cuenta de que los ataques pasan desapercibidos y aumentar sus capacidades de detección y recomendar cambios en sus sistemas de detección de intrusiones.

La presentación de informes se refiere a la notificación de un incidente dentro de la organización y a organizaciones e individuos fuera de la organización. Aunque no hay necesidad de informar una infección menor de malware al CEO de una empresa, la administración de nivel superior necesita saber sobre violaciones de seguridad graves.

Como ejemplo, la firma de cobro de deudas médicas R1 RCM fue golpeada por un ataque de Ransomware en agosto de 2020. R1 RCM se ha asociado con más de 750 compañías de atención médica y tenían datos personales de millones de pacientes. Esto incluyó números de Seguro Social, datos de diagnóstico médico y datos financieros. Según los informes, el ataque ocurrió aproximadamente una semana antes de que la compañía planeara publicar sus informes financieros trimestrales. Aunque R1 RCM no proporcionó detalles de comunicaciones internas, puede apostar que alguien notificó al CEO poco después de que se detectó el ataque.

SANS sugiere este formato general para el reporte de incidentes:

¿Cuándo se detectó el problema por primera vez y por quién?	El alcance del incidente	Cómo se contuvo y erradicó
Trabajo realizado durante la recuperación	Áreas donde los equipos CIRT fueron efectivos	Áreas que necesitan mejorar

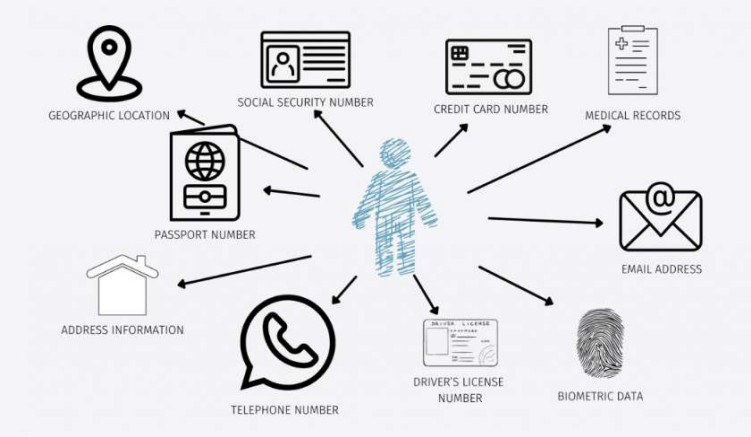
Otros Elementos Importantes a Considerar

La gestión de incidentes no incluye un contraataque contra el atacante

Es importante enfatizar que la gestión de incidentes no incluye un contraataque contra el atacante. Lanzar ataques contra otros es contraproducente y a menudo ilegal. Si un empleado puede identificar al atacante y lanzar un ataque, es probable que resulte en una escalada de las acciones del atacante. En otras palabras, el atacante ahora puede considerarlo personal y lanzar regularmente ataques de rencor.

Además, es probable que el atacante se esconda detrás de una o más víctimas inocentes. Los atacantes a menudo usan métodos de suplantación de identidad para ocultar su identidad o lanzar ataques de zombis en una botnet. Los contraataques pueden ser contra una víctima inocente en lugar de un atacante.

Protección de la información de identificación personal (PII)

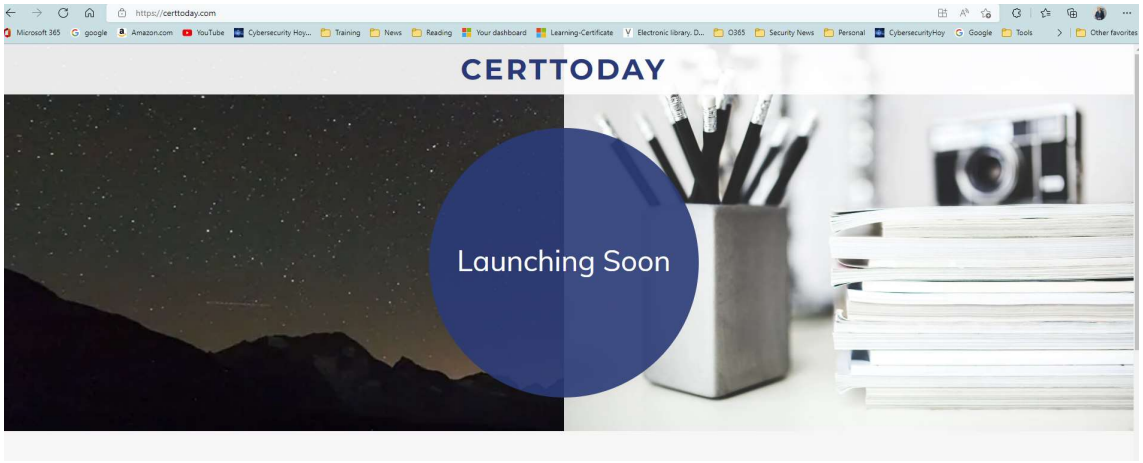


Muchas jurisdicciones tienen leyes específicas que rigen la protección de la información de identificación personal (PII). Si una violación de datos expone la PII, la organización debe informarlo. Las diferentes leyes tienen diferentes requisitos de informes, pero la mayoría incluyen el requisito de notificar a las personas afectadas por el incidente. En otras palabras, si un ataque a un sistema resultó en que un atacante obtuviera PII sobre usted, los propietarios del sistema tienen la responsabilidad de informarle del ataque y de los datos a los que accedieron los atacantes.

Ejemplo: Expirian

En respuesta a incidentes de seguridad graves, la organización debe considerar la posibilidad de informar del incidente a los organismos oficiales. En los Estados Unidos, esto puede significar notificar a la Oficina Federal de Investigaciones (FBI), las oficinas del fiscal de distrito y las agencias estatales y locales de aplicación de la ley. En Europa, las organizaciones pueden denunciar el incidente a la Organización Internacional de Policía Criminal (INTERPOL) o a alguna otra entidad en función del incidente y su ubicación. Estas agencias pueden ayudar en las investigaciones, y los datos que recopilan pueden ayudarlos a prevenir futuros ataques contra otras organizaciones.

Las organizaciones a veces optan por no involucrar a las fuerzas del orden para evitar publicidad negativa o una investigación intrusiva. Sin embargo, esta no es una opción si la información personal está expuesta. Además, algunos estándares de terceros, como el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), requieren que las organizaciones informen ciertos incidentes de seguridad a las fuerzas del orden. Muchos incidentes no se denuncian porque no se reconocen como incidentes. Esto es a menudo el resultado de una capacitación inadecuada. La solución obvia es garantizar que el personal tenga la capacitación pertinente. La capacitación debe enseñar a las personas cómo reconocer incidentes, qué hacer en la respuesta inicial y cómo reportar un incidente.


https://certtoday.com
CERTTODAY
Launching Soon

My Blog

All Posts Cybersecurity News Webinar

October 14, 2022 | Webinar

Plan de Respuestas a Incidentes

Sábado 15 de Octubre de 10 a 11AM. GRATIS.

Continue Reading

October 12, 2022 | Cybersecurity News

Glut of Fake LinkedIn Profiles Pits HR Against the Bots

A recent proliferation of phony executive profiles on LinkedIn is creating something of an identity crisis for the business networking site, and for companies that rely on it to hire and screen prospective employees. Th...

Continue Reading

Referencias

- https://www.securitymetrics.com/blog/6-phases-incident-response-plan
- https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/
- https://www.exabeam.com/incident-response/incident-response-plan/
- https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/