LECCIÓN 1: INTRODUCCIÓN IDENTIFICAR UN INCIDENTE.

RECONOCIMIENTO Y RESPUESTA ANTE INCIDENTES

• Es un conjunto de políticas y procedimientos de seguridad de la información que puede utilizar para identificar, contener y eliminar ataques cibernéticos.

• permite a una organización detectar y detener ataques rápidamente.

• Lo ayuda a minimizar los daños y prevenir futuros ataques.

La respuesta ante incidentes es un conjunto de políticas y procedimientos de seguridad de la información que puede utilizar para identificar, contener y eliminar ciberataques. El objetivo de la respuesta ante incidentes es habilitar a una organización para que detecte y detenga ataques rápidamente, lo que ayuda a minimizar el daño y evitar ataques futuros del mismo tipo.

RECONOCIMIENTO DE INCIDENTES

No todos los eventos son incidentes que necesitan corregirse de inmediato.

• Iniciar sesión desde una ubicación remota
• Disco duro defectuoso que todavía está completamente operativo
• Empleado tratando de acceder a recursos a los que no debería acceder

¿Cómo sabría una empresa si se estaba produciendo un abuso?
¿Cómo diferenciarían entre eventos anormales que necesitan su atención e incidentes que necesitan analizarse y corregirse de inmediato?

No todos los eventos son incidentes que necesitan corregirse de inmediato. Veamos algunos ejemplos de tales eventos:

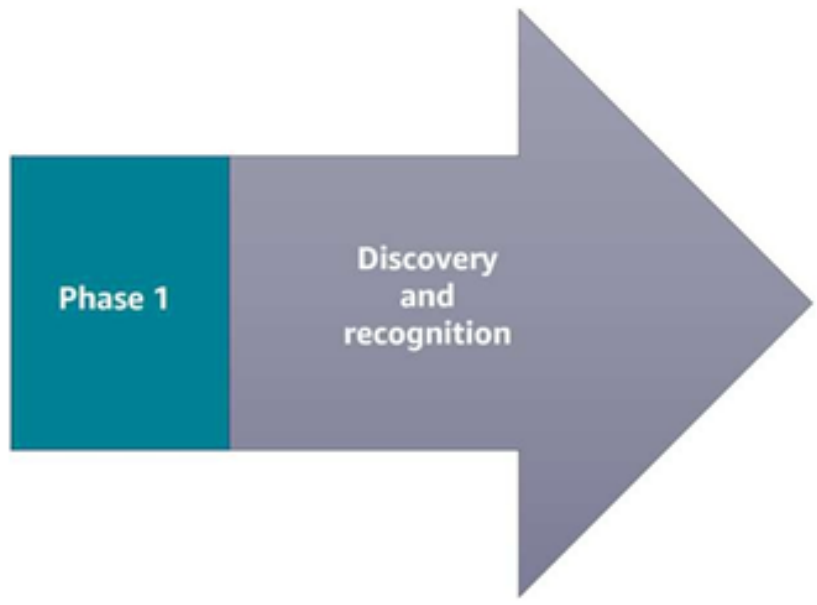
Inicio de sesión desde una ubicación remota: un empleado puede estar viajando o utilizando una red privada virtual (VPN) aprobada.

Empleado que intenta acceder a recursos a los que no debería acceder: aunque esto podría no constituir una infracción si se deniega el acceso, sigue siendo una información de comportamiento que debe supervisar.

Disco duro averiado que todavía está en pleno funcionamiento: conocer esta información permite a una empresa programar oportunamente un ciclo de las unidades sin entrar en pánico ni cambiarlas en caliente cuando es demasiado tarde y ya ha fallado. El intercambio en caliente es el acto de quitar componentes o conectarlos a un sistema informático mientras la alimentación permanece encendida.

FASE 1: DESCUBRIMIENTO Y RECONOCIMIENTO

- **Identificación, registro y categorización de incidentes**
- **Notificación y escalado de incidentes**
- **Investigación y diagnóstico**



La respuesta a incidentes tiene dos fases. La primera fase es la fase de descubrimiento y reconocimiento. Aquí es donde se lleva a cabo la identificación, el registro y la categorización del incidente. Una vez que se identifica un incidente a través de informes de usuarios, análisis de soluciones o identificación manual, el incidente se registra y puede comenzar una investigación y categorización.

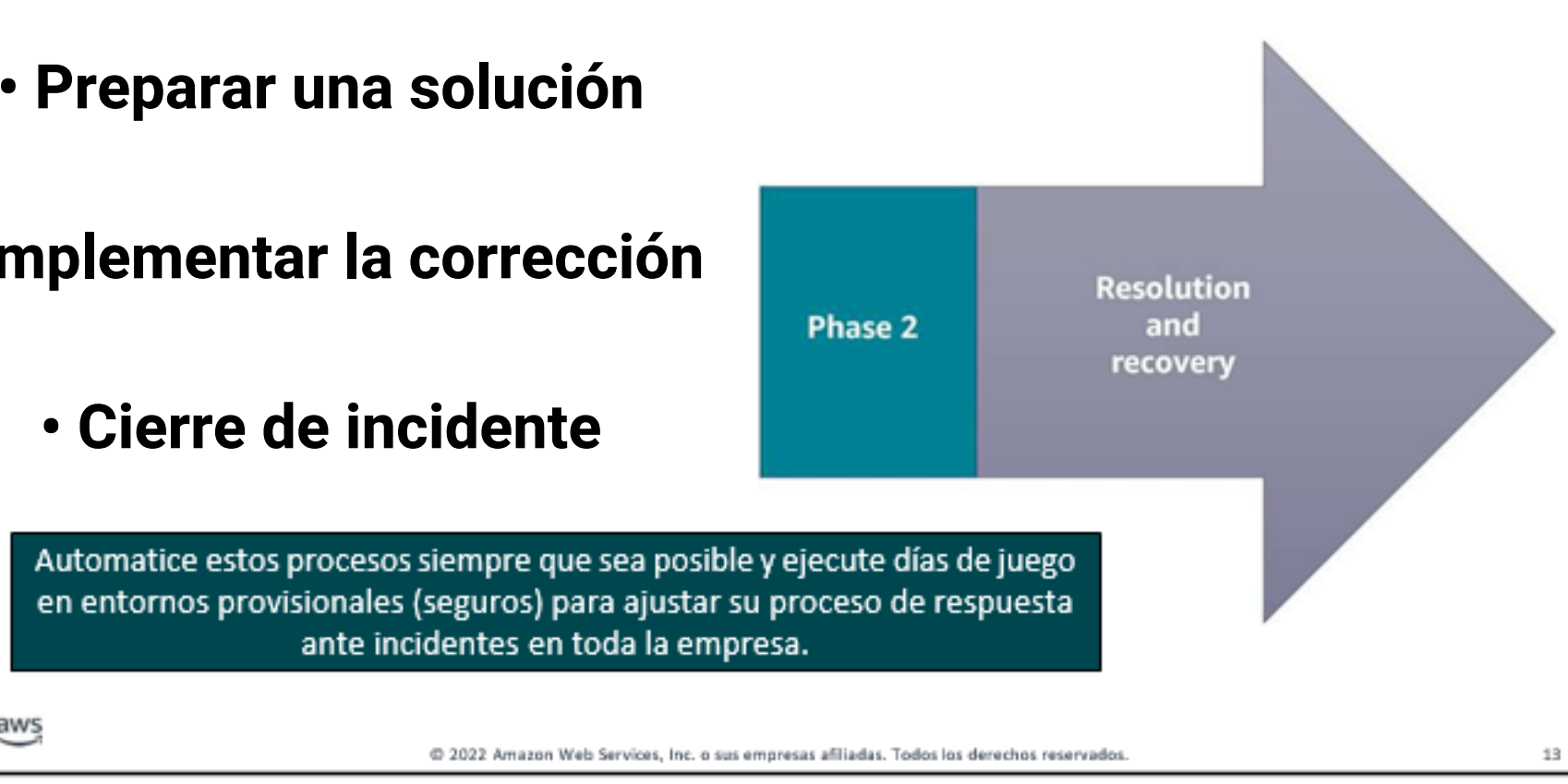
Durante esta fase, se recibe una notificación. El usuario configura las notificaciones y las alertas específicas las inician para enviar un correo electrónico, un mensaje de texto SMS o una notificación automática a través de una aplicación móvil. La escalada de incidentes es lo que sucede cuando un empleado no puede resolver un incidente por sí mismo y necesita pasar la tarea a un empleado más experimentado o especializado.

La investigación y el diagnóstico incluyen la realización de una investigación de incidentes para recopilar respuestas y desarrollar estrategias para resolver cualquier amenaza.

AWS ofrece una variedad de servicios y productos que ayudan a las empresas a descubrir e identificar eventos que podrían conducir a un incidente o que ya se han convertido.

FASE 2: RESOLUCIÓN Y RECUPERACIÓN

- **Aislamiento forense (si es software, reproducir el error)**
- **Preparar una solución**
- **Implementar la corrección**
- **Cierre de incidente**



Cuando una empresa ha identificado la falla de un componente, una reducción en la calidad del servicio o una vulnerabilidad que necesita solución, pasa a la fase de resolución y recuperación de la respuesta ante incidentes.
Esta segunda fase consta de lo siguiente:

Aislamiento forense:

Aísle el incidente y realice una inmersión profunda para descubrir el problema.

Los análisis forenses suelen requerir la captura de la imagen del disco o de la configuración “tal y como está” de un sistema operativo. El problema podría ser un error en el código base. Si es así, entonces necesita reproducir el error. Si no puede reproducir el error que experimentó el cliente, no podrá solucionarlo.

Preparación de una corrección:
Reproduzca el problema, aplique una solución y pruebe.

Implementación de la corrección:
Empuje cualquier infraestructura nueva, como código, o cualquier código de aplicación nuevo a producción.

Cierre de incidente:
Resuelva el incidente.

AWS ofrece una variedad de servicios y productos que ayudan a las empresas a solucionar un incidente.

ESTOS SON ALGUNOS APRENDIZAJES CLAVE DE ESTA LECCIÓN:

La respuesta ante incidentes es un conjunto de políticas y procedimientos de seguridad de la información que puede utilizar para identificar, contener y eliminar ciberataques.

No todos los eventos son incidentes que necesitan corregirse de inmediato.

La primera fase de un incidente es la fase de descubrimiento y reconocimiento.

La segunda fase de un incidente es la fase de resolución y recuperación.