

INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 22



1 de FeBREro de 2024

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Enunciado 2](#_Toc157703075)

[Gestión de incidentes: Escaneo de redes 3](#_Toc157703076)

[Preparación 3](#_Toc157703077)

[Identificación 3](#_Toc157703078)

[Contención 4](#_Toc157703079)

[Mitigación 4](#_Toc157703080)

[Recuperación 5](#_Toc157703081)

[Actuaciones post-incidentes 5](#_Toc157703082)

# Enunciado

Realiza la Gestión del Incidente solicitado siguiendo las siguientes fases :

1º.- Preparación.-

Afecta a todos los activos.-

2º.- Identificación.-

Afecta solamente al equipo con el IDS/IPS.-

3º.- Contención.-

Afecta solamente al equipo con el IDS/IPS.-

4º.- Mitigación.-

Afecta a todos los activos.-

5º.- Recuperación.-

Afecta a todos los activos.-

6º.- Actuaciones post-incidente.-

------------------------------------

Activos Informáticos :

1º.- CPD1 : Expedientes académicos + laborales .-

2º.- CPD2 : Moodle Centros ( Aula Virtual ) + Página Web .-

3º.- Equipos Equipo Directivo +Admon + Sala de Profesoras/es + Ordenadores Departamentos +Ordenador Profesor Aula.-

4º.- Ordenadores de Laboratorio.-

5º.- Elementos de red .-

# Gestión de incidentes: Escaneo de redes

# Preparación

**Revisión y actualización de políticas de seguridad:**

- Evaluar las políticas de seguridad existentes en relación con las mejores prácticas de la industria y los estándares de cumplimiento.

- Actualizar las políticas para abordar nuevas amenazas y vulnerabilidades, así como para incluir procedimientos específicos para la gestión de incidentes.

**Garantizar software de seguridad actualizado:**

- Implementar un sistema de gestión de parches para asegurar que todos los sistemas estén actualizados con los últimos parches de seguridad.

- Configurar actualizaciones automáticas para el software de seguridad, como antivirus y firewalls, para garantizar su eficacia contra las amenazas emergentes.

**Realizar copias de seguridad:**

- Establecer un programa regular de copias de seguridad automatizadas para todos los datos críticos, con almacenamiento redundante tanto en local como en la nube.

- Realizar pruebas periódicas de restauración de datos para verificar la integridad y la capacidad de recuperación del sistema de copias de seguridad.

# Identificación

**Monitoreo continuo:**

- Configurar el IDS/IPS para monitorear todos los puntos de entrada y salida de la red, así como el tráfico interno, en busca de patrones de comportamiento anómalo.

- Utilizar firmas y reglas específicas para detectar actividades maliciosas conocidas, así como técnicas de detección basadas en comportamiento para identificar amenazas nuevas y desconocidas.

**Alertas tempranas:**

- Configurar alertas automáticas para notificar al equipo de seguridad cuando se detecten eventos sospechosos, proporcionando detalles sobre el tipo de actividad detectada y la ubicación en la red.

- Establecer un protocolo de escalada para responder rápidamente a alertas críticas y coordinar acciones de mitigación.

# Contención

**Respuesta inmediata:**

- Implementar medidas de contención automáticas para bloquear el tráfico malicioso y aislar los sistemas comprometidos, minimizando el impacto en el resto de la red.

- Desconectar físicamente los sistemas afectados de la red para evitar una mayor propagación del incidente mientras se investiga la causa raíz.

**Restricción de acceso:**

- Limitar el acceso privilegiado a los sistemas comprometidos solo al personal autorizado necesario para llevar a cabo la investigación y la respuesta al incidente.

- Implementar controles de acceso adicionales, como autenticación multifactor, para proteger los sistemas críticos y evitar accesos no autorizados.

# Mitigación

**Corrección de vulnerabilidades:**

- Identificar las vulnerabilidades explotadas durante el incidente mediante análisis forense y pruebas de penetración, y aplicar parches de seguridad y actualizaciones para mitigar el riesgo.

- Implementar medidas proactivas de seguridad, como configuraciones seguras por defecto y políticas de acceso mínimas, para reducir la superficie de ataque.

**Análisis forense:**

- Recopilar y analizar evidencia digital, incluidos registros de eventos, archivos de registro y volcados de memoria, para determinar la causa y el alcance del incidente.

- Utilizar herramientas forenses avanzadas para reconstruir la secuencia de eventos y identificar a los posibles culpables, en caso de que se haya producido un ataque deliberado.

**Refuerzo de la seguridad:**

- Implementar controles de seguridad adicionales, como sistemas de detección y prevención de intrusiones, sistemas de gestión de identidades y accesos, y cifrado de datos, para proteger los activos críticos contra futuros ataques.

# Recuperación

**Restauración de sistemas:**

- Restaurar los sistemas afectados utilizando las copias de seguridad más recientes disponibles, priorizando la recuperación de los datos críticos y los servicios esenciales.

- Verificar la integridad de los datos restaurados para garantizar que no hayan sido comprometidos durante el incidente, utilizando herramientas de validación de integridad y comparación de archivos.

**Pruebas de funcionalidad:**

- Realizar pruebas exhaustivas de todos los sistemas y servicios restaurados para garantizar su funcionalidad y rendimiento adecuados antes de devolverlos al entorno de producción.

- Supervisar de cerca los sistemas restaurados durante un período de tiempo para detectar cualquier anomalía o comportamiento inesperado que pueda indicar una persistencia del incidente.

# Actuaciones post-incidentes

**Evaluación de la respuesta:**

- Realizar una revisión detallada del incidente, incluyendo una evaluación de la efectividad de las medidas de respuesta y las áreas de mejora identificadas durante el proceso.

- Documentar todas las acciones tomadas durante la gestión del incidente, incluyendo las decisiones clave, los hallazgos forenses y las lecciones aprendidas para futuras referencias.

**Actualización de políticas:**

- Utilizar los hallazgos del incidente para actualizar y mejorar las políticas y procedimientos de seguridad de la organización, asegurándose de abordar las vulnerabilidades identificadas y las deficiencias en la respuesta al incidente.

- Comunicar los cambios en las políticas de seguridad a todo el personal y proporcionar capacitación adicional según sea necesario para garantizar su cumplimiento.

**Capacitación del personal:**

- Ofrecer capacitación y concienciación en seguridad adicionales al personal, destacando las lecciones aprendidas del incidente y proporcionando orientación sobre cómo reconocer y reportar posibles amenazas en el futuro.

- Realizar simulacros de incidentes regulares para mantener al personal preparado y asegurarse de que estén familiarizados con los procedimientos de respuesta en caso de emergencia.