

INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 31



19 de marzo de 2024

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Enunciado 2](#_Toc161742000)

[GESTIÓN DE INCIDENTE--Compromiso de Cuenta con Privilegios. 3](#_Toc161742001)

[Preparación 3](#_Toc161742002)

[Identificación 3](#_Toc161742003)

[Contención 3](#_Toc161742004)

[Mitigación 3](#_Toc161742005)

[Recuperación 4](#_Toc161742006)

[Actuaciones post-incidentes 4](#_Toc161742007)

# Enunciado

como el robo de credenciales de acceso mediante interpretación de tráfico o mediante el acceso a documentos físicos.

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 INCIDENTE--Compromiso de Cuenta con Privilegios.

# Preparación

**- Equipo de respuesta a incidentes:** Designa un equipo responsable de gestionar el incidente, que incluya a expertos en seguridad de la información, administradores de sistemas y representantes de las partes interesadas pertinentes.

**- Recursos técnicos:** Asegúrate de que el equipo tenga acceso a herramientas de seguridad como sistemas de detección de intrusos (IDS/IPS), software antivirus, registros de tráfico de red y sistemas de gestión de incidentes.

**- Procedimientos de respuesta:** Desarrolla y revisa los procedimientos de respuesta a incidentes, incluyendo la asignación de roles y responsabilidades, los pasos a seguir para la contención y mitigación del incidente, y los protocolos de comunicación interna y externa.

**- Contactos de emergencia:** Mantén actualizada una lista de contactos de emergencia, incluyendo proveedores de servicios de seguridad cibernética, autoridades reguladoras y personal legal.

# Identificación

**- Monitoreo de tráfico de red:** Utiliza el equipo con IDS/IPS para monitorear el tráfico de red en busca de actividades sospechosas, como intentos de acceso no autorizado o transferencias de datos inusuales.

**- Análisis de registros:** Examina los registros de tráfico de red y de sistemas en busca de anomalías, como intentos de inicio de sesión fallidos, accesos desde ubicaciones inusuales o transferencias de datos inusuales.

**- Alertas de seguridad:** Configura alertas en el sistema de detección de intrusos para notificar al equipo de respuesta a incidentes sobre actividades potencialmente maliciosas.

# Contención

**- Bloqueo de tráfico malicioso:** Utiliza el equipo con IDS/IPS para bloquear el tráfico identificado como malicioso y evitar una mayor propagación del incidente.

**- Aislamiento de sistemas comprometidos:** Desconecta los sistemas afectados de la red y oíslos para evitar que los atacantes continúen accediendo a ellos o propagando el malware.

**- Restricción de accesos:** Limita el acceso al entorno afectado solo al personal autorizado necesario para la investigación y la recuperación.

# Mitigación

**- Cambio de credenciales:** Inmediatamente después de contener el incidente, cambia todas las credenciales comprometidas, incluyendo contraseñas de usuario, claves de acceso a sistemas y certificados de seguridad.

**- Actualización de sistemas:** Aplica parches de seguridad y actualizaciones de software en todos los sistemas afectados para corregir las vulnerabilidades que podrían haber sido explotadas por los atacantes.

**- Auditoría de seguridad:** Realiza auditorías de seguridad adicionales para identificar y corregir cualquier otra vulnerabilidad que pueda haber sido explotada durante el incidente.

# Recuperación

**- Restauración desde copias de seguridad:** Restaura los sistemas afectados desde copias de seguridad limpias y verificadas para asegurarte de eliminar cualquier malware o acceso no autorizado.

**- Verificación de servicios:** Verifica la funcionalidad de los servicios restaurados para asegurarte de que estén operativos de manera segura y sin compromisos.

# Actuaciones post-incidentes

**- Documentación detallada:** Documenta todas las acciones tomadas durante el incidente, incluyendo hallazgos relevantes, pasos de respuesta y lecciones aprendidas.

**- Capacitación y concienciación:** Proporciona sesiones de capacitación para el personal sobre prácticas de seguridad cibernética y conciencia de amenazas para reducir el riesgo de futuros incidentes.

**- Revisión de políticas:** Revisa y actualiza las políticas de seguridad de la información para abordar las lecciones aprendidas del incidente y mitigar los riesgos futuros.