# INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 29

7 DE MARZO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

# Índice

# 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 INCIDENTE--Intento de Acceso con Vulneración de Credenciales.

## Preparación

- Realiza un inventario detallado de todos los activos informáticos, incluyendo servidores, equipos de red, aplicaciones y datos críticos.

- Establece políticas de seguridad claras y procedimientos de respuesta a incidentes para garantizar una respuesta rápida y efectiva.

- Implementa medidas de seguridad proactivas, como firewalls, sistemas de detección de intrusiones, antivirus y sistemas de gestión de parches.

- Capacita al personal en seguridad de la información y en cómo reconocer y reportar incidentes de seguridad.

## Identificación

- Configura los sistemas de detección de intrusiones (IDS/IPS) para monitorear y analizar el tráfico de red en busca de patrones y comportamientos sospechosos.

- Utiliza herramientas de análisis de registros para examinar los registros de eventos en busca de indicadores de compromiso (IoC) y actividades anómalas.

- Implementa alertas tempranas y sistemas de notificación para informar al equipo de seguridad sobre posibles incidentes en tiempo real.

## Contención

- Activa los protocolos de respuesta a incidentes para contener la amenaza y evitar que se propague a otros sistemas.

- Desconecta los sistemas comprometidos de la red principal para evitar una mayor propagación del incidente.

- Bloquea el tráfico malicioso utilizando reglas de firewall y políticas de seguridad específicas.

## Mitigación

- Identifica y corrige las vulnerabilidades que fueron explotadas durante el incidente.

- Aplica parches de seguridad y actualizaciones en todos los sistemas para cerrar posibles brechas de seguridad.

- Implementa medidas adicionales de seguridad, como reforzar contraseñas, aplicar controles de acceso más estrictos y segmentar la red para limitar el alcance del ataque.

## Recuperación

- Restaura los sistemas afectados a un estado operativo normal utilizando copias de seguridad y puntos de restauración, asegurándote de que los datos no se vean comprometidos.

- Realiza análisis forense en los sistemas comprometidos para determinar el alcance del daño y la naturaleza del ataque.

- Verifica la integridad de los sistemas restaurados y realiza pruebas exhaustivas para asegurarte de que estén libres de malware y vulnerabilidades.

## Actuaciones post-incidentes

- Realiza una revisión exhaustiva del incidente para identificar las causas subyacentes y las lecciones aprendidas.

- Actualiza las políticas y procedimientos de seguridad para mitigar riesgos similares en el futuro.

- Proporciona informes detallados sobre el incidente, incluyendo el impacto, las acciones tomadas y las recomendaciones para mejorar la postura de seguridad de la organización.