INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 19

22 DE ENERO 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 .-

Ejercicio

1. Preparación:

Objetivo:

Estar listos para responder a incidentes de seguridad de manera efectiva.

Activos:

- Asegurar que todos los sistemas tengan software de seguridad actualizado: Mantener actualizados los programas antivirus, firewalls y otros sistemas de seguridad en todos los activos informáticos.

- Realizar copias de seguridad periódicas de los datos críticos: Implementar un plan de copias de seguridad regular para garantizar la disponibilidad de los datos en caso de un incidente.

- Documentar procedimientos de respuesta a incidentes: Crear y mantener documentación detallada sobre cómo responder a diferentes tipos de incidentes, incluyendo contactos de emergencia y roles.

2. Identificación:

Objetivo:

Detectar la presencia de un incidente de seguridad lo antes posible.

Equipo con IDS/IPS:

- Monitorear activamente el tráfico de red en busca de comportamientos sospechosos: Utilizar sistemas de detección de intrusiones para analizar el tráfico y detectar actividades anómalas.

- Configurar alertas para notificar posibles incidentes: Establecer alertas automáticas que informen a los responsables de seguridad sobre posibles amenazas.

3. Contención:

Objetivo:

Limitar la propagación y el impacto del incidente.

Equipo con IDS/IPS:

- Implementar reglas para bloquear el tráfico malicioso identificado: Configurar los IDS/IPS para bloquear o limitar la comunicación con sistemas sospechosos.

- Desconectar sistemas comprometidos de la red: Aislar sistemas afectados para prevenir la propagación de la amenaza.

4. Mitigación:

Objetivo:

Reducir el impacto y prevenir futuros incidentes.

Activos:

- Aplicar parches de seguridad y actualizaciones: Mantener todos los sistemas actualizados con los últimos parches de seguridad.

- Fortalecer las políticas de seguridad: Revisar y mejorar las políticas de seguridad, como contraseñas, permisos de acceso y políticas de firewall.

5. Recuperación:

Objetivo:

Restaurar la funcionalidad normal del sistema.

Activos:

- Restaurar sistemas desde copias de seguridad verificadas: Utilizar las copias de seguridad previamente realizadas para restaurar los sistemas a un estado de funcionamiento.

- Realizar pruebas de funcionamiento antes de poner en producción: Verificar que los sistemas restaurados funcionen correctamente antes de permitir el acceso normal.

6. Actuaciones Post-Incidente:

Objetivo:

Analizar el incidente y tomar medidas para evitar recurrencias.

Activos:

- Realizar una revisión exhaustiva del incidente: Analizar cómo ocurrió el incidente, qué se vio afectado y qué medidas se tomaron.

- Actualizar y mejorar los procedimientos de seguridad: Modificar los procedimientos de seguridad según lo aprendido del incidente para fortalecer las defensas.

- Capacitar al personal en medidas de seguridad preventivas: Proporcionar formación continua al personal para aumentar la conciencia de seguridad y la capacidad de respuesta.