ALBERTO MÉNDEZ NÚÑEZ

Fundamentos de la Ciberseguridad

CIB

**Amenaza:** es todo aquello que puede poner en peligro nuestra información.

**Vulnerabilidad:** es una debilidad o un fallo en nuestro sistema que puede ser explotada por un atacante.

**Confidencialidad:** garantizar que la información solo sea accesible a las personas autorizadas.

**Integridad:** asegurar que la información no sea alterada de manera no autorizada.

**Disponibilidad:** que la información esté disponible y utilizable cuando los usuarios autorizados la necesiten.

**Malware:** software malicioso diseñado para dañar, robar información o tomar el control de sistemas.

**Ingeniería social:** manipulación psicológica de personas para obtener acceso a información o sistemas.

**DoS:** ataque de denegación de servicio que busca hacer que un servicio no esté disponible saturándolo con peticiones falsas desde un mismo dispositivo.

**DDoS:** ataque de denegación de servicio distribuido que busca hacer que un servicio no esté disponible saturándolo con peticiones falsas desde varios dispositivos.

**Man-in-the-Middle:** ataque en el que un intruso intercepta y manipula la comunicación entre dos partes sin que lo sepan.

Exploi**t:** código o técnica que aprovecha una vulnerabilidad en un sistema para comprometerlo.

**Inyección SQL:** ataque que inserta código SQL malicioso en una consulta para acceder o modificar bases de datos.

**Cross-Site-Scripting:** ataque que inyecta scripts maliciosos en páginas web vistas por otros usuarios.

**Cifrar:** transformar datos con un algoritmo de cifrado para proteger la información.

**Ransomware:** tipo de malware que cifra los archivos del usuario y exige un pago para liberarlos.

**Autenticación Multifactor:** método de verificación que requiere más de un factor.

**Roles:** responsabilidades asignadas a un usuario dentro de un sistema.

**Permisos:** autorizaciones que se le otorgan a un usuario que controlan las cosas que puede o no hacer en un sistema.

**Regla de firewall:** instrucción de seguridad que controla qué tráfico de red está permitido o bloqueado.

**Filtrado de puertos:** técnica para permitir o bloquear el tráfico que usa ciertos puertos de red.

**Filtrado de protocolos:** control del tráfico según el tipo de protocolo.

**Router:** dispositivo que dirige el tráfico entre diferentes redes y aplica medidas básicas de seguridad.

**Herramientas de monitoreo:** Software o sistemas que supervisan continuamente la red, servidores, aplicaciones o dispositivos para detectar cambios, problemas de rendimiento o actividad sospechosa.

**Herramientas de auditoría:** Sistemas que permiten revisar y evaluar la seguridad, configuraciones y cumplimiento de políticas.

**Incidentes de seguridad:** Eventos o series de eventos que comprometen la confidencialidad, integridad o disponibilidad de la información o los sistemas.

**Detección:** Proceso de identificar eventos de seguridad o actividad sospechosa en la red o sistemas.

**Análisis:** Etapa donde se investigan los incidentes detectados para entender el alcance, la causa y el impacto.

**Contención:** Acciones para limitar la propagación o el impacto de un incidente mientras se desarrolla la respuesta.

**Erradicación:** Eliminar completamente la causa raíz del incidente.

**Recuperación:** Restaurar los sistemas a su estado normal de funcionamiento tras un incidente de seguridad.

**Aprendizaje:** Revisión posterior al incidente para identificar mejoras en procesos, políticas y herramientas, reduciendo riesgos futuros.

**Indicadores de compromiso:** Evidencias que muestran que un sistema ha sido comprometido o atacado.

**Estrategias proactivas:** Medidas preventivas para reducir la probabilidad de incidentes de seguridad.

**Análisis forense:** Investigación detallada de un incidente de seguridad para descubrir cómo ocurrió, quién lo causó y qué se vio afectado.

**Cortafuegos:** Dispositivo o software que controla el tráfico de red según reglas predefinidas, permitiendo o bloqueando conexiones.

**IDS:** Sistema de detección de intrusiones que monitorea la red o sistemas para identificar actividad sospechosa o ataques.

**IPS:** Sistema de prevención de intrusiones que detecta y bloquea automáticamente actividad maliciosa en tiempo real.

**Antivirus:** Software que detecta, bloquea y elimina malware en sistemas y dispositivos.

**Cortafuegos basado en red:** Firewall que protege toda la red y filtra tráfico entre segmentos, aplicando políticas centralizadas.

**Cortafuegos basado en host:** Firewall instalado en un **equipo individual** (servidor, PC o dispositivo) para protegerlo del tráfico no autorizado.

**Antimalware:** Software diseñado para **detectar, prevenir y eliminar todo tipo de malware** (virus, troyanos, ransomware, spyware, etc.).

**RGPD:** Normativa europea que regula la **protección de datos personales** de ciudadanos de la UE.

**ENS:** Marco normativo español que establece **medidas de seguridad para los sistemas de información** del sector público.

**Datos sensibles:** Información que, por su naturaleza, requiere **mayor protección** debido a su carácter personal o confidencial.

**Políticas de acceso:** Normas y reglas que determinan **quién puede acceder a qué información o recursos** dentro de un sistema o red.

**Ciclo de vida de la información:** Conjunto de **etapas por las que pasa la información** desde su creación hasta su destrucción:

**Diagnóstico de fallos:** Proceso de **identificación y análisis de problemas o errores** en sistemas, redes o aplicaciones.

**Propuesta de mejora:** Sugerencia o plan para **optimizar procesos, sistemas o controles de seguridad** basándose en el diagnóstico o auditoría realizada.

**Registro de incidencias:** Documento o sistema que **documenta todos los incidentes ocurridos**, incluyendo detalles, responsables, acciones tomadas y resultados.