ÍNDICE

1. Amenazas y vulnerabilidades. 3
Confidencialidad 3
Disponibilidad 3
Malware 3
Ingeniería social 3
Ataques a la red (DoS y DDoS) 3
Man-in-the-Middle (MitM) 4
Exploits 4
Inyección SQL 4
Cross-Site Scripting (XSS) 4
Redes inalámbricas sin cifrar o con cifrados obsoletos 4
Ransomware 4
2. Medidas de protección básicas 4
Autenticación Multifactor (MFA) 4
Roles y permisos 5
Reglas de firewall 5
Filtro de puertos y protocolos 5
Routers 5
Monitoreo y auditoría 5
3. Análisis de los incidentes de seguridad 5
Ciclo de vida de un incidente 5
Detección 5
Análisis 6
Contención 6
Erradicación 6
Recuperación 6
Aprendizaje 6
Indicadores de compromiso (IoC) 6
Estrategias proactivas 6
Análisis forense 6
4. Herramientas y tecnologías de aplicación. 7
Cortafuegos (Firewall) 7
IDS (Intrusion Detection System) 7
IPS (Intrusion Prevention System) 7

Software Antivirus 7
Cortafuegos basados en red 7
Cortafuegos basados en host 7
Antimalware 7
5. Normativa y buenas prácticas de uso. 7
Reglamento General de Protección de Datos (RGPD) 7
ISO/IEC 27001 8
Esquema Nacional de Seguridad (ENS) 8
Datos sensibles 8
Políticas de acceso 8
Diagnóstico de fallos 8
Propuestas de mejora 8
Registro de incidencias 8

1. Amenazas y vulnerabilidades.

Las **amenazas** informáticas son acciones, eventos o circunstancias, intencionadas o no, que atentan contra la seguridad, confidencialidad, integridad o disponibilidad de sistemas informáticos, redes y datos. Su objetivo suele ser el robo de información, la interrupción de servicios o la interrupción del funcionamiento normal de un sistema, y pueden provenir de fuentes como hackers, empleados descontentos o errores accidentales.

Las **vulnerabilidades** informáticas son debilidades o fallos en sistemas, software, hardware o redes que pueden ser explotados por atacantes para comprometer la seguridad de la información, obteniendo acceso no autorizado, robando datos, o interrumpiendo servicios. Estas fallas pueden originarse por errores de programación, configuraciones incorrectas, software desactualizado, o fallos en el diseño de un sistema.

Confidencialidad

Garantiza que la información solo sea accesible y conocida por las entidades (personas, procesos o sistemas) autorizadas. Implica mantener los datos en secreto o privados para prevenir su divulgación no autorizada, intencional o accidental.
Integridad

Asegura que la información y los sistemas se mantienen precisos, completos y consistentes durante todo su ciclo de vida. Impide que los datos sean modificados o eliminados de forma no autorizada.

Disponibilidad

Es la capacidad de asegurar que los usuarios autorizados tengan acceso fiable y oportuno a la información y a los recursos del sistema (aplicaciones, redes, equipos) cuando sea necesario.

Malware

Abreviatura de Malicious Software (Software Malicioso). Es cualquier programa informático diseñado para infiltrarse o dañar un sistema sin el consentimiento del usuario. Incluye virus, gusanos, troyanos, y más.

Ingeniería social

Conjunto de técnicas de manipulación psicológica utilizadas por los atacantes para engañar a las personas y lograr que realicen acciones o revelen información confidencial. No se enfoca en fallos técnicos, sino en el factor humano (ej.: phishing, vishing).

Ataques a la red (DoS y DDoS)

- DoS (Denial of Service - Denegación de Servicio): Intento malicioso de hacer que un servicio o recurso de red (como un sitio web o servidor) sea inaccesible para sus usuarios legítimos al sobrecargarlo con tráfico o solicitudes desde una sola fuente.

- DDoS (Distributed Denial of Service - Denegación de Servicio Distribuida): Es una forma de ataque DoS donde la sobrecarga proviene de múltiples fuentes (a menudo una "botnet" o red de ordenadores comprometidos), lo que hace mucho más difícil su mitigación.

Man-in-the-Middle (MitM)

Un tipo de ciberataque en el que el atacante se inserta de forma encubierta entre dos partes que se comunican. El atacante intercepta, y a menudo modifica, la comunicación o los datos que fluyen entre ellas, haciéndose pasar por una de las partes ante la otra.

Exploits

Es un fragmento de código, datos o secuencia de comandos diseñado para aprovechar una vulnerabilidad o fallo de seguridad en un sistema operativo, aplicación o red, generalmente con el fin de obtener un control no autorizado o causar una denegación de servicio.

Inyección SQL

Una vulnerabilidad en aplicaciones web donde un atacante inserta una o varias sentencias SQL maliciosas en una consulta (generalmente a través de campos de entrada de usuario) que la aplicación envía a su base de datos. Esto puede permitir al atacante ver, modificar o eliminar datos, e incluso obtener acceso de administrador.

Cross-Site Scripting (XSS)

Una vulnerabilidad en aplicaciones web que permite a un atacante inyectar scripts maliciosos (típicamente JavaScript) en el contenido de una página web visitada por otros usuarios. El navegador de la víctima ejecuta este código, lo que puede resultar en el robo de cookies, el secuestro de sesiones o la alteración del contenido de la página.

Redes inalámbricas sin cifrar o con cifrados obsoletos

Se refiere a redes Wi-Fi que o bien no utilizan ningún tipo de cifrado (redes abiertas), dejando las comunicaciones totalmente expuestas, o utilizan protocolos de cifrado antiguos e inseguros (como WEP o versiones obsoletas de WPA), que pueden ser vulnerados o descifrados fácilmente por un atacante.

Ransomware

Un tipo de malware diseñado para cifrar (encriptar) los archivos o bloquear el sistema operativo de la víctima, impidiéndole el acceso a sus datos. El atacante exige un rescate (generalmente en criptomonedas) a cambio de la clave de descifrado.

2. Medidas de protección básicas

Autenticación Multifactor (MFA)

Un método de autenticación de identidad que requiere que el usuario presente dos o más factores de verificación independientes para obtener acceso a un sistema o recurso. Estos factores suelen ser algo que el usuario sabe (contraseña), algo que el usuario posee (móvil, token) y/o algo que el usuario es (huella dactilar, biometría).

Roles y permisos

- Roles: Conjunto de privilegios y responsabilidades predefinidos que se asignan a un usuario o grupo de usuarios dentro de un sistema (ejemplo: "Administrador", "Usuario Estándar", "Invitado").

- **Permisos**: Las capacidades específicas que un usuario, a través de su rol, tiene para interactuar con un recurso (ejemplo: leer, escribir, ejecutar, eliminar un archivo o registro).

Reglas de firewall

Directrices o políticas preconfiguradas que especifican qué tráfico de red se permite (aceptar) y qué tráfico se rechaza (denegar) en función de diversos criterios. Son esenciales para filtrar y controlar el flujo de datos entre redes (o dentro de ellas).

Filtro de puertos y protocolos

Una función de las firewalls que inspecciona el tráfico de red: - Puertos: Se utiliza para permitir o denegar la comunicación basándose en el número de puerto de red (ejemplo: puerto 80 para HTTP, 443 para HTTPS). - Protocolos: Se utiliza para permitir o denegar basándose en el protocolo de comunicación utilizado (ejemplo: TCP, UDP, ICMP).

Routers

Un dispositivo de red que opera en la Capa 3 (Red) del modelo OSI. Su función principal es encaminar paquetes de datos entre diferentes redes informáticas (por ejemplo, entre tu red local e Internet), eligiendo el camino más eficiente para la transmisión.

Monitoreo y auditoría

- Monitoreo: Proceso continuo de vigilancia de un sistema, una red o una aplicación para recopilar, analizar y evaluar datos de actividad en tiempo real. Su objetivo es detectar incidentes de seguridad, anomalías o cambios operativos.

- Auditoría: Revisión sistemática y periódica de los registros (logs), configuraciones, políticas y procedimientos de seguridad para evaluar su efectividad y garantizar el cumplimiento de normativas.

3. Análisis de los incidentes de seguridad

Ciclo de vida de un incidente

Conjunto de etapas estructuradas que una organización sigue para gestionar y responder a un incidente de seguridad, desde que se detecta hasta que se aprende de la experiencia.

Detección

La fase inicial del ciclo de vida donde se identifican actividades, anomalías o eventos que indican una posible intrusión, ataque o fallo de seguridad en el sistema.

Análisis

La etapa donde se examinan los datos recopilados (registros, tráfico, logs) para comprender la naturaleza, el alcance y la causa raíz del incidente.

Contención

La acción de tomar medidas inmediatas para detener la propagación del incidente y limitar el daño, aislando los sistemas afectados sin apagarlos necesariamente (ejemplo: desconectar un servidor de la red).

Erradicación

La fase en la que se eliminan completamente la causa raíz del incidente, los elementos maliciosos (como el malware) y las vulnerabilidades que fueron explotadas por el atacante.

Recuperación

El proceso de restaurar los sistemas y servicios afectados a su estado normal de funcionamiento, asegurando que estén limpios, parcheados y listos para volver a la producción.

Aprendizaje

La etapa final, y crucial, donde se documenta todo el proceso, se realiza una revisión post-incidente y se identifican las lecciones aprendidas para mejorar las políticas, procedimientos y defensas de seguridad futuras.

Indicadores de compromiso (IoC)

Evidencias forenses que indican que una red, sistema o aplicación ha sido objeto de una intrusión o ataque de seguridad. Pueden ser hashes de archivos maliciosos, direcciones IP de atacantes, nombres de dominio, o patrones de actividad inusual en el sistema.

Estrategias proactivas

En seguridad, se refiere a la adopción de medidas y controles que buscan prevenir incidentes antes de que ocurran, en lugar de solo reaccionar a ellos (ejemplo: instalación y correcta configuración de firewalls, actualización de sistemas, etc.).

Análisis forense

La aplicación de técnicas científicas y analíticas para recopilar, preservar, analizar y presentar evidencias digitales de manera legalmente admisible. Es fundamental para comprender cómo ocurrió un incidente, identificar al atacante y apoyar acciones legales.

4. Herramientas y tecnologías de aplicación.

Cortafuegos (Firewall)

Un sistema de seguridad de red que monitorea y controla el tráfico de red entrante y saliente basándose en un conjunto predefinido de reglas. Actúa como una barrera entre una

red de confianza y una que no lo es (como Internet).

IDS (Intrusion Detection System)

Un sistema que monitorea el tráfico de red o la actividad del sistema en busca de patrones maliciosos conocidos o comportamientos que indican una posible intrusión. Su función es alertar al personal de seguridad, pero no toma acción directa para detener el ataque.

IPS (Intrusion Prevention System)

Un sistema que, además de monitorear y alertar (como un IDS), puede tomar acciones automáticas para prevenir o bloquear un ataque en tiempo real. Puede descartar paquetes maliciosos, restablecer conexiones o bloquear tráfico de la IP de origen.

Software Antivirus

Programa diseñado para detectar, prevenir y eliminar software malicioso, incluyendo virus, gusanos y troyanos. Utiliza bases de datos de firmas de código malicioso conocido y, a menudo, heurística para identificar nuevas amenazas.

Cortafuegos basados en red

Dispositivo físico o virtual que se coloca en la periferia de una red (ejemplo: entre la red local e Internet). Protege la red en su conjunto, controlando el tráfico que entra y sale de ella.

Cortafuegos basados en host

Aplicación o software instalado directamente en un dispositivo (servidor, PC). Protege solo a ese equipo específico, controlando el tráfico que entra y sale de dicho host.

Antimalware

Término amplio que se refiere a cualquier software diseñado para prevenir, detectar y eliminar cualquier forma de malware (software malicioso). Este término es más general que antivirus e incluye protección contra ransomware, spyware, y más.

5. Normativa y buenas prácticas de uso.

Reglamento General de Protección de Datos (RGPD)

(GDPR, por sus siglas en inglés) Es el reglamento de la Unión Europea que establece el marco legal para la protección de datos personales de los ciudadanos de la UE. Impone obligaciones estrictas sobre cómo las organizaciones deben recopilar, procesar, almacenar y proteger la información personal.

ISO/IEC 27001

Es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. Ayuda a gestionar los riesgos de seguridad de la información.

Esquema Nacional de Seguridad (ENS)

Marco normativo español que establece la política de seguridad en la utilización de medios electrónicos para el sector público (administraciones) y para los proveedores que colaboren con ellas. Su objetivo es garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.

Datos sensibles

Categoría de información personal que, si se divulga, podría causar un daño significativo a la persona. Incluyen datos relacionados con el origen racial o étnico, opiniones políticas, creencias religiosas, vida sexual, datos de salud o datos biométricos. El RGPD establece una protección reforzada para estos datos.

Políticas de acceso

Normas y procedimientos que definen quién (usuarios o sistemas) puede acceder a qué recursos (datos, aplicaciones, sistemas) y bajo qué condiciones. Son un pilar fundamental del control de acceso en cualquier entorno profesional.

Diagnóstico de fallos

Proceso sistemático y técnico para identificar, analizar y determinar la causa raíz de un problema, mal funcionamiento o error en un sistema, aplicación o componente de red. Es crucial para una corrección efectiva.

Propuestas de mejora

Acciones o recomendaciones específicas, derivadas del diagnóstico de fallos o de la gestión de riesgos, destinadas a corregir deficiencias de seguridad, optimizar procesos, reducir vulnerabilidades e incrementar la eficacia del SGSI de la organización.

Registro de incidencias

Documento o base de datos que registra de manera formal y detallada todos los eventos de seguridad o incidentes ocurridos (desde la detección hasta el cierre). Es fundamental para la trazabilidad, el análisis forense, el aprendizaje y el cumplimiento normativo.