Fundamentos – Componentes de Sistemas de TI

Ciberseguridad

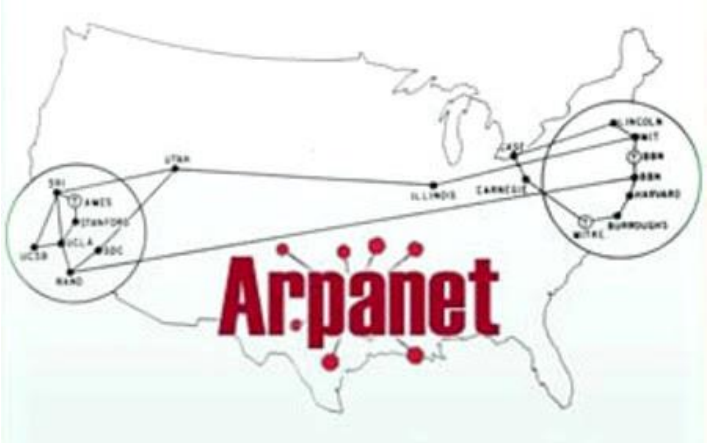
FPUNA

Seguridad en Redes de Computadoras

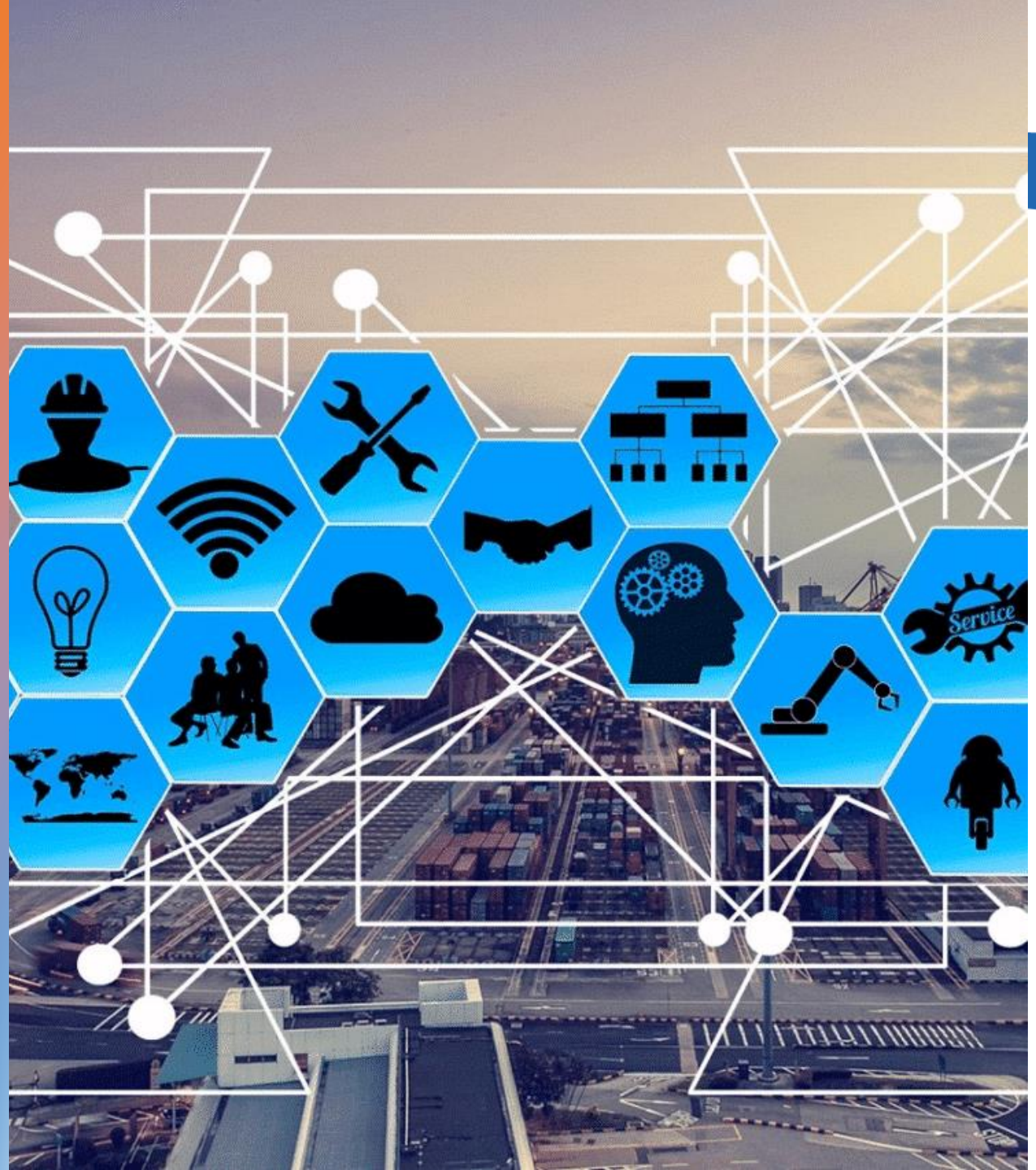
Seguridad en Redes de Computadoras

La seguridad de redes se encarga de proteger la **infraestructura**, los **recursos** y el **tráfico** de una red informática contra **intrusiones**, **accesos no autorizados**, **usos indebidos**, **modificaciones** y **denegaciones de servicio**. Su objetivo principal es mantener la **confidencialidad**, **integridad** y **disponibilidad** de la información y los sistemas que circulan por la red.

Un poco de historia



Las preocupaciones sobre la seguridad de las redes comenzaron a surgir a medida que las redes informáticas crecían en tamaño y complejidad. En la década de 1970, con el desarrollo de ARPANET, la precursora de Internet, se identificaron las primeras vulnerabilidades y se implementaron las primeras medidas de seguridad, como la autenticación de usuarios y el control de acceso.



Actualidad

En el mundo digital actual, la seguridad de redes es mucho más importante. Las redes son omnipresentes, conectando a personas, dispositivos, aplicaciones y datos en todo el planeta. Esta conectividad también crea nuevas oportunidades para los ciberatacantes, quienes utilizan métodos cada vez más sofisticados para explotar vulnerabilidades y acceder a información confidencial, interrumpir operaciones o incluso secuestrar sistemas.

Conocimientos clave para gestionar la seguridad de redes

- **Tecnologías de seguridad**
- **Arquitectura de redes**
- **Gestión de riesgos**
- **Cumplimiento normativo**
- **Buenas prácticas**

Tecnologías de seguridad

Firewalls, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), redes privadas virtuales (VPN), software antivirus y antimalware, entre otras.

Firewalls (Cortafuegos)

- Es un sistema de seguridad que controla y filtra el tráfico de red que ingresa y sale de una red protegida. Actúa como una barrera entre la red interna y el mundo exterior, como Internet, bloqueando accesos no autorizados y protegiendo los datos sensibles.

¿Cómo funcionan los firewalls?

- Los firewalls analizan cada paquete de datos que circula por la red, comparándolo con un conjunto de reglas predefinidas. Estas reglas determinan si el paquete es legítimo y se le permite continuar su camino, o si es sospechoso y debe ser bloqueado.

Tipos de Firewalls

- **Firewalls de hardware**: Son dispositivos físicos independientes que se instalan en la red. Ofrecen un alto nivel de seguridad, pero pueden ser costosos y difíciles de configurar.
- **Firewalls de software**: Son programas que se instalan en un ordenador o servidor. Son más económicos y flexibles que los firewalls de hardware, pero pueden tener un impacto en el rendimiento del sistema.
- **Firewalls de aplicaciones web**: Están diseñados para proteger aplicaciones web específicas. Filtran el tráfico web y bloquean ataques como el cross-site scripting (XSS) y la inyección de SQL (SQLi).

Beneficios de los firewalls

- **Protección contra intrusiones**: Previenen el acceso no autorizado a la red y a los datos sensibles.
- **Prevención de** ataques: Ayudan a bloquear malware, phishing, ransomware y otras amenazas.
- **Control del tráfico**: Permiten controlar qué tipo de tráfico se permite en la red.
- **Mejora del rendimiento**: Ayudan a optimizar el uso del ancho de banda de la red.

Tecnologías de seguridad

Firewalls, **sistemas de detección de intrusiones (IDS)**, sistemas de prevención de intrusiones (IPS), redes privadas virtuales (VPN), software antivirus y antimalware, entre otras.

Sistemas de Detección de Intrusiones (IDS)

- Es un dispositivo o software que monitoriza la actividad de la red y busca patrones que puedan indicar un ataque o actividad maliciosa. Cuando se detecta una actividad sospechosa, el IDS genera una alerta para que el administrador de la red pueda investigar y tomar las medidas necesarias.

Tipos de IDS

- **IDS basados en red (NIDS):** Monitorizan el tráfico de red en busca de actividades sospechosas.
- **IDS basados en host (HIDS):** Monitorizan la actividad de un solo equipo en busca de actividades sospechosas.
- **IDS basados en aplicaciones:** Monitorizan el tráfico de una aplicación específica en busca de actividades sospechosas.

¿Cómo funcionan los IDS?

Los IDS utilizan dos métodos principales para detectar intrusiones:

- **Detección basada en firmas**: Compara el tráfico de red con una base de datos de firmas conocidas de ataques.
- **Detección basada en anomalías**: Busca patrones de comportamiento que se desvían de la actividad normal de la red.

Beneficios de usar IDS

- **Detección temprana de intrusiones**: Permiten identificar ataques en sus primeras etapas, lo que facilita la respuesta y la minimización del daño.
- **Mejora de la respuesta a incidentes**: Las alertas de IDS pueden ayudar a los administradores de red a identificar la fuente del ataque y tomar las medidas necesarias para contenerlo.
- **Disuasión de ataques**: La presencia de un IDS puede disuadir a los atacantes de intentar atacar la red.

Tecnologías de seguridad

Firewalls, sistemas de detección de intrusiones (IDS), **sistemas de prevención de intrusiones (IPS)**, redes privadas virtuales (VPN), software antivirus y antimalware, entre otras.

Sistemas de prevención de intrusiones (IPS)

- Un sistema de prevención de intrusiones (IPS) es un dispositivo o software que monitoriza la actividad de la red y toma medidas automáticas para prevenir intrusiones y ataques. A diferencia de los sistemas de detección de intrusiones (IDS), que solo alertan sobre actividades sospechosas, los IPS pueden bloquear el tráfico malicioso en tiempo real.

¿Cómo funcionan los IPS?

Los IPS utilizan las mismas técnicas de detección que los IDS, como la detección basada en firmas y la detección basada en anomalías. Sin embargo, cuando se detecta una actividad sospechosa, el IPS puede tomar medidas como:

- **Bloquear el tráfico**: El IPS puede bloquear el tráfico malicioso en la capa de red o de transporte.
- **Desviar el tráfico**: El IPS puede desviar el tráfico sospechoso a un dispositivo de análisis para su inspección.
- **Generar una alerta**: El IPS puede generar una alerta para que el administrador de la red pueda investigar la actividad sospechosa.

Beneficios de usar IPS

- **Prevención proactiva de intrusiones**: Los IPS pueden bloquear ataques antes de que causen daño.
- **Reducción del tiempo de respuesta**: Los IPS pueden responder a las intrusiones de forma automática y en tiempo real.
- **Mejora de la seguridad de la red**: Los IPS pueden ayudar a proteger la red contra una amplia gama de amenazas.

Tecnologías de seguridad

Firewalls, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), **redes privadas virtuales (VPN)**, software antivirus y antimalware, entre otras.

Redes privadas virtuales (VPN)

Es una tecnología que crea una conexión segura y encriptada entre un dispositivo y una red a través de Internet. La VPN funciona como un túnel privado que permite al usuario navegar por la web de forma anónima y segura, ocultando su dirección IP y ubicación real.

Tipos de VPN

- **VPN gratuitas**: Suelen ser más lentas y tener menos opciones que las VPN de pago.
- **VPN de pago**: Ofrecen mayor velocidad, seguridad y privacidad.
- **VPN empresariales**: Diseñadas para empresas que necesitan proteger sus datos confidenciales.

Funcionamiento de la VPN

1. El usuario establece una conexión con un servidor VPN.
2. El tráfico del usuario se encripta y se envía a través del servidor VPN.
3. El servidor VPN reenvía el tráfico a Internet con una dirección IP diferente.
4. El usuario navega por Internet de forma segura y anónima.

Beneficios de usar una VPN

- **Seguridad**: La VPN encripta el tráfico del usuario, lo que lo protege de miradas indiscretas y ataques cibernéticos.
- **Privacidad**: La VPN oculta la dirección IP del usuario, lo que le permite navegar por Internet de forma anónima.
- **Acceso a contenido bloqueado**: La VPN permite al usuario acceder a contenido que está bloqueado en su región.

Tecnologías de seguridad

Firewalls, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), redes privadas virtuales (VPN), **software antivirus y antimalware**, entre otras.

Software antivirus y antimalware: Protegiendo tu equipo contra amenazas

El **antivirus** es un programa diseñado para detectar, prevenir y eliminar virus de un ordenador. Los antivirus funcionan escaneando el equipo en busca de archivos infectados y, si se encuentran, los eliminan o los ponen en cuarentena.

El **antimalware** es un programa más amplio que un antivirus, ya que puede detectar y eliminar una variedad de software malicioso, incluyendo virus, troyanos, spyware, ransomware y adware.

Diferencias entre antivirus y antimalware

- **Alcance**: El antivirus se centra principalmente en virus, mientras que el antimalware abarca una gama más amplia de amenazas.
- **Profundidad de análisis**: El antimalware suele realizar un análisis más profundo del equipo en busca de malware.
- **Protección en tiempo real**: Ambos tipos de software pueden ofrecer protección en tiempo real, que analiza los archivos y programas a medida que se ejecutan.

Beneficios de usar un software antivirus y antimalware

- Protección contra malware: Protege tu equipo contra una amplia gama de amenazas.
- Prevención de infecciones: Puede evitar que tu equipo se infecte con malware en primer lugar.
- Eliminación de malware: Puede eliminar el malware de tu equipo si ya se ha infectado.

Recomendaciones

- Se recomienda mantener actualizado el software antivirus y antimalware.
- Es importante realizar análisis regulares del equipo en busca de malware.
- Se debe tener cuidado al abrir archivos adjuntos de correo electrónico y descargar archivos de Internet.

Arquitectura de redes

- **Diseño de redes seguras**, segmentación de redes, microsegmentación.

Diseño de redes seguras

El diseño de redes seguras es una disciplina fundamental dentro de la arquitectura de redes que se enfoca en la creación de redes informáticas resistentes a **intrusiones**, **accesos no autorizados** y **ataques cibernéticos**. Su objetivo principal es proteger la información y los sistemas que circulan por la red, garantizando su **confidencialidad**, **integridad** y **disponibilidad**.

Elementos clave del diseño de redes seguras

- **Tecnologías de seguridad**: Implementación de firewalls, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), redes privadas virtuales (VPN), software antivirus y antimalware, entre otras.
- **Arquitectura de redes**: Diseño de redes segmentadas y microsegmentadas, con zonas de seguridad bien definidas para diferentes tipos de tráfico y usuarios.
- **Gestión de riesgos**: Identificación de activos, evaluación de vulnerabilidades, análisis de amenazas, gestión de incidentes y planes de respuesta.
- **Cumplimiento normativo**: Cumplimiento de leyes y regulaciones relacionadas con la seguridad de la información, como la Ley de Protección de Datos Personales.
- **Buenas prácticas**: Implementación de políticas de seguridad, procedimientos de seguridad, formación y concienciación en seguridad para usuarios.

Beneficios del diseño de redes seguras

- **Protección contra ataques:** Reduce el riesgo de intrusiones, accesos no autorizados, malware y otras amenazas.
- **Minimización de daños:** En caso de un ataque, limita el impacto y facilita la recuperación.
- **Mejora del rendimiento:** Optimiza el uso del ancho de banda y la eficiencia de la red.
- **Aumento de la confianza:** Genera confianza en los usuarios y stakeholders sobre la seguridad de la información.

Arquitectura de redes

- Diseño de redes seguras, **segmentación de redes**, microsegmentación.

Segmentación de redes: Un pilar fundamental para la seguridad

La segmentación de redes es una técnica fundamental en la arquitectura de redes que consiste en dividir una red en subredes más pequeñas y aisladas. Esta práctica permite mejorar la seguridad, el rendimiento y la escalabilidad de la red.

¿Por qué segmentar una red?

- **Seguridad:** La segmentación permite aislar dispositivos y datos sensibles, limitando el acceso a usuarios autorizados y reduciendo el riesgo de intrusiones y ataques.
- **Rendimiento:** Al dividir la red en subredes más pequeñas, se reduce el tráfico de red en cada subred, lo que mejora el rendimiento y la eficiencia.
- **Escalabilidad:** La segmentación facilita la expansión de la red al agregar nuevas subredes sin afectar al resto de la red.
- **Cumplimiento normativo:** La segmentación puede ayudar a cumplir con las normas y regulaciones relacionadas con la seguridad de la información.

Métodos de segmentación de redes

- **Segmentación por VLAN:** Se basa en la creación de redes virtuales independientes dentro de la misma infraestructura física.
- **Segmentación por firewalls:** Se utilizan firewalls para controlar el tráfico entre las diferentes subredes.
- **Segmentación por software:** Se utilizan aplicaciones de software para crear subredes virtuales.

Tipos de subredes

- **Red de acceso:** Donde se encuentran los dispositivos de los usuarios.
- **Red de distribución:** Conecta la red de acceso con la red de servidores.
- **Red de servidores:** Donde se encuentran los servidores que albergan los datos y aplicaciones.
- **Red DMZ:** Zona desmilitarizada para alojar servidores web y otros servicios que necesitan acceso desde Internet.

Beneficios de la segmentación de redes

- **Mejora la seguridad:** Reduce el riesgo de intrusiones y ataques.
- **Mejora el rendimiento:** Reduce el tráfico de red y mejora la eficiencia.
- **Facilita la gestión:** Permite administrar las subredes de forma independiente.
- **Mejora la escalabilidad:** Facilita la expansión de la red.
- **Reduce los costos:** Puede ayudar a reducir los costos de seguridad y mantenimiento.

Arquitectura de redes

- Diseño de redes seguras, segmentación de redes, **microsegmentación**.

Microsegmentación: Un enfoque granular para la seguridad de redes

- La **microsegmentación** es una técnica avanzada dentro de la arquitectura de redes que lleva la segmentación tradicional a un nivel más granular. En lugar de dividir la red en subredes amplias, la microsegmentación **crea segmentos a nivel de aplicación o servicio**, proporcionando un control más preciso sobre el acceso a los recursos de la red.

¿Por qué usar la microsegmentación?

- **Mejora la seguridad:** Permite un control más granular del acceso a los recursos, lo que reduce el riesgo de intrusiones y ataques.
- **Minimiza el impacto de las intrusiones:** Si un segmento se ve comprometido, el impacto se limita a ese segmento, protegiendo el resto de la red.
- **Aumenta la flexibilidad:** Permite adaptar la seguridad a las necesidades específicas de cada aplicación o servicio.
- **Facilita la gestión:** Simplifica la administración de la seguridad al centralizar las políticas de acceso.

Métodos de microsegmentación

- **Firewalls de aplicaciones web (WAF):** Protegen las aplicaciones web de ataques comunes.
- **Redes de superposición privadas virtuales (VXLAN):** Permiten crear segmentos virtuales independientes dentro de la misma infraestructura física.
- **Software Defined Networking (SDN):** Permite controlar el tráfico de red de forma centralizada y programática.

Beneficios de la microsegmentación

- **Mayor seguridad:** Reduce significativamente el riesgo de intrusiones y ataques.
- **Menor impacto de las intrusiones:** Limita el daño en caso de un ataque.
- **Mayor flexibilidad:** Permite adaptar la seguridad a las necesidades específicas.
- **Gestión simplificada:** Centraliza las políticas de acceso y facilita la administración.
- **Mejora del cumplimiento:** Facilita el cumplimiento de las normas y regulaciones.

Gestión de riesgos

- **Identificación de activos**, evaluación de vulnerabilidades, análisis de amenazas, gestión de incidentes.

Identificación de activos: El primer paso para la seguridad

- La **identificación de activos** es un proceso fundamental dentro de la **gestión de riesgos en redes**. Consiste en **identificar, clasificar y valorar todos los recursos informáticos** de una organización, incluyendo hardware, software, datos, aplicaciones y servicios.

¿Por qué es importante la identificación de activos?

- Permite conocer los activos que se necesitan proteger.
- Ayuda a comprender el valor de los activos y el impacto que tendría su pérdida.
- Facilita la evaluación de los riesgos a los que están expuestos los activos.
- Permite la implementación de medidas de seguridad adecuadas para proteger los activos.

¿Cómo se realiza la identificación de activos?

- **Inventariado:** Se realiza un inventario de todos los recursos informáticos de la organización.
- **Clasificación:** Se clasifican los activos según su tipo, valor, criticidad y ubicación.
- **Valoración:** Se determina el valor de cada activo, considerando su impacto en el negocio.

Metodologías para la identificación de activos

- **Manual:** Se realiza un inventario manual de los activos.
- **Automatizada:** Se utilizan herramientas de software para automatizar el proceso de inventario.

Beneficios de la identificación de activos

- **Mejora la seguridad:** Permite la implementación de medidas de seguridad más precisas.
- **Reduce los costos:** Permite optimizar la inversión en seguridad.
- **Mejora la toma de decisiones:** Facilita la toma de decisiones estratégicas sobre la seguridad de la información.
- **Mejora el cumplimiento:** Facilita el cumplimiento de las normas y regulaciones.

Gestión de riesgos

- Identificación de activos, **evaluación de vulnerabilidades**, análisis de amenazas, gestión de incidentes.

Evaluación de vulnerabilidades: Un paso crucial para la seguridad

La **evaluación de vulnerabilidades** es un proceso fundamental dentro de la **gestión de riesgos en redes**. Consiste en **identificar, clasificar y evaluar las debilidades de seguridad** en los sistemas informáticos de una organización.

¿Por qué es importante la evaluación de vulnerabilidades?

- Permite conocer las vulnerabilidades que pueden ser explotadas por los atacantes.
- Ayuda a comprender el impacto que tendría un ataque exitoso.
- Facilita la priorización de las medidas de seguridad que deben implementarse.

¿Cómo se realiza la evaluación de vulnerabilidades?

- **Análisis manual:** Se realiza un análisis manual de los sistemas informáticos para identificar vulnerabilidades.
- **Análisis automatizado:** Se utilizan herramientas de software para automatizar el proceso de identificación de vulnerabilidades.

Tipos de análisis de vulnerabilidades

- **Análisis de red:** Se analiza la red para identificar vulnerabilidades en los dispositivos y servicios de red.
- **Análisis de aplicaciones:** Se analizan las aplicaciones para identificar vulnerabilidades en el código fuente o en la configuración.
- **Análisis de sistemas operativos:** Se analiza el sistema operativo para identificar vulnerabilidades en el software o en la configuración.

Beneficios de la evaluación de vulnerabilidades

- **Mejora la seguridad:** Permite la implementación de medidas de seguridad para mitigar las vulnerabilidades.
- **Reduce los costos:** Permite evitar los costos asociados a un ataque exitoso.
- **Mejora la toma de decisiones:** Facilita la toma de decisiones estratégicas sobre la seguridad de la información.
- **Mejora el cumplimiento:** Facilita el cumplimiento de las normas y regulaciones.

Gestión de riesgos

- Identificación de activos, evaluación de vulnerabilidades, **análisis de amenazas**, gestión de incidentes.

Análisis de amenazas: Anticipando los peligros en la red

- El **análisis de amenazas** es un proceso fundamental dentro de la **gestión de riesgos en redes**. Consiste en **identificar, clasificar y evaluar las amenazas** a las que están expuestos los sistemas informáticos de una organización.

¿Por qué es importante el análisis de amenazas?

- Permite conocer las amenazas que pueden afectar a la organización.
- Ayuda a comprender el impacto que tendría una amenaza exitosa.
- Facilita la priorización de las medidas de seguridad que deben implementarse.

¿Cómo se realiza el análisis de amenazas?

- **Recopilación de información:** Se recopila información sobre las amenazas existentes, incluyendo su tipología, objetivos y métodos de ataque.
- **Análisis de la información:** Se analiza la información recopilada para identificar las amenazas más relevantes para la organización.
- **Evaluación de las amenazas:** Se evalúa el impacto que tendría una amenaza exitosa en la organización.

Tipos de amenazas

- **Amenazas externas:** Amenazas que provienen de fuera de la organización, como ataques cibernéticos, malware y phishing.
- **Amenazas internas:** Amenazas que provienen de dentro de la organización, como errores humanos, robo de información y sabotaje.

Beneficios del análisis de amenazas

- **Mejora la seguridad:** Permite la implementación de medidas de seguridad para prevenir o mitigar las amenazas.
- **Reduce los costos:** Permite evitar los costos asociados a un ataque exitoso.
- **Mejora la toma de decisiones:** Facilita la toma de decisiones estratégicas sobre la seguridad de la información.
- **Mejora el cumplimiento:** Facilita el cumplimiento de las normas y regulaciones.

Gestión de riesgos

- Identificación de activos, evaluación de vulnerabilidades, análisis de amenazas, **gestión de incidentes**.

Gestión de incidentes: Respuesta rápida y efectiva ante las amenazas

- La **gestión de incidentes** es un proceso fundamental dentro de la **gestión de riesgos en redes**. Se enfoca en la **detección**, **análisis**, **respuesta y recuperación de incidentes de seguridad** que puedan afectar a los sistemas informáticos de una organización.

¿Por qué es importante la gestión de incidentes?

- **Minimiza el impacto de los incidentes:** Permite una respuesta rápida y efectiva a los incidentes, lo que reduce el daño potencial.
- **Mejora la capacidad de recuperación:** Facilita la recuperación de la organización después de un incidente.
- **Ayuda a prevenir futuros incidentes:** Permite aprender de los incidentes pasados y tomar medidas para prevenir su recurrencia.

¿Cómo se realiza la gestión de incidentes?

- **Preparación:** Se define un plan de respuesta a incidentes que incluye roles, responsabilidades y procedimientos.
- **Detección:** Se implementan mecanismos para detectar incidentes de manera temprana.
- **Análisis:** Se analiza el incidente para determinar su alcance, impacto y causa.
- **Respuesta:** Se toman las medidas necesarias para contener el incidente y restaurar los sistemas afectados.
- **Recuperación:** Se restablecen los sistemas a su estado normal y se toman medidas para prevenir futuros incidentes.

Tipos de incidentes

- **Incidentes de seguridad:** Ataques cibernéticos, malware, phishing, etc.
- **Incidentes técnicos:** Fallas de hardware, errores de software, etc.
- **Incidentes humanos:** Errores humanos, negligencia, etc.

Beneficios de la gestión de incidentes

- **Reduce los costos:** Minimiza el impacto financiero de los incidentes.
- **Mejora la imagen de la organización:** Demuestra que la organización está preparada para enfrentar los incidentes de manera efectiva.
- **Mejora la confianza de los clientes y partners:** Demuestra que la organización es un entorno seguro para hacer negocios.
- **Mejora el cumplimiento:** Facilita el cumplimiento de las normas y regulaciones.

Cumplimiento normativo

- Leyes y regulaciones relacionadas con la seguridad de la información, como la Ley de Protección de Datos Personales.

Buenas prácticas

- Políticas de seguridad, procedimientos de seguridad, formación y concienciación en seguridad para usuarios.