ÁREA 3. DESARROLLO DE SOFTWARE DE APLICACIÓN

SUBÁREA 3.4 SEGURIDAD INFORMÁTICA

TEMAS IMPORTANTE:

**Definición de Seguridad Informática:**

**Amenazas y vulnerabilidades:**

Las amenazas y vulnerabilidades son dos conceptos relacionados con la seguridad informática y es importante entender la diferencia entre ellos para poder proteger adecuadamente los sistemas y datos.

* Amenazas: se refieren a los posibles riesgos o peligros que pueden afectar a los sistemas y datos. Las amenazas pueden provenir de diversas fuentes, incluyendo hackers malintencionados, virus y malware, desastres naturales, errores humanos, entre otros.
* Vulnerabilidades: se refieren a las debilidades en los sistemas y aplicaciones que pueden ser explotadas por los atacantes para acceder a los datos o sistemas. Las vulnerabilidades pueden ser de diversas formas, como errores de software, configuraciones inadecuadas, falta de actualizaciones, entre otras.

Es importante destacar que una vulnerabilidad en sí misma no representa una amenaza. Una vulnerabilidad es solo una debilidad potencial en el sistema que podría ser explotada para causar daño o comprometer la seguridad. Para que una vulnerabilidad se convierta en una amenaza real, un atacante tendría que explotarla para acceder a los sistemas o datos.

**¿Qué es un activo informático y su clasificación?**

Un activo informático es cualquier elemento o recurso que tenga un valor para la organización en términos de información y/o funcionalidad. Los activos informáticos son una parte importante de la infraestructura tecnológica de una organización y su gestión y protección es esencial para mantener la seguridad informática.

Los activos informáticos se pueden clasificar en tres categorías principales:

* Hardware: se refiere a los componentes físicos de los sistemas informáticos, como computadoras, servidores, routers, dispositivos móviles, impresoras, entre otros.
* Software: se refiere a los programas y aplicaciones informáticas que se utilizan en los sistemas informáticos, como sistemas operativos, software de productividad, software de seguridad, entre otros.
* Datos: se refiere a la información almacenada en los sistemas informáticos, como archivos de texto, imágenes, videos, bases de datos, correos electrónicos, entre otros.

Es importante destacar que cada categoría de activos informáticos puede tener diferentes subcategorías y clasificaciones específicas según las necesidades y características de la organización. Por ejemplo, dentro de la categoría de hardware, se pueden distinguir servidores web, dispositivos de almacenamiento, dispositivos de red, entre otros. La clasificación de los activos informáticos es esencial para una adecuada gestión de la seguridad informática, ya que permite una mejor identificación y protección de los activos críticos y valiosos para la organización.

**Análisis de riesgos**

El análisis de riesgos es un proceso que tiene como objetivo identificar, evaluar y priorizar los riesgos asociados a los sistemas informáticos y a la información que se maneja en una organización. Este proceso es fundamental para la gestión de la seguridad informática, ya que permite conocer los posibles riesgos a los que está expuesta la organización y establecer medidas preventivas y de mitigación para reducir el impacto de los riesgos identificados.

El análisis de riesgos generalmente se lleva a cabo en tres fases:

1. Identificación de riesgos: se trata de un proceso de recopilación de información para identificar los posibles riesgos a los que está expuesta la organización. En esta fase se pueden utilizar diversas técnicas, como entrevistas, cuestionarios, revisión de políticas y procedimientos, entre otras.
2. Evaluación de riesgos: en esta fase se analiza el impacto y la probabilidad de cada riesgo identificado para determinar su nivel de riesgo. El impacto se refiere a las consecuencias que tendría la materialización del riesgo en términos de daño a los activos informáticos y la información, mientras que la probabilidad se refiere a la posibilidad de que se materialice el riesgo. Para la evaluación de riesgos se pueden utilizar diferentes métodos, como el análisis cuantitativo o cualitativo.
3. Tratamiento de riesgos: en esta fase se determinan las medidas a tomar para reducir el impacto y la probabilidad de los riesgos identificados. Estas medidas pueden ser preventivas, como controles de seguridad y políticas de seguridad, o de mitigación, como planes de contingencia y recuperación ante desastres.

**Identificar vulnerabilidades y amenazas, diferencia entre vulnerabilidad y amenaza**

Identificar vulnerabilidades y amenazas es un paso importante en la gestión de la seguridad informática, ya que permite conocer los posibles puntos débiles en los sistemas informáticos y los riesgos a los que están expuestos.

Una vulnerabilidad es una debilidad o fallo en los sistemas informáticos que puede ser explotado por un atacante para comprometer la seguridad de la información o los activos informáticos de una organización. Las vulnerabilidades pueden estar relacionadas con los sistemas operativos, las aplicaciones informáticas, las redes, los dispositivos móviles, entre otros. Por ejemplo, una vulnerabilidad podría ser una contraseña débil que permita a un atacante acceder a una cuenta de usuario sin autorización.

Por otro lado, una amenaza es cualquier factor externo o interno que pueda aprovechar una vulnerabilidad para causar daño a los sistemas informáticos o a la información. Las amenazas pueden ser intencionales o no intencionales, y pueden provenir de personas, programas maliciosos, desastres naturales, entre otros. Por ejemplo, una amenaza podría ser un ataque de phishing que utiliza una vulnerabilidad en un software de correo electrónico para engañar a un usuario y obtener acceso a su información confidencial.

Es importante destacar que, aunque las vulnerabilidades y las amenazas están estrechamente relacionadas, son conceptos diferentes. Las vulnerabilidades son debilidades o fallos en los sistemas informáticos que pueden ser explotados, mientras que las amenazas son factores externos o internos que pueden aprovechar esas vulnerabilidades para causar daño. Por lo tanto, identificar tanto las vulnerabilidades como las amenazas es esencial para la gestión de la seguridad informática y para la implementación de medidas preventivas y de mitigación.

**Evaluación del riesgo (impacto – probabilidad)**La evaluación del riesgo es una parte importante del proceso de gestión de la seguridad informática y consiste en determinar la probabilidad y el impacto de la materialización de un riesgo. La probabilidad se refiere a la posibilidad de que ocurra un evento, mientras que el impacto se refiere a las consecuencias que tendría ese evento en caso de ocurrir.

La evaluación del riesgo se puede realizar utilizando diferentes enfoques, como el análisis cuantitativo o cualitativo. En el análisis cuantitativo, se utiliza información numérica para evaluar el impacto y la probabilidad del riesgo. Por ejemplo, se pueden utilizar estadísticas históricas para determinar la probabilidad de un evento y se pueden calcular los costos asociados para evaluar el impacto. En el análisis cualitativo, se utiliza información subjetiva para evaluar el impacto y la probabilidad del riesgo. Por ejemplo, se pueden utilizar encuestas o juicios de expertos para determinar el impacto y la probabilidad.

Para evaluar el riesgo utilizando el enfoque de impacto-probabilidad, se puede utilizar una matriz de riesgo que relaciona el impacto y la probabilidad de un evento con una clasificación de riesgo. Por ejemplo, se puede utilizar una escala del 1 al 5 para evaluar el impacto y la probabilidad, donde 1 representa un impacto o probabilidad muy baja y 5 representa un impacto o probabilidad muy alta. Luego, se pueden asignar diferentes clasificaciones de riesgo según los valores obtenidos en la matriz, por ejemplo, alto, medio o bajo riesgo.

La evaluación del riesgo permite identificar los riesgos más críticos para la organización y determinar las medidas de seguridad necesarias para mitigar o reducir el impacto de los riesgos identificados. También es importante realizar una evaluación del riesgo de forma periódica, ya que los riesgos pueden cambiar con el tiempo debido a cambios en los sistemas informáticos, las amenazas y las vulnerabilidades.

**Amenazas y vulnerabilidades:**

**Tipos de amenazas**

Hay una amplia gama de amenazas que pueden comprometer la seguridad informática de una organización. Algunos de los tipos de amenazas más comunes incluyen:

* Malware: cualquier tipo de software malicioso que se instala en un sistema informático sin el conocimiento o consentimiento del usuario. El malware puede incluir virus, troyanos, gusanos, spyware y ransomware, entre otros.
* Ataques de phishing: un intento de engañar a un usuario para que revele información confidencial, como contraseñas o información bancaria, a través de correos electrónicos, mensajes de texto u otras formas de comunicación.
* Ataques de fuerza bruta: un intento de adivinar una contraseña o una clave de cifrado probando repetidamente diferentes combinaciones de contraseñas hasta que se encuentra la correcta.
* Ataques de denegación de servicio (DoS): un intento de inundar un sistema informático con tráfico malicioso para que el sistema no pueda procesar solicitudes legítimas.
* Robo de identidad: un intento de obtener información personal de una persona, como nombre, fecha de nacimiento, número de Seguro Social, para hacerse pasar por esa persona y obtener acceso no autorizado a sus cuentas.

Por otro lado, las vulnerabilidades son debilidades o fallas en los sistemas informáticos que pueden ser explotados por un atacante para comprometer la seguridad de la información o los activos informáticos de una organización. Algunos ejemplos de vulnerabilidades incluyen:

* Contraseñas débiles o fáciles de adivinar.
* Sistemas operativos o aplicaciones desactualizados
* Configuraciones incorrectas de seguridad en los sistemas informáticos.
* Falta de parches de seguridad o actualizaciones de software.
* Sistemas con permisos de acceso incorrectos o excesivos.

**Medidas para contrarrestar amenazas, plan de respuesta a riesgos:**

Para contrarrestar las amenazas y reducir los riesgos en la seguridad informática, es importante implementar una serie de medidas de seguridad y un plan de respuesta a riesgos. Algunas medidas de seguridad que se pueden implementar incluyen:

* Actualización de software: mantener todos los sistemas y aplicaciones informáticas actualizadas para evitar vulnerabilidades conocidas.
* Uso de contraseñas seguras: implementar políticas de contraseñas fuertes y alentar a los usuarios a actualizar sus contraseñas regularmente.
* Control de acceso: implementar sistemas de control de acceso, que limitan los permisos de los usuarios y restringen el acceso a información confidencial.
* Seguridad física: asegurar los equipos informáticos y servidores en un lugar físicamente seguro, controlar el acceso a la red, y mantener los equipos bajo llave.
* Entrenamiento de los usuarios: proporcionar a los usuarios una formación adecuada en seguridad informática para que puedan identificar y evitar amenazas comunes, como los ataques de phishing.

Además de implementar medidas de seguridad, es importante tener un plan de respuesta a riesgos. Un plan de respuesta a riesgos es un conjunto de procedimientos para responder a incidentes de seguridad, como un ataque de malware o una brecha de seguridad. Algunas de las características clave de un plan de respuesta a riesgos son:

* Definición de roles y responsabilidades: definir claramente quién es responsable de qué en la respuesta a incidentes de seguridad.
* Procedimientos de notificación: establecer un protocolo claro para notificar a las partes pertinentes en caso de un incidente de seguridad.
* Evaluación de riesgos: determinar el impacto y la probabilidad del incidente y la mejor forma de abordarlo.
* Procedimientos de recuperación: desarrollar un plan para restaurar los sistemas informáticos y la información a un estado seguro después de un incidente de seguridad.
* Documentación y evaluación: documentar el incidente de seguridad y las respuestas tomadas para poder evaluar el éxito del plan de respuesta y hacer mejoras para el futuro.

Un plan de respuesta a riesgos puede ayudar a minimizar el impacto de un incidente de seguridad y asegurar la continuidad del negocio en caso de un incidente.

**Controles de acceso**Los controles de acceso son medidas de seguridad que se utilizan para proteger los sistemas informáticos y los datos sensibles de acceso no autorizado. Estos controles pueden incluir medidas físicas, técnicas y administrativas.

Algunos ejemplos de controles de acceso incluyen:

* Contraseñas seguras: implementar políticas de contraseñas fuertes y alentar a los usuarios a actualizar sus contraseñas regularmente.
* Autenticación multifactorial: requerir múltiples factores para verificar la identidad del usuario, como una contraseña y un código de autenticación enviado a su teléfono móvil.
* Control de acceso basado en roles: restringir el acceso a la información confidencial y los sistemas críticos a solo aquellos usuarios que tienen una necesidad legítima de acceder a ellos, según su función en la organización.
* Monitoreo de acceso: monitorear y registrar el acceso a los sistemas y la información, para detectar y responder a intentos de acceso no autorizados.
* Controles físicos: proteger el acceso físico a los sistemas y la información, utilizando medidas como cerraduras, alarmas y sistemas de videovigilancia.

**Mecanismos de seguridad para proteger la información:**

Existen varios mecanismos de seguridad que se pueden utilizar para proteger la información en diferentes entornos. A continuación se describen algunos mecanismos comunes de seguridad para proteger la información en sistemas web, plataformas móviles y redes de computadoras.

Sistemas web:

* Certificados SSL/TLS: utilizados para asegurar la comunicación entre el navegador web y el servidor mediante la encriptación de la información transmitida.
* Firewalls de aplicaciones web (WAF): se utilizan para proteger las aplicaciones web contra ataques comunes, como inyección de SQL, cross-site scripting (XSS) y cross-site request forgery (CSRF).
* Autenticación y control de acceso: se utilizan para garantizar que solo los usuarios autorizados tengan acceso a la información.
* Gestión de sesiones: se utilizan para asegurar que los usuarios estén autenticados en todo momento y que sus sesiones estén protegidas.

Plataformas móviles:

* Seguridad de la plataforma: se utilizan mecanismos de seguridad integrados en la plataforma, como el cifrado de almacenamiento y la autenticación de dispositivos.
* Actualizaciones regulares de software: se asegura de mantener el sistema operativo y las aplicaciones actualizadas para evitar vulnerabilidades conocidas.
* Controles de acceso: se utilizan mecanismos de autenticación y control de acceso para garantizar que solo los usuarios autorizados tengan acceso a la información.
* Protección de datos: se utilizan técnicas de cifrado para proteger los datos sensibles almacenados en el dispositivo.

Redes de computadoras:

* Firewalls de red: se utilizan para proteger la red de computadoras contra ataques externos y limitar el tráfico entrante y saliente.
* Detección de intrusiones (IDS) y prevención de intrusiones (IPS): se utilizan para detectar y responder a intentos de intrusión en la red.
* Red privada virtual (VPN): se utiliza para encriptar el tráfico de la red y proteger la información transmitida a través de Internet.
* Autenticación y control de acceso: se utilizan para garantizar que solo los usuarios autorizados tengan acceso a la red y a la información.

**Criptografía:**

**Definición, historia y categorización**

La criptografía es la disciplina que se encarga del estudio de técnicas y algoritmos matemáticos para garantizar la confidencialidad, integridad y autenticidad de la información en sistemas de comunicación. Esta disciplina tiene una larga historia que se remonta a la antigüedad, cuando se utilizaban técnicas simples de cifrado para proteger la información de posibles adversarios

La criptografía moderna se desarrolló en el siglo XX con la llegada de la tecnología digital y las computadoras. Se comenzaron a desarrollar algoritmos más complejos que permitían una mayor seguridad y rapidez en la encriptación y descifrado de información.

La criptografía se puede categorizar en dos ramas principales: la criptografía simétrica y la criptografía asimétrica.

* Criptografía simétrica: También conocida como cifrado de clave secreta, es una técnica de cifrado en la que se utiliza una misma clave para encriptar y descifrar la información. La seguridad de este método radica en la protección de la clave utilizada. Los algoritmos más comunes de criptografía simétrica son AES (Advanced Encryption Standard) y DES (Data Encryption Standard).
* Criptografía asimétrica: También conocida como cifrado de clave pública, es una técnica de cifrado en la que se utilizan dos claves diferentes, una pública y otra privada. La clave pública se utiliza para encriptar la información y la clave privada se utiliza para descifrarla. Este método garantiza una mayor seguridad, ya que la clave privada no se comparte y solo el destinatario tiene acceso a ella. El algoritmo más común de criptografía asimétrica es RSA (Rivest-Shamir-Adleman).

Además de estas dos ramas principales, existen otras técnicas de criptografía, como la criptografía hash, que se utiliza para garantizar la integridad de la información y la autenticación de mensajes, y la criptografía cuántica, que utiliza principios de la física cuántica para garantizar la seguridad de la información.

**• Algoritmos de cifrado simétrico**

**o Ventajas, en qué escenarios conviene utilizarse.**

Los algoritmos de cifrado simétrico, también conocidos como cifrado de clave secreta, son técnicas de cifrado en las que se utiliza una misma clave para encriptar y descifrar la información. Algunos de los algoritmos de cifrado simétrico más utilizados son:

* AES (Advanced Encryption Standard): Es un algoritmo de cifrado simétrico ampliamente utilizado en la actualidad. Fue adoptado como el estándar de cifrado del gobierno de los Estados Unidos en 2001 y es considerado uno de los algoritmos de cifrado más seguros.
* DES (Data Encryption Standard): Es uno de los algoritmos de cifrado simétrico más antiguos, desarrollado en los años 70. Aunque ha sido desplazado por algoritmos más modernos como AES, sigue siendo utilizado en algunos sistemas legados.

Las ventajas de utilizar algoritmos de cifrado simétrico son:

* Mayor velocidad: Los algoritmos de cifrado simétrico son más rápidos que los algoritmos de cifrado asimétrico, ya que solo se necesita una clave para encriptar y descifrar la información.
* Eficiencia en el uso de recursos: Los algoritmos de cifrado simétrico son más eficientes en el uso de recursos que los algoritmos de cifrado asimétrico, lo que los hace ideales para su uso en sistemas con recursos limitados.
* Mayor facilidad de implementación: Los algoritmos de cifrado simétrico son más fáciles de implementar que los algoritmos de cifrado asimétrico, lo que los hace ideales para su uso en sistemas con restricciones de tiempo y presupuesto.

Los algoritmos de cifrado simétrico son adecuados para su uso en escenarios en los que la velocidad y la eficiencia son importantes, como el cifrado de grandes volúmenes de datos en sistemas de almacenamiento y transmisión de datos en línea, el cifrado de contraseñas y credenciales, y el cifrado de archivos locales en sistemas operativos. Sin embargo, su principal desventaja es la necesidad de compartir la clave de cifrado con las partes autorizadas, lo que puede aumentar el riesgo de que la clave sea comprometida y la información sea accesible para los atacantes. Por esta razón, los algoritmos de cifrado simétrico no son adecuados para todos los escenarios y se debe evaluar cuidadosamente la seguridad de la clave utilizada y las posibles amenazas a la seguridad antes de utilizarlos.

**• Algoritmos de cifrado asimétrico**

**o Ventajas, en qué escenarios conviene utilizarse.**

Los algoritmos de cifrado asimétrico, también conocidos como cifrado de clave pública, son técnicas de cifrado que utilizan dos claves diferentes para encriptar y descifrar la información. Cada usuario tiene una clave pública y una clave privada. Algunos de los algoritmos de cifrado asimétrico más utilizados son:

* RSA: Es uno de los algoritmos de cifrado asimétrico más conocidos. Fue desarrollado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977.
* ElGamal: Es un algoritmo de cifrado asimétrico desarrollado por Taher Elgamal en 1985. Es utilizado en algunos sistemas de correo electrónico y en sistemas de cifrado de archivos.

Las ventajas de utilizar algoritmos de cifrado asimétrico son:

* Mayor seguridad: Los algoritmos de cifrado asimétrico ofrecen una mayor seguridad que los algoritmos de cifrado simétrico, ya que las claves de encriptación y descifrado son diferentes.
* No es necesario compartir la clave: Como cada usuario tiene su propia clave pública y privada, no es necesario compartir la clave de encriptación y descifrado, lo que aumenta la seguridad del sistema.
* Firma digital: Los algoritmos de cifrado asimétrico permiten la creación de firmas digitales, que son útiles para verificar la autenticidad de un mensaje o documento.

Los algoritmos de cifrado asimétrico son adecuados para su uso en escenarios en los que se requiere una mayor seguridad, como en la transmisión de información confidencial, en la autenticación de usuarios y en la firma digital de documentos. Además, son particularmente útiles en situaciones en las que no se puede confiar en que las claves se mantengan seguras, ya que no es necesario compartir la clave de cifrado y descifrado. Sin embargo, los algoritmos de cifrado asimétrico son más lentos y requieren más recursos que los algoritmos de cifrado simétrico, por lo que no son adecuados para su uso en sistemas que requieren una alta velocidad o eficiencia. Además, el cifrado asimétrico es menos resistente a ataques de fuerza bruta que el cifrado simétrico.

• **Autenticación y firmas digitales**

La autenticación y las firmas digitales son dos técnicas de seguridad importantes en la protección de la información digital. A continuación, se explican brevemente ambos conceptos:

* Autenticación: Es el proceso de verificar la identidad de un usuario o dispositivo para garantizar que tiene acceso autorizado a un sistema o recurso. La autenticación se realiza mediante el uso de credenciales de autenticación, como contraseñas, tarjetas inteligentes o huellas dactilares. La autenticación puede ser de varios tipos, como la autenticación de contraseña, la autenticación de dos factores o la autenticación de múltiples factores. La autenticación es importante en la prevención de accesos no autorizados a la información digital.
* Firmas digitales: Son técnicas que permiten verificar la integridad y autenticidad de un documento digital. Una firma digital es un conjunto de datos criptográficos que se adjuntan a un documento digital y que se utilizan para verificar que el documento no ha sido modificado desde su creación y que proviene de la persona que lo firmó. Las firmas digitales son importantes en la prevención de la falsificación de documentos digitales y en la protección de la propiedad intelectual.

En ambos casos, se utilizan técnicas criptográficas, como el cifrado de clave pública, para garantizar la seguridad de la información. Los algoritmos de cifrado asimétrico se utilizan para generar claves únicas para cada usuario y para asegurar que los datos transmitidos no puedan ser interceptados y leídos por terceros no autorizados.

La autenticación y las firmas digitales se utilizan en una amplia variedad de aplicaciones, desde el inicio de sesión en sistemas informáticos y el acceso a sitios web hasta la firma de contratos y la transmisión de información confidencial. La seguridad de la información se ha convertido en un tema cada vez más importante en la era digital, y la autenticación y las firmas digitales son herramientas valiosas para garantizar la seguridad y la privacidad de la información.