Universidad del Caribe

2000 CANCUN, QUINTANA ROO, MÉXICO

CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

Alumno: Abdiel Gabriel Hau Tun

Matricula: 200300588

Docente: Ismael Jiménez Sánchez

Carrera: Ingeniería en Datos e Inteligencia Organizacional.

Materia: Seguridad de Datos

26/01/2023

Conceptos Básicos de Ciberseguridad

- **CIA TRIAD**

La tríada de la CIA se refiere a confidencialidad, integridad y disponibilidad, y describe un modelo diseñado para guiar las políticas de seguridad de la información (infosec) dentro de una organización. A veces se hace referencia al modelo como la tríada AIC (que significa disponibilidad, integridad y confidencialidad) para evitar confusión con la Agencia Central de Inteligencia.

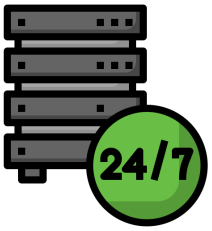
1.- **Confidencialidad.** Aproximadamente equivalentes a la privacidad, las medidas de confidencialidad están diseñadas para evitar intentos de acceso no autorizados a la información confidencial. Es común que los datos se clasifiquen según la cantidad y el tipo de daño que podrían causar si cayeran en las manos equivocadas. De acuerdo con esas categorías, se pueden implementar medidas de seguridad de datos más o menos estrictas.

2.- Integridad. La coherencia, precisión y confiabilidad de los datos deben mantenerse durante todo su ciclo de vida. Los datos no deben modificarse en tránsito y se deben tomar medidas para garantizar que personas no autorizadas no puedan modificarlos, por ejemplo, en violaciones de datos.

3.- Disponibilidad. La información debe ser consistente y fácilmente accesible para las partes autorizadas. Esto implica mantener adecuadamente el hardware y la infraestructura técnica y los sistemas que contienen y muestran la información.

¿Por qué es importante la tríada de la CIA?

La consideración conjunta de estos tres principios dentro del marco de la tríada guía el desarrollo de políticas de seguridad para las organizaciones. Al evaluar las necesidades y los casos de uso de posibles nuevos productos y tecnologías, la tríada ayuda a las organizaciones a formular preguntas específicas sobre cómo se proporciona valor en esas tres áreas clave.



- **Usability triangle**

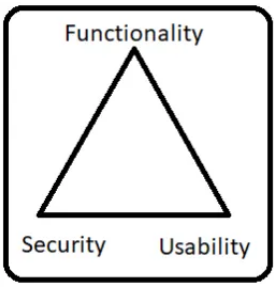
Existe una interdependencia entre estos tres atributos. Cuando la seguridad aumenta, la usabilidad y la funcionalidad disminuyen. Cualquier organización debe equilibrar estas tres cualidades para llegar a un sistema de información equilibrado.

El triángulo de usabilidad, también conocido como triángulo de seguridad-funcionalidad-usabilidad, es un marco utilizado en el diseño y desarrollo de sistemas para representar el equilibrio, a menudo difícil, entre tres atributos clave:

Seguridad: La capacidad de un sistema para resistir el acceso no autorizado, la modificación o la destrucción de sus datos y funcionalidad.

Funcionalidad: Las características y capacidades que ofrece el sistema, satisfaciendo las necesidades previstas de sus usuarios.

Usabilidad: la facilidad con la que los usuarios pueden aprender, navegar e interactuar con el sistema para lograr sus objetivos.



- **Riesgo**

Un riesgo de ciberseguridad son las probabilidades de que una amenaza se materialice y tu información, datos personales o el acceso a tus cuentas bancarias queden expuestas o sean modificadas por delincuentes.

La ciberseguridad busca gestionar y mitigar estos riesgos a través de prácticas como el uso de firewalls, antivirus, actualizaciones de software, políticas de acceso, cifrado, entre otras medidas. La comprensión y gestión efectiva del riesgo son fundamentales para proteger la integridad, confidencialidad y disponibilidad de los activos digitales.

- **MFA**

La autenticación multifactor (multi factor authentication o MFA) es una tecnología de seguridad que requiere múltiples métodos de autenticación de categorías independientes de credenciales para verificar la identidad de un usuario para un inicio de sesión u otra transacción.

La autenticación multifactor combina dos o más credenciales independientes: lo que el usuario sabe, cómo una contraseña; lo que tiene el usuario, como un token de seguridad; y qué es el usuario, mediante el uso de métodos de verificación biométrica.

El objetivo de MFA es crear una defensa en capas que dificulte que una persona no autorizada acceda a un objetivo, como una ubicación física, un dispositivo informático, una red o una base de datos. Si un factor se ve comprometido o roto, el atacante todavía tiene al menos una o más barreras que romper antes de entrar con éxito en el objetivo.

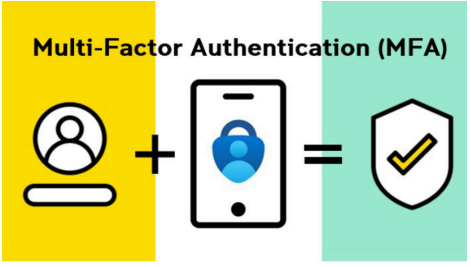
Métodos de autenticación MFA

Factor de conocimiento. La autenticación basada en el conocimiento generalmente requiere que el usuario responda una pregunta de seguridad personal. Las tecnologías de factores de conocimiento generalmente incluyen contraseñas, números de identificación personal (PIN) de cuatro dígitos y contraseñas de un solo uso (OTP).

Factor de posesión. Los usuarios deben tener algo específico en su poder para iniciar sesión, como una insignia, un token, un llavero o una tarjeta de módulo de identidad de suscriptor (SIM) de teléfono. Para la autenticación móvil, un teléfono inteligente a menudo proporciona el factor de posesión junto con una aplicación OTP.

Factor de herencia. Cualquier rasgo biológico que tenga el usuario que esté confirmado para iniciar sesión.

La autenticación multifactor se introdujo para fortalecer el acceso de seguridad a sistemas y aplicaciones a través de hardware y software. El objetivo era autenticar la identidad de los usuarios y asegurar la integridad de sus transacciones digitales. La desventaja de MFA es que los usuarios a menudo olvidan las respuestas a las preguntas personales que verifican su identidad, y algunos usuarios comparten tokens de identificación personal y contraseñas. MFA tiene otros beneficios y desventajas.



- **Vulnerabilidad.**

Una vulnerabilidad se refiere a una debilidad en un sistema que puede ser explotada por atacantes para realizar acciones maliciosas o acceder a información confidencial.

Los expertos en ciberseguridad tienen como objetivo detectar y mitigar las vulnerabilidades antes de que sean explotadas por atacantes malintencionados. Para lograr esto, utilizan herramientas y técnicas avanzadas para escanear la red y las aplicaciones en busca de vulnerabilidades conocidas, así como también realizan pruebas de penetración para identificar posibles debilidades en la seguridad.

Vulnerabilidades más destacadas:

- Errores en la gestión de recursos: Una aplicación permite que se consuma un exceso de recursos afectando a la disponibilidad de los mismos.
- Error de configuración: Problemas de configuración de software o de los servicios web.
- Factor humano: Negligencias causadas generalmente por la falta de formación y concienciación.
- Validación de entrada: Fallo en la validación de datos introducidos en aplicaciones.
- Salto de directorio: Fallo en la depuración de un programa, en la validación de caracteres especiales.
- Permisos, privilegios y/o control de acceso: Fallos en la protección y gestión de permisos.

- **Amenaza**

Una amenaza en ciberseguridad abarca cualquier acción malintencionada o situación que ponga en riesgo la seguridad de tus dispositivos y datos en el mundo digital. Las crean ciberdelincuentes que buscan acceder, dañar o robar información privada.

Las amenazas de un sistema informático provienen principalmente de ataques externos (malware, denegación de servicio o inyecciones SQL, entre otros), de no cumplir las políticas de seguridad (conectar dispositivos no autorizados a la red o utilizar contraseñas débiles) y de sucesos inesperados (como incendios o robos físicos, por ejemplo).

Podemos nombrar las amenazas más importantes a las que se enfrenta una infraestructura IT son:

Código malicioso. Estos ataques malware atacan dispositivos y servidores con el fin de robar información sensible, como datos bancarios o credenciales de acceso. Los ataques ransomware son una de las mayores amenazas hoy en día para los sistemas informáticos de las empresas.

Robo de identidad. Otra amenaza que pone en riesgo los sistemas de una organización es el phishing o robo de identidad. La amenaza consiste en engañar al usuario para que facilite de forma involuntaria sus credenciales de acceso a un tercero que las utilizará de forma fraudulenta.

Amenazas Persistentes Avanzadas. Las conocidas como APT (Amenazas Persistentes Avanzadas) son ataques coordinados que se dirigen a una empresa para robar sus datos. Son una de las amenazas más difíciles de detectar, ya que utilizan técnicas de ingeniería social.

Denegación de servicio. Los ataques DDoS son una amenaza que se cierne sobre servidores que pretenden ser colapsados enviándoles una enorme cantidad de peticiones (haciendo que no puedan atenderlas, e incluso que terminen cayendo).

Negligencia. Los usuarios suelen ser la mayor amenaza para un sistema informático. Los errores humanos y el no incumplimiento de las políticas y normas de seguridad de la empresa ponen en peligro los sistemas y los datos de la empresa.

- **Impacto**

En ciberseguridad, el "impacto" se refiere a la magnitud del daño o las consecuencias que pueden surgir como resultado de una amenaza que ha explotado una vulnerabilidad en un sistema o red. El impacto evalúa la gravedad de los posibles efectos adversos en la integridad, confidencialidad y disponibilidad de la información o activos digitales. En términos simples, es el resultado negativo que puede ocurrir después de que se ha materializado una amenaza.

Algunos ejemplos de impacto en ciberseguridad incluyen:

Pérdida de Datos: La información confidencial puede ser comprometida o robada, lo que podría tener consecuencias graves para la organización o los individuos afectados.

Interrupción de Servicios: Un ataque exitoso podría resultar en la interrupción de servicios críticos, lo que afectaría la disponibilidad de los recursos digitales.

Daño Financiero: Los ataques cibernéticos pueden causar pérdidas financieras directas, como robo de fondos o costos asociados con la recuperación de sistemas comprometidos.

Daño a la reputación: La divulgación de incidentes de seguridad o la pérdida de datos sensibles pueden dañar la reputación de una organización, afectando su relación con clientes, socios y el público en general.

Impacto en la privacidad: La exposición de información personal puede tener implicaciones significativas para la privacidad de individuos, lo que puede resultar en sanciones legales y daño a la confianza del público.

Fallo de Cumplimiento Normativo: Si una organización está sujeta a regulaciones específicas, un incidente de seguridad podría dar lugar a violaciones de normativas y leyes, con posibles sanciones legales.



Referencias Bibliográficas.

Mejia, R. (s. f.). ¿QUÉ ES LA TRIADA DE SEGURIDAD ó CIA TRIAD? y POR QUÉ DEBERÍA INTERESARTE. https://blog.smartekh.com/que-es-la-triada-de-seguridad-o-cia-triad-y-por-que-deberia-interesarte#:~:text=La%20CIA%20TRIAD%20est%C3%A1%20conformada,Disponibilidad

VirusZzWarning. (2022, 23 abril). Introduction || Ethical Hacking — Part 1.1 - System weakness. Medium. https://systemweakness.com/introduction-ethical-hacking-part-1-1-4a55f87e1d88

¿Qué es un riesgo de ciberseguridad? | Actinver. (s. f.). https://actinver.com/que-es-riesgo-ciberseguridad#:~:text=Un%20riesgo%20de%20ciberseguridad%20son,o%20sean%20modificadas%20por%20delincuentes.

De TechTarget, C. (2021, 19 julio). Autenticación multifactor o MFA. ComputerWeekly.es. https://www.computerweekly.com/es/definicion/Autenticacion-multifactor-o-MFA#:~:text=La%20autenticaci%C3%B3n%20multifactor%20(multi%20factor,de%20sesi%C3%B3n%20u%20otra%20transacci%C3%B3n.

De La Iglesia, E. D. (2023, 11 mayo). Tipos de vulnerabilidades en ciberseguridad. https://www.campusciberseguridad.com/blog/item/118-tipos-de-vulnerabilidades-en-ciberseguridad