CONCEPTOS BASICOS DE SEGURIDAD

Tarea #995

200300590
Israel Alejandro Cel Alcocer

Conceptos Básicos

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.

Usability triangle: 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.

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.

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)

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.