Universidad del Istmo

Campus Tehuantepec

Carrera: Ingeniería en computación

Grupo: 704

Alumno:

Juan Emmanuel Becerril Nolasco

Materia: Redes II

Profesor: Carlos Mijangos Jimenéz

1er Parcial

Trabajo: “Investigación sobre la triada de la ciberseguridad”

Santo Domingo Tehuantepec, a 27 de octubre del 2025

Triada de la ciberseguridad (CID)

Las tres letras de la "tríada de la CID" significan confidencialidad, integridad y disponibilidad. La tríada de la CID es un modelo común que constituye la base para el desarrollo de sistemas de seguridad. Se utilizan para encontrar vulnerabilidades y métodos para crear soluciones.
La confidencialidad, integridad y disponibilidad de la información es crucial para la operación de un negocio, y la tríada CIA segmenta estas tres ideas en puntos focales separados. Esta diferenciación es útil porque ayuda a guiar a los equipos de seguridad a medida que identifican las diferentes formas en que pueden abordar cada inquietud.

1. Confidencialidad

La confidencialidad implica los esfuerzos de una organización para garantizar que los datos se mantengan en secreto o privados. Para lograr esto, el acceso a la información debe controlarse para evitar el intercambio no autorizado de datos, ya sea intencional o accidental y asegurar la integridad de la información.

Un componente clave para mantener la confidencialidad es asegurarse de que las personas sin la autorización adecuada no tengan acceso a activos importantes dentro de un negocio. Por el contrario, un sistema eficaz también garantiza que aquellos que necesitan tener acceso tengan los privilegios necesarios.

Hay varias maneras en que la confidencialidad y seguridad de la información puede verse en riesgo. Esto puede implicar ataques directos destinados a obtener acceso a los sistemas que el atacante no tiene los derechos para ver. También puede involucrar a un atacante que intenta infiltrarse directamente en una aplicación o base de datos para tomar datos o alterarlos.

Para combatir las violaciones de la confidencialidad, puede clasificar y etiquetar datos restringidos, habilitar políticas de control de acceso, cifrar datos y usar sistemas de autenticación multifactor (MFA).

2. Integridad

La integridad implica asegurarse de que los datos trabajados, por ejemplo, dentro de un negocio, sean confiables y estén libres de alteraciones. La integridad de los datos se mantiene solo si estos son auténticos, precisos y confiables.

A menudo, comprometer la integridad se hace intencionalmente. Un atacante puede omitir un sistema de detección de intrusos (IDS, por sus siglas in inglés), cambiar las

configuraciones de archivos para permitir el acceso no autorizado o alterar los registros que mantiene el sistema para ocultar el ataque y poner en riesgo la seguridad de la información, aunque la integridad también puede violarse por accidente.

Para proteger la integridad de la información y los datos, se puede usar hash, cifrado, certificados digitales o firmas digitales. Para los sitios web, se puede emplear autoridades de certificación (CA) confiables que verifiquen la autenticidad de un sitio web para que los visitantes sepan que en verdad acceden al sitio que pretendían visitar.

Un método para verificar la integridad es el no repudio, que se refiere a cuando algo no puede ser repudiado o denegado. Por ejemplo, si los empleados de una empresa utilizan firmas digitales al enviar correos electrónicos, no se puede negar el hecho de que el correo electrónico proviene de ellos. Además, el destinatario no puede negar que recibió el correo electrónico del remitente.

3. Disponibilidad

Incluso si los datos se mantienen confidenciales y se mantiene su integridad, a menudo son inútiles, a menos que estén disponibles para aquellos en la organización y los clientes a los que prestan servicios. Esto significa que los sistemas, las redes y las aplicaciones deben funcionar como deberían y cuándo deberían. Además, las personas con acceso a información específica deben ser capaces de consumirla cuando lo necesitan, y llegar a los datos no debería tomar una cantidad de tiempo excesiva.

Para garantizar la disponibilidad, las organizaciones pueden utilizar redes, servidores y aplicaciones redundantes. Estos pueden programarse para que estén disponibles cuando el sistema primario se haya interrumpido o roto. También puede mejorar la disponibilidad manteniéndose al tanto de las actualizaciones de los paquetes de software y los sistemas de seguridad.

De esta manera, es menos probable que una aplicación funcione mal o que una amenaza relativamente nueva se infiltre dentro de un sistema y ponga en riesgo la integridad de la información. Las copias de seguridad y los planes completos de recuperación ante desastres también ayudan a una empresa a recuperar la disponibilidad poco después de un evento negativo.