Pilares de la Ciberseguridad

Triada CIA (Confidencialidad, Integridad, Disponibilidad)

La triada CIA (Confidencialidad, Integridad, Disponibilidad) ha sido la base de la Ciberseguridad durante mucho tiempo

Estos principios básicos **se utilizan como un marco para guiar las políticas, prácticas y controles de Ciberseguridad que se establecen** en un entorno tecnológico

Triada CIA | Confidencialidad

El concepto de confidencialidad se refiere a la **capacidad de garantizar que la información no se encuentra disponible o es revelada a individuos que no tienen autorización para consultarla**

Deben aplicarse una serie de controles, que aseguren que se cumplen afirmaciones como las siguientes:

- La información almacenada en un sistema de información no puede ser consultada por error o de manera intencionada sin la autorización de quien la ha almacenado

- La información que se transmite desde un punto A a un punto B, no puede ser consultada por error o de manera intencionada sin la autorización de quien la ha transmitido

Triada CIA | Integridad

El concepto de integridad se refiere a la **capacidad de garantizar la exactitud y completitud de la información a lo largo de todo su ciclo de vida**

Deben aplicarse una serie de controles, que aseguren que se cumplen afirmaciones como las siguientes:

- La información almacenada en un sistema de información no puede ser modificada por error o de manera intencionada sin el conocimiento de quien la ha almacenado

- La información que se transmite desde un punto A a un punto B, no puede ser modificada por error o de manera intencionada sin el conocimiento de quien la ha transmitido

Triada CIA | Disponibilidad

El concepto de disponibilidad se refiere a la **capacidad de garantizar que la información se encuentra disponible siempre que se requiere** acceder a ella

Deben aplicarse una serie de controles, que aseguren que se cumplen afirmaciones como las siguientes:

- La información almacenada en un sistema de información debe poder ser accesible siempre que sea necesario

Triada CIA | ¿Es suficiente?

Autenticación: es el **proceso de verificar la identidad de un usuario**. Cuando un usuario intenta acceder a un recurso o servicio, se le solicita que proporcione credenciales, como un nombre de usuario y contraseña. Estos datos se comparan con la información almacenada en el sistema. Si coinciden, el proceso de autenticación ha sido exitoso y el usuario es reconocido por el sistema como legítimo

Autorización: es el proceso que **sigue a la autenticación**. Una vez que el sistema ha autenticado la identidad de un usuario, el siguiente paso es **determinar qué recursos puede acceder y qué acciones puede realizar**. Esto se logra a través de políticas de autorización que definen los derechos de acceso de un usuario.

No repudio: se refiere a la capacidad de garantizar que, **cuando se realiza un intercambio de información, el receptor de la información no puede negar haberla recibido**, y el emisor de la información no puede negar haberla enviado.