

CONCEPTOS BASICOS DE SEGURIDAD:

1. **CIA TRIAD:** Es un modelo común que forma la base para el desarrollo de sistemas de seguridad. Las tres letras en "CIA triad" representan Confidencialidad, Integridad y Disponibilidad.

<https://www.itgovernance.co.uk/blog/wp-content/uploads/2023/02/image-2.png>

- **Confidencialidad:** Se refiere a los esfuerzos de una organización para asegurar que los datos se mantengan en secreto o privados.
- **Integridad:** Los datos deben mantenerse en un estado correcto y nadie debe poder modificarlos incorrectamente, ya sea accidentalmente o maliciosamente.
- **Disponibilidad:** Los usuarios autorizados deben poder acceder a los datos cuando lo necesiten.

2. **USABILITY TRIANGLE:** se refiere a un enfoque que integra tres aspectos fundamentales en el desarrollo de productos y experiencias digitales, donde se busca el mantener (en el mejor de los casos) un equilibrio entre las 3 características.

<https://cdn.getmidnight.com/d0f1c52a0107bd8707444bbf130a0234/2022/08/functionality-usability-security.webp>

- **Seguridad:** Este componente se refiere a la protección de la información y la privacidad de los usuarios. En el contexto del "Usability Triangle", la seguridad implica que el producto o sistema debe ser capaz de proteger los datos sensibles de los usuarios, prevenir accesos no autorizados y garantizar la integridad de la información.
- **Funcionalidad:** La funcionalidad se refiere a la capacidad del producto o sistema para cumplir con las necesidades y expectativas de los usuarios. Esto implica que el producto debe ofrecer las características y herramientas necesarias para que los usuarios puedan realizar sus tareas de manera efectiva.
- **Usabilidad:** La usabilidad se refiere a la facilidad de uso y la experiencia del usuario al interactuar con el producto o sistema. Incluye aspectos como la facilidad de aprendizaje, la eficiencia en el uso, la satisfacción del usuario y la capacidad de recuperación ante errores.

3. **Riesgo:** Es la exposición a una situación donde hay una posibilidad de sufrir un daño o de estar en peligro.
4. **MFA (Autenticación Multifactor):** Es un método de autenticación que requiere que el usuario proporcione dos o más factores de verificación para obtener acceso a un recurso, como una aplicación, una cuenta en línea o una VPN.
5. **Vulnerabilidad:** Es el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes, sean ellos desastres naturales, desigualdades económicas, políticas, sociales o culturales.
6. **Amenaza:** Es un gesto, una expresión o una acción que anticipa la intención de dañar a alguien en caso de que la persona amenazada no cumpla con ciertas exigencias.

7. **Impacto:** Es el choque o la colisión de dos objetos o seres. También puede referirse al efecto de una fuerza aplicada bruscamente.