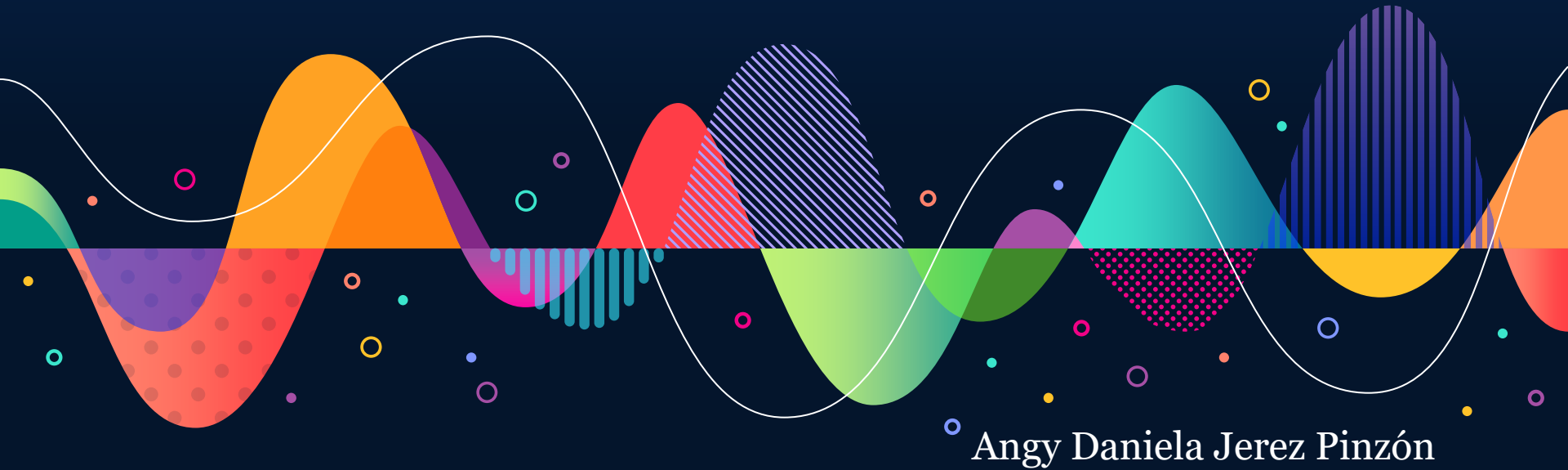


Seguridad Informática



Angy Daniela Jerez Pinzón

¿Qué es seguridad informática?



La **seguridad informática** es la protección de la información y especialmente el procesamiento de la información. La seguridad de la información tiene por objeto impedir la **manipulación de datos y sistemas por terceros no autorizados**. El significado de esto es que los sistemas social-técnicos, es decir, las personas y la tecnología, dentro de las empresas / organizaciones y sus datos están protegidos contra daños y amenazas. Esto no sólo significa información y datos, sino también centros de datos físicos o servicios de nube



¿Cuál es el objetivo de la seguridad informática?





La información se ha vuelto cada vez más valiosa en los últimos años. Por lo tanto, es muy importante protegerla. La seguridad de la información se define por los **tres objetivos** de protección de la tecnología de la información: **disponibilidad, integridad y confidencialidad**. Estos deben ser mantenidos. Además, hay otras partes que deben ser añadidas: autenticidad, responsabilidad, no repudio y fiabilidad.

Confidencialidad de la información



La confidencialidad de la seguridad informática significa que los datos sólo son accesibles a determinadas personas autorizadas. Por ejemplo, sólo un determinado grupo de personas puede acceder a los datos que contiene. En otras palabras, hay que definir la protección de acceso. Esto significa que también deben asignarse derechos de acceso. Otro punto central en la confidencialidad de la información es el transporte de datos. Esto siempre debería estar cifrado, – simétrica o asimétricamente. Esto significa que las personas no autorizadas no pueden acceder a los contenidos

Integridad de la información



La integridad de la información debe asegurar que el **contenido y los datos** están siempre **completos y correctos**. Esto significa que los sistemas también deben funcionar correctamente para su propósito.

- ★ Por ejemplo, los datos no deben ser alterados por transmisión o procesamiento. Esto también significa que terceros no autorizados tienen la posibilidad de borrar o reemplazar datos (parciales). Si se produce un caso así, hay que asegurarse de que se impida **este tipo de manipulación** y de que se pueda detectar y corregir la brecha de seguridad.

Disponibilidad de la información



Garantizar la disponibilidad de la información respectiva significa que el **procesamiento de los datos dentro de los sistemas funciona sin problemas**. Los datos deben poder recuperarse correctamente en el momento deseado. Esto significa que los sistemas informáticos deben ser protegidos contra los fallos. Por eso también hay pruebas de carga para comprobar los límites, de modo que las operaciones comerciales se mantengan, en cualquier caso.

