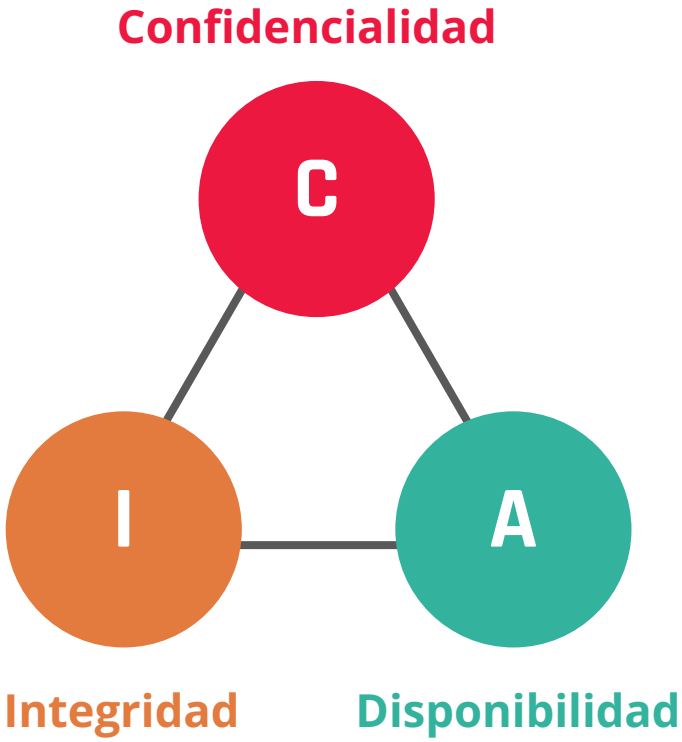
Clase 24 - Amenazas Informáticas

1

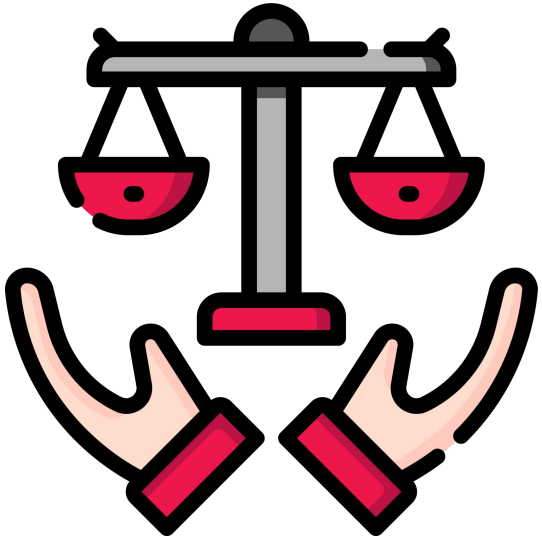
Información

La información es recurso clave para tomar decisiones, dimensionar cosas, y disminuir riesgos. La misma cuenta con tres dimensiones conocidas como: integridad, disponibilidad y confidencialidad, también llamadas CIA por sus siglas en inglés. Los atacantes de un sistema van a tratar de vulnerar algunas de esas dimensiones.



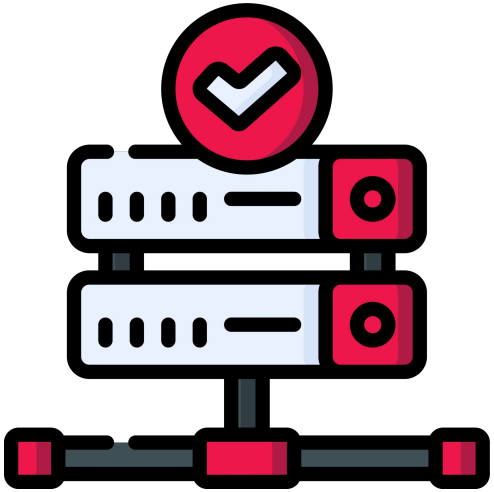
Integridad

Consiste en que la información se encuentre completa, entera y que los datos que están dentro del sistema sean los que deberían ser. Un ejemplo de esta dimensión sería el ataque a una base de datos y la modificación de los datos que hay en la misma, con lo cual podemos seguir viendo la información, pero la misma es errónea debido a que la original fue alterada.



Disponibilidad

Significa que la información una persona/usuario debe poder tener acceso a la información en el momento que lo necesita, es decir, en tiempo y forma. Un típico ataque a este tipo de dimensión es el ataque de denegación de servicio.



Confidencialidad

Refiere a que la información tiene que estar disponible únicamente para las personas que tienen acceso a esta información y bloqueada para el acceso a terceros. Por ejemplo, los datos personales e historiales médicos.

2 Protección de la información

“

La **protección de la información** se basa en garantizar el completo y total funcionamiento de las 3 dimensiones, para ello, debemos implementar medidas preventivas y reactivas.

”

Medidas preventivas se refiere a todas las acciones que pueden tomarse para evitar problemas no deseados.
Por otro lado, las **medidas reactivas** son aquellas donde ya se ocasionó un problema de seguridad y hay que solventarlo.

Protección de la confidencialidad

La confidencialidad puede romperse de varias maneras, tanto directas (hackeando la seguridad) como indirectas a través de errores humanos. Algunas técnicas para asegurar la confiabilidad pueden ser:

Nombre	Descripción
Encriptación	Significa cambiar el formato de los datos con la razón de que si estos son interceptados solo las personas autorizadas sepan cómo leerlos (medida preventiva).
Controles de acceso	Asegurar que solo las personas autorizadas puedan acceder a la información (medida preventiva).
Borrado remoto	Se refiere al esfuerzo de mantener los datos siempre privados, en el caso de que se perdiera el acceso, la capacidad de bloquear el dispositivo o borrar la información (medida reactiva).
Capacitación al personal	Existe un concepto llamado **ingeniería social**, el cual es la denominación que se le da a cómo los usuarios son engañados para otorgar sus accesos, la capacitación en estos problemas es una acción preventiva para evitarlos.

Protección de la integridad

La integridad puede romperse de varias maneras similares a la de la confiabilidad, por lo cual, varias de sus acciones de seguridad son reutilizadas. Algunas técnicas para asegurar la integridad pueden ser:

Nombre	Descripción
Auditorias	Se utilizan para comprobar que la información coincide con lo que debería ser correcto (medida reactiva).
El control de versiones	Si ha ocurrido un inconveniente con la información, diversas herramientas de control de versiones ayudan a “volver a un estado anterior” (medida reactiva).
Firmas digitales	Esta medida permite asegurar la autenticidad del documento (medida preventiva).
Detección de intrusos	Diseñados para detectar problemas cuando un acceso no autorizado se ha cometido (medida reactiva).

Protección de la disponibilidad

La disponibilidad debe tenerse en cuenta para cuando ocurra un problema de seguridad como de forma preventiva al mismo. Algunas técnicas para asegurar la disponibilidad pueden ser:

Nombre	Descripción
Tolerancia a fallos	La capacidad de los sistemas o servidores a que si algún tipo de fallo sucede, la información pueda ser utilizada (preventiva o reactiva dependiendo la situación).
Redundancia	De esta forma la información y las validaciones de acceso se repitan tanto que la información está segura de no perderse en su totalidad (preventiva).
Parches de seguridad	Cuando se detecta una falla, debe solucionarse el problema para que no vuelva a ocurrir, igualmente si la falla fue por un software, actualizarlo con la vulnerabilidad resuelta.


DigitalHouse>
Coding School