

UNIVERSIDAD DE CIENCIAS MÉDICAS DE LA HABANA
Centro Provincial de Información de Ciencias Médicas

Seguridad Informática. Conceptos Básicos.



Lic. Brian Kindelán Iglesias
Gestor de Información en Salud
Área Tecnológica CPICMH
Email: blogscpi@infomed.sld.cu

Concepto:

- La **seguridad informática** consiste en asegurar que los recursos del sistema de información (Material informático o programa) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.



- La seguridad de los datos y de la información comprende 5 aspectos fundamentales:



- - **Confidencialidad** -> Es decir, no desvelar datos a usuarios no autorizados. Esto comprende también la privacidad (Protección de datos personales).
- - **Integridad** -> Permite asegurar que los datos no sean falseados.
- - **Disponibilidad** -> Que la información se encuentre accesible en todo momento a los usuarios autorizados.
- - **Autenticación** -> Es la situación en la cuál se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice.
- - **No repudio** -> Permite probar las partes en una comunicación frente a un tercero. También se puede llamar irrenunciabilidad



Confidencialidad

- Se trata de la cualidad que debe poseer un documento u archivo para que este solo entienda de manera comprensible o sea leído por la persona o sistema que esté autorizada.
- Un documento es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. Esto evita que una interceptación de un mensaje pueda ser leído por una persona no autorizada.



Integridad

- ▶ La integridad es la cualidad que posee un documento que no ha sido alterado y que además permite comprobar que no se ha manipulado el documento original.
- ▶ También es una forma de dar al destinatario de que el correo no ha sido modificado.

Disponibilidad

- Se trata de la capacidad de un servicio de unos datos o de un sistema a ser accesible y utilizable por los usuarios autorizados cuando éstos lo requieran.
- También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, es decir, evitar su pérdida o bloqueo.
- La disponibilidad suele ser un factor muy importante en servidores o páginas masivamente grandes, como puede ser facebook, ya que necesitan mantener la información disponible las 24 horas del día los 7 días de la semana.



Autenticación

- Es la situación en la cual se puede verificar que un documento pertenece a quién el documento dice.
- Aplicada a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aplicar algún modo de que se pueda verificar que dicha persona es quien dice ser.
- La autenticación en la informática se suele hacer con un usuario y contraseña.

Amenazas








Amenazas

- PERSONAS
 - LÓGICAS
 - FÍSICAS
- 

De estas amenazas se derivan los tipos de seguridad informática:



- Seguridad física y seguridad Lógica

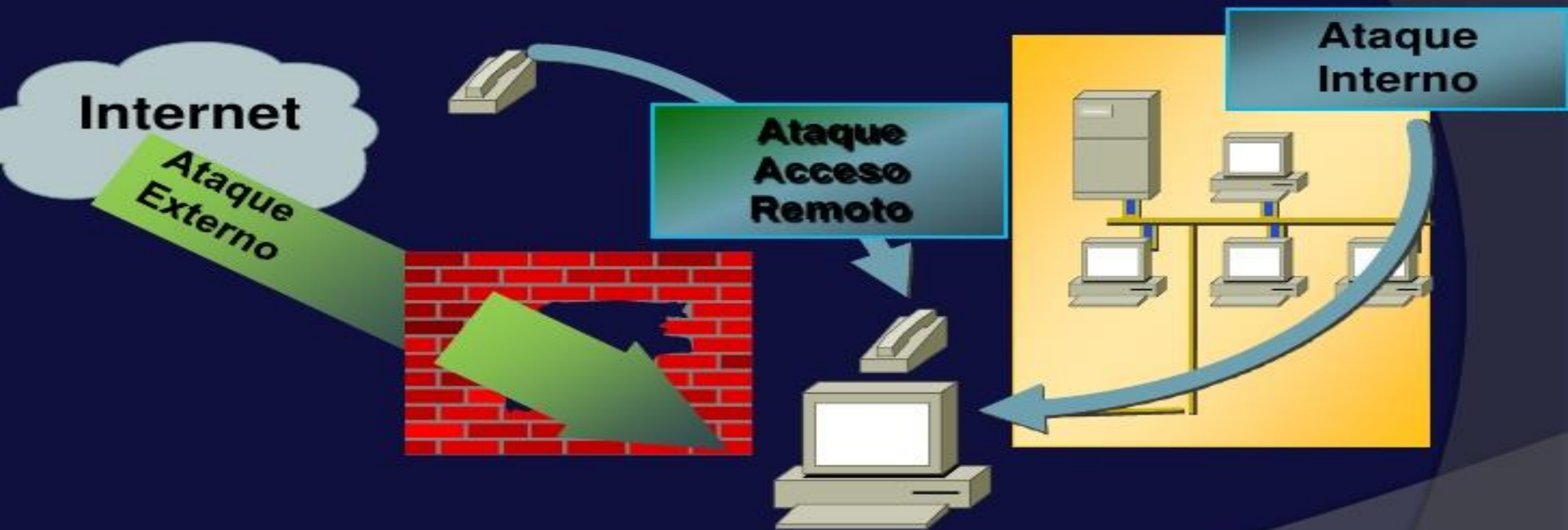


De esta forma, tenemos varias posibles violaciones de seguridad a un sistema, o sea, varias **amenazas**, entre las cuales destacamos:

- Destrucción de información.
- Modificación de la información.
- Robo, remoción o pérdida de la información o los recursos.
- Interrupción de servicios.

Debemos todavía definir "**ataque**": es la realización efectiva de una amenaza en forma intencional.

¿De quién nos protegemos?





Nivel de seguridad

- ▶ La magnitud y nivel requerido de seguridad en un sistema de red depende del tipo de entorno en el que trabaja la red. Una red que almacena datos para un banco importante, requiere una mayor seguridad que una LAN que enlaza equipos en una pequeña organización de voluntarios.



Varios mecanismos utilizados para implementar políticas de seguridad en las redes.

- - Criptografía.
- - Firma digital.
- - Autenticación.
- - Control de acceso.
- - Rótulos de seguridad.
- - Detección, registro e informe de eventos.
- - Llenado de tráfico.
- - Control de ruteo.



TELEMONTOREAMOS
Seguridad Electrónica

VIGILADO SUPERVISORIAL Res. 20157200011017 de 26-02-2015



CONTROL DE ACCESO

Control de asistencia

Lectores biometricos, de huellas y tarjetas

Cerraduras



- 
- 
- Tomar conciencia de las medidas de seguridad informática de nuestra institución y cumplirlas a cabalidad nos evitará en gran medida ser afectados por un ataque tanto externo como interno.
 - Debemos estar siempre alertas ante cualquier amenaza sea intencional o no intencional.
 - Mientras mas barreras de seguridad tenga el atacante menos probabilidades de ingresar con éxito en el objetivo tendrá.

Muchas Gracias



Lic. Brian Kindelán Iglesias
Gestor de Información en Salud
Área Tecnológica CPICMH
Email: blogscpi@infomed.sld.cu