Amenazas Informáticas

Grupo 1

Acosta Brenda, Colonia Silvina, Miyashiro Luciana, Opradolce Mar, Ramirez Linda Jessenia.

1.Tipos de Amenazas (MALWARE)

MALWARE (Malicious software)

*Los más conocidos y comunes son:

VIRUS	GUSANOS	TROYANOS
Se copia a sí mismo en los sistemas	Se copia a otras máquinas por medio de la red	Basados en el “Caballo de Troya”
Infecta a todo el dispositivo	Satura el sistema	Programas sin licencia y cracks
Son de poca infección(solo afecta a un dispositivo)	Mayor capacidad de infección	Pueden crear backdoors

Los malwares más peligrosos

Recopila información de un ordenador informático y transmite la información a una entidad externa sin el permiso del usuario.

Paquete de software diseñado para permanecer oculto en su equipo mientras proporciona acceso y control remotos.

Los malwares más peligrosos

Conjunto o red de robots informáticos que controlan todos los ordenadores infectados de forma remota.

Este se introduce en el dispositivo, luego cifra por completo el sistema operativo o algunos de los archivos. Finalmente, se le exige a la víctima el pago de un rescate.

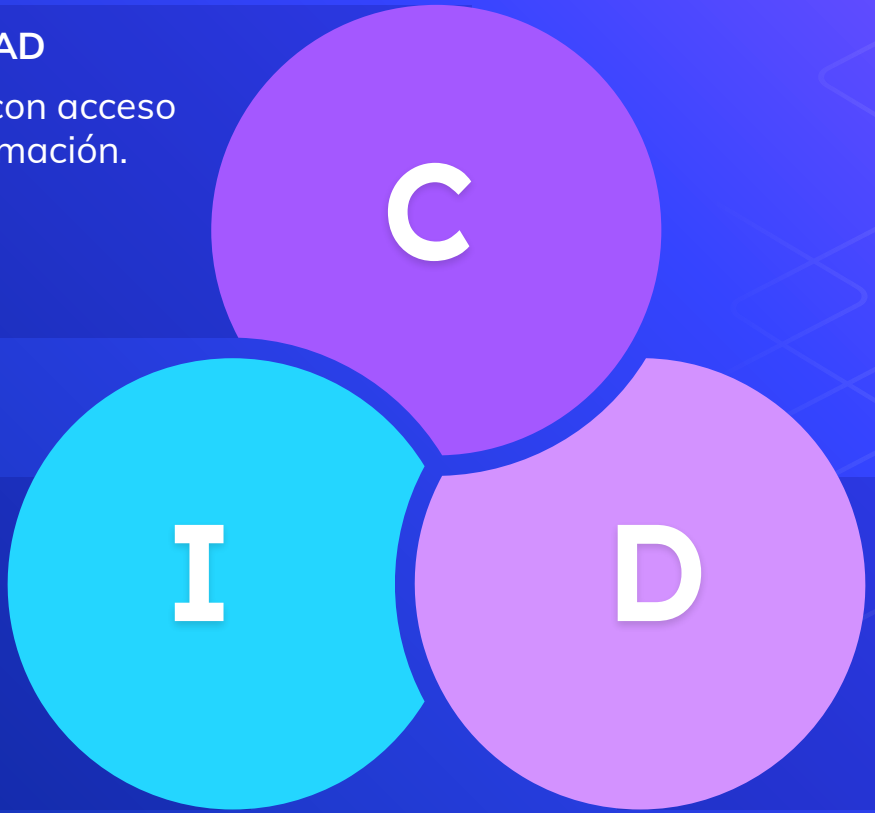
2. Seguridad Informática

La información es clave para tomar decisiones y disminuir riesgos.

Dimensiones de la información

CONFIDENCIALIDAD

Solo las personas con acceso pueden ver la información.



INTEGRIDAD

Los datos deben ser correctos y no estar alterados.

DISPONIBILIDAD

Debo poder acceder a la información.

Protección de la Confidencialidad

Encriptación

Cambia el formato de los datos.

Si son interceptados estarán solo las personas autorizadas podrán leerlos.

(preventiva)

Control de acceso

Controlan que solo las personas autorizadas puedan acceder a la información.

(preventiva)

Borrado remoto

En caso de que se pierda el acceso a la información, se puede bloquear el acceso o borrarla, para que no se publique.

(reactiva)

Capacitación del personal

Se lo llama ingeniería social.

(preventiva)

Protección de la Integridad

Auditorías

Se comprueba que la información sea la correcta.

(reactiva)

Control de versiones

Permite volver a una versión anterior donde la información no ha sido alterada.

(reactiva)

Firmas digitales

Permite identificar la entidad que originó el documento y confirmar que no ha sido alterado desde que fue firmado.

(preventiva)

Detección de intrusos

Detecta los accesos no autorizados.

(reactiva)

Protección de la Disponibilidad

Tolerancia a fallos

Permite que la información siga disponible a pesar de fallos en el servidor o el sistema.

Redundancia

Tener un respaldo de la información por si esta se pierde.

Parches de seguridad

Cuando se resuelven problemas de vulnerabilidad se debe actualizar el sistema para que no vuelvan a ocurrir.

3.
Ingeniería Social

La ingeniería social es el método de obtener información confidencial a través de usuarios legítimos del sistema a atacar.

Técnicas

Pretexting

Investigación previa por parte del atacante

Escenario inventado

Mentira elaborada

Lleva a develar información

Baiting

Dispositivo de almacenamiento “olvidado”

Lugar facil de encontrar

Software malicioso

Técnicas

Phishing

SMS, E-mail, redes sociales, etc

Engaño

Robo de información

Vishing

Llamadas telefónicas

Técnicas

Redes sociales

Obtener información

Relacionarse

Estafa

Técnicas

Ciberbullying

Entre iguales

Daño psicológico

Acoso

Chantaje

Grooming

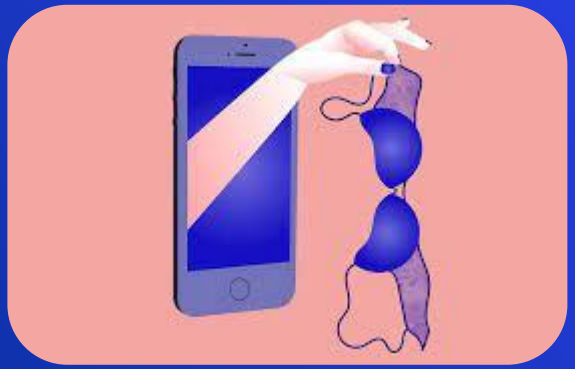
Un adulto hacia un menor

Abuso sexual

Técnicas

Sexting

Principalmente a través del celular



Difusion

Contenido sexual

Sextortion

Chantaje

Muchas gracias!