SEGURIDAD DE LA INFORMACIÓN Y ÉTICA EN INFORMÁTICA



Prof.Dilsa Vergara





1

OBJETIVOS:



- Comprender la importancia de la seguridad y aspectos legales asociados con el uso de los computadores.
- Conocer las amenazas y ataques existentes para los sistemas informáticos y la forma de contrarrestarlas.
- Conocer los aspectos éticos de la profesión de tecnologías de información y comunicación y las responsabilidades implícitas en la

2



- Serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización. (ISO 7498)
- La seguridad informática es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática. Es una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos en una organización.

Qué es la seguridad informática?

Objetivos de la Seguridad Informática Proteger los recursos informáticos del daño, la alteración, el robo y la pérdida de equipos, medios de almacenamiento, software y los datos. Mantener la continuidad de los procesos organizacionales que soportan los sistemas de información.

4



Evidencias que ameritan seguridad informática

- 1 El crecimiento del acceso a Internet y de usuarios conectados incrementa la posibilidad de amenazas informáticas.
- 2 Crecimiento de la información disponible de empresas y sus empleados en redes sociales → Ingeniería Social.
- Mensajes de e-mail que contienen attachments que permiten vulnerabilidades en las aplicaciones instaladas por los usuarios.
- 4 Aumento de programas maliciosos.





5

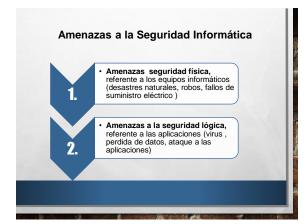


Vulnerabilidades y amenazas a la seguridad informática

La vulnerabilidad es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir perdidas en la organización.

Amenaza: es cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático provocando perdidas materiales , financieras o de otro tipo a la organización.





8

Medidas de seguridad





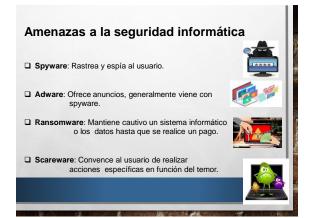
- Las medidas de seguridad es cualquier medio empleado para eliminar o reducir un riesgo.
- El objetivo es reducir las vulnerabilidades de los activos, las probabilidades de ocurrencia de las amenazas y el impacto en la organización.
- Existen herramientas para garantizar la seguridad como los antivirus, parches, copias de seguridad, entre otras.



Amenazas (Malwares)

- Malware es la abreviatura de "malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.
- Incluye virus, gusanos, troyanos, etc.

10





P	his	hir	
	1113		м

- Phishing se refiere a la captación de datos personales realizada de manera ilícita o fraudulenta a través de internet. Es una palabra del inglés que se origina de su homófona "fishing", que significa 'pesca', en alusión al objetivo del phishing: pescar datos, ver "quién muerde el anzuelo". El phishing es ejecutado por un phisher o 'pescador'.
- El phishing es una técnica de ingeniería social que emplea el envío masivo de correos electrónicos spam en nombre de una entidad bancaria, con la finalidad de obtener datos personales y financieros (principalmente aquellos asociados a claves de acceso), o de redirigir a los usuarios a una página web falsa de la entidad donde estos tengan que depositar sus datos.

Phishing.



• Como rasgos característicos, los correos de phishing suelen solicitar al usuario, con carácter de urgencia, la confirmación o el envío de determinados datos bajo la excusa de problemas técnicos, cambios en la política de seguridad, detección de posibles fraudes, promociones o concursos. Incluso, puede incorporar la fórmula coactiva de que si el usuario no realiza la acción solicitada inmediatamente, su tarjeta o cuenta podrá ser bloqueada.

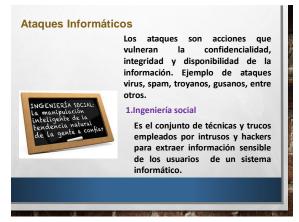
14

VIRUS

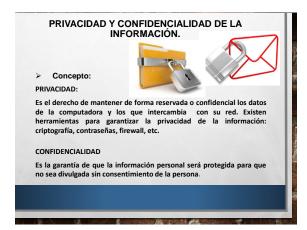


- Un virus informático es un malware que tiene por objetivo alterar el normal funcionamiento del ordenador sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este.
- Pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Troyanos Los troyanos son software malicioso que se le presenta al usuario como un programa legitimo, pueden crear una puerta trasera que permite la administración remota. Gusanos Se duplica a sí mismo, se propaga sin la ayuda de una persona, causan problemas en la red.







PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN > Protección a la privacidad. Para proteger su privacidad e información sensitiva usted necesita tomar varias medidas, incluyendo prevenir, detectar y responder a una gran variedad de ataques. Hay muchos riesgos, y unos son más serios que otros. Algunos de los peligros son: - Virus que infectan todo su sistema. - Personas que entran a su sistema y hacen modificaciones a sus archivos. - Hackers que usan su computadora para atacar a otros. - Ladrones que roban su computadora y su información personal.







