

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 contrarrestarlos.
- Conocer los aspectos éticos de la profesión de tecnologías de información y comunicación y las responsabilidades implícitas en la misma.

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?**

3

Objetivos de la Seguridad Informática

1.

- Proteger los recursos informáticos del daño, la alteración, el robo y la pérdida de equipos, medios de almacenamiento, software y los datos.

2.

- 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**.
- 3 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 pérdidas en la organización.

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

6

Vulnerabilidades a la seguridad informática

Vulnerabilidad ligada a

- Aspectos organizativos
- Factor humano
- Equipos
- Programas o aplicaciones
- Condiciones ambientales

7

Amenazas a la Seguridad Informática

1.

- **Amenazas seguridad física**, referente a los equipos informáticos (desastres naturales, robos, fallos de suministro eléctrico)

2.

- **Amenazas a la seguridad lógica**, referente a las aplicaciones (virus, pérdida de datos, ataque a las aplicaciones)

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.

9



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

Amenazas a la seguridad informática

- ❑ **Spyware:** Rastrea y espía al usuario.
- ❑ **Adware:** Ofrece anuncios, generalmente viene con spyware.
- ❑ **Ransomware:** Mantiene cautivo un sistema informático o los datos hasta que se realice un pago.
- ❑ **Scareware:** Convince al usuario de realizar acciones específicas en función del temor.



11

SPAM

- Se le llama spam a mensajes de email no deseados o no solicitados que provienen de un remitente que usted no conoce. Los emails de spam se mandan en grandes volúmenes y su contenido es casi idéntico.
- El spam se divide en dos categorías:
 - Mensajes que molestan**, como solicitudes para que compre productos o servicios.
 - Emails maliciosos** que buscan engañarlo para que usted revele su información personal para que alguien pueda defraudarlo o dañar su computadora.



12

Phishing.

- 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.



13

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



¿QUÉ SON LOS VIRUS INFORMÁTICOS?



- 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.

15

Troyanos

Los troyanos son software malicioso que se le presenta al usuario como un programa legítimo, 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.



16

Ataques Informáticos

Los ataques son acciones que vulneran la confidencialidad, integridad y disponibilidad de la información. Ejemplo de ataques virus, spam, troyanos, gusanos, entre otros.



1. Ingeniería social

Es el conjunto de técnicas y trucos empleados por intrusos y hackers para extraer información sensible de los usuarios de un sistema informático.

17

Ataques Informáticos



2. Denegación de servicio

También llamado ataque DoS (Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

18

PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.



➤ Concepto:

PRIVACIDAD:

Es el derecho de mantener de forma reservada o confidencial los datos de la computadora y los que intercambia con su red. Existen herramientas para garantizar la privacidad de la información: criptografía, contraseñas, firewall, etc.

CONFIDENCIALIDAD

Es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

19

PRIVACIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

➤ Protección a la privacidad.

Para proteger su privacidad e información sensible 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.



20

No existen garantías de que algunas de estas cosas no sucedan, incluso si usted toma las mejores precauciones. Sin embargo, usted puede tomar medidas para minimizar los riesgos a su computadora e información personal. Finalmente, la seguridad de su computadora depende de usted.




21

ASPECTOS ÉTICOS DE LA PROFESIÓN Y RESPONSABILIDADES


1. Propiedad Intelectual.

La propiedad intelectual, es toda creación del intelecto humano. Los derechos de propiedad intelectual protegen los intereses de los creadores al ofrecerles prerrogativas en relación con sus creaciones.



2. Plagiarismo.

Es una infracción al derecho de autor a cerca de una obra artística o intelectual de cualquier tipo, en la que se incurre cuando se presenta una obra ajena como propia u original.




22

ASPECTOS ÉTICOS DE LA PROFESIÓN Y RESPONSABILIDADES


3. Software pirata.

Es un programa que ha sido duplicado y distribuido sin autorización. Una serie de actividades se podrían considerar como piratería de software, la más común es cuando se hace múltiples copias de un programa para luego venderlas sin pagar ningún tipo de regalías al creador de dicho software.



4. Derechos de copia.

Es una limitación al derecho exclusivo que la ley concede al autor y al propietario de contenidos a hacer copias de ellos.



23



24
