

Escuela AGROTÉCNICA DE ZONDA

Docente: Profesor Víctor Daniel Peralta

Año: Segundo **División:** 1ra, 2da y 3ra **Ciclo:** Básico

Turno: Tarde

Área curricular: Informática.

Título de la propuesta: **SEGURIDAD INFORMÁTICA**

La Seguridad informática es una disciplina que se relaciona con diversas técnicas, aplicaciones y dispositivos, encargados de asegurar la integridad y privacidad de la información de un usuario, contenida en un sistema informático.

Técnicamente es imposible lograr un sistema informático 100% seguro, pero con buenas medidas de seguridad, se evitan daños y problemas, que quiera ocasionar cualquier intruso.



SEGURIDAD CON RESPECTO A LA NATURALEZA DE LA AMENAZA:

Según su naturaleza, las seguridades son dos:

SEGURIDAD FÍSICA: La que se relaciona con el Hardware, por ej. Mantenimiento eléctrico, mantenimiento anti-incendio, control de la humedad, etc.

SEGURIDAD LÓGICA: La que se refiere al Software, por ej. Aplicaciones para seguridad, herramientas informáticas, etc.

DELITO INFORMÁTICO

Un delito informático o crimen cibernético, se refiere a actividades ilícitas realizadas por medio de ordenadores o de internet, y tienen como objetivo la destrucción y el daño de computadoras, medios electrónicos y redes informáticas.



Algunos delitos informáticos son aún mayores y complejos, estos pueden incluir delitos tradicionales como el fraude, el robo, chantaje falsificación, en las cuales se ha utilizado redes informáticas. Desafortunadamente existe una gran variedad de actividades delictivas realizadas por medios informáticos, como por ejemplo:

- El ingreso ilegal a sistemas.
- La interceptación ilegal de redes.
- Interferencia de datos.
- Daños a la información (borrado, deterioro, alteración).
- Mal uso de artefactos.
- Chantajes, fraude electrónico.
- Ataque a Sistemas.
- Violentar la información confidencial.

MALWARE: “LOS PROGRAMAS MALICIOSOS”



MALWARE es la abreviatura de **Malicious Software (Software Malicioso)**, término que engloba a todo tipo de programa o código de computadora cuya función es producir inconvenientes, destrucción, daño o causar un mal funcionamiento y/o quebrantar la seguridad de un equipo o sistema informático.

HACKERS Y CRACKERS

Un **Hacker** es una persona que tiene un conocimiento profundo sobre el funcionamiento de las redes informáticas, y que por tanto puede advertir sus errores y fallas de seguridad. En general, estos suelen vulnerar los sistemas informáticos con fines de protagonismo.

Los **Crackers** también detentan sólidos conocimientos en sistemas informáticos y tratan de acceder sin autorización, aunque a diferencia de los Hackers, este tipo de intrusos suelen tener malas intenciones (daño, beneficio personal o para terceros).



A continuación describiremos algunos de los Malware que existen. Hay de diferentes tipos:

- ❖ **Los Virus:**
Los Virus informáticos son sencillamente programas maliciosos (malware) que “infectan” a otros archivos del sistema con la intención de modificarlos o dañarlos. Su nombre lo adoptan de la similitud que tienen con los archivos biológicos.
- ❖ **Los Caballos de Troya o “Trojanos”:**
Son programas que tienen una funcionalidad conocida (por ejemplo, un juego) pero además tienen una función oculta (como ser capturar las claves que escribe el usuario y mandarlas en un mensaje de correo electrónico a otra persona).
- ❖ **Los Worms o “Gusanos”:**
Se reproducen sin necesidad de interacción de los usuarios, por ejemplo, atacando los servicios de red vulnerables. Su cometido no es el de infectar ficheros, simplemente es el de reproducirse a gran velocidad, llegando así a colapsar nuestro sistema.
- ❖ **Bombas Lógicas:**

La particularidad más notoria de las bombas lógicas reside en que mientras no se cumplan ciertas condiciones, el virus no realizará ninguna acción destructiva, permaneciendo escondido al acecho de nuestros datos.

❖ **Keyloggers:**

Es una aplicación destinada a registrar todas las teclas que un usuario tipea en su computadora. Algunos registran además otro tipo de información útil, como ser imágenes de pantalla. Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados..

❖ **Spyware:**

Son aplicaciones que recogen y envían información sobre las páginas web más utilizadas por el usuario, su tiempo de conexión, los datos relativos al equipo, e incluso, hay algunos diseñados para informar si el software que utiliza el equipo es original o no. Esta información es explotada para propósitos de mercadotecnia.

❖ **BackDoors:**

Estos programas están diseñados para abrir una “puerta trasera” en nuestro sistema, de modo tal de permitir al creador de esta aplicación tener acceso al sistema y hacer lo que desee con él.

❖ **Adware:**

El Adware es software que despliega publicidad de distintos productos o servicios.

Dispositivos de Protección

Así como te vacunas para evitar enfermedades o vas al doctor periódicamente para controlar que todo esté bien, en tu PC pasa lo mismo. Una de las formas de mantenerla con buena salud es instalando un programa antivirus y también es necesario tener en cuenta elementos tales como los antispyware, Firewall, Filtros, copias de seguridad y “contraseña robustas”.

❖ **Antispyware:**

Hay muchos programas antiespía, pero uno de los mejores es SpybotSearch&Destroy. Tiene herramientas para detectar, eliminar y prevenir el Spyware en tu computadora. Todos los antispyware son muy útiles, pero debes usarlos con cierto cuidado. Ocurre que a veces, al tratar de eliminar algunos programas espías, accidentalmente se puede borrar o dañar algún archivo de Windows o de alguna otra aplicación.

❖ **Firewall:**

El Firewall o “cortafuegos” consiste en un sistema diseñado para evitar accesos no autorizados desde o hacia un equipo o red informática privada. Pueden estar implementados a nivel de hardware o software, o en combinación de ambos.

❖ **Filtros:**

Los filtros son programas o configuraciones que permiten restringir el acceso a sitios o contenidos considerados inconvenientes. Los hay de distintos tipos y algunos también funcionan como antivirus y antisпам. Estos dispositivos pueden

seleccionar contenidos, establecer horarios de uso y ofrecer registros de los sitios visitados.

❖ **Antivirus:**

Para disminuir las amenazas que presentan los códigos o programas “maliciosos”, se suele utilizar programas antivirus. Sin embargo, es importante resaltar que estos programas no son siempre efectivos, ya que suelen detectar el código malicioso en base a patrones conocidos; es decir que no detectan automáticamente los últimos desarrollos. Por eso debemos mantener nuestro antivirus actualizado.

❖ **Copias de Seguridad:**

Como medida preventiva, y ante la amenaza de programas maliciosos que pueden ingresar y dañar nuestros equipos, se recomienda realizar –con cierta regularidad– copias de seguridad (backs up) en medios externos (C.D., pendrive, etc.) que respalden la información contenida en nuestras máquinas.

❖ **Claves robustas:**

Existen algunas técnicas para formar claves “robustas”, es decir que conjugan cierta dificultad para averiguarlas, con características que permiten que los usuarios la puedan recordar fácilmente:

- No utilices palabras comunes ni nombres de fácil deducción para terceros (nombres de mascotas, nombre de equipo de fútbol favorito, etc.), ya que estas claves podrían ser obtenidas fácilmente mediante el uso de técnicas automáticas que pueden acceder a la cuenta del usuario con palabras extraídas de diccionarios de palabras comunes.
- No las vincules a una característica personal (teléfono, número de documento, patente del automóvil, etc.)
- Combiná caracteres alfabéticos, mayúsculas y minúsculas, números, caracteres especiales como espacio, guión, símbolo \$, etc.
- Crearlas utilizando al menos ocho caracteres.
- Usá un acrónimo de algo fácil de recordar. Ejemplo: NorCarTren (Norma, Carlos, Tren).
- Añadí un número al acrónimo para mayor seguridad: NorCarTren09 (Norma, Carlos, Tren, edad de su hijo/a).
- Elegir una palabra sin sentido, aunque pronunciable (galpo-glio).
- Reemplazá algunas letras por signos o números (3duar0palmit0)
- Elegí una clave que no puedas olvidar, para evitar escribirla en alguna parte (arGentina6-0).



ACTIVIDAD PARA LOS ALUMNOS**SEGURIDAD INFORMÁTICA: Cuestionario:**

- 1) ¿A qué llamamos Seguridad Informática?
- 2) ¿Cuál es la Seguridad que se refiere al Hardware y cuál al Software? Ejemplifique.
- 3) ¿Qué es un Delito informático? De al menos 5 ejemplos.
- 4) ¿A que nos referimos cuando hablamos de Malware?
- 5) Realice una diferenciación entre el concepto de “Hackers” y el concepto de “Crackers”.
- 6) Defina qué es un:
 - a) Virus.
 - b) Caballo de Troya o Troyano.
 - c) Gusanos.
 - d) Bombas Lógicas
 - e) Keyloggers.
 - f) Spyware.
 - g) Backdoors.
 - h) Adware.
- 7) ¿Qué es un Dispositivo de Protección?
- 8) A que llamamos:
 - a) Antivirus.
 - b) Antispyware.
 - c) Firewall.
 - d) Filtros.
- 9) ¿Cuál es el concepto de Copia de Seguridad o Back –up?
- 10) Describa al menos 5 técnicas para poder formar y elaborar una clave robusta.

Coordinador Nelson Ahumada– a cargo de Dirección Escuela Agrotécnica de Zonda – Depto. de Zonda.