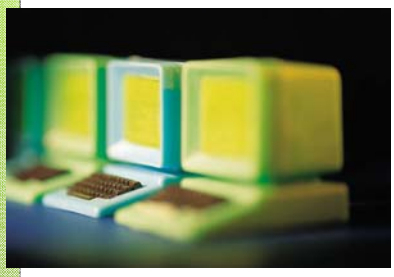

Introducción a la Seguridad Informática

Dra. Maricela Bravo

La información como activo estratégico

Recordando

¿Qué es un sistema de información?

Es el conjunto que resulta de la integración de cuatro elementos: Hardware, software, datos y usuarios.

¿Cuál es el objetivo de integrar estos componentes?

Hacer posible el procesamiento automático de los datos, mediante el uso de computadoras.

Recordando

¿Qué son datos?

Símbolos que representan hechos, situaciones, condiciones o valores. Los datos son la materia prima que procesamos para producir información.

¿Qué es la información?

El resultado de procesar o transformar los datos. La información es significativa para el usuario.

Contenido

- Conceptos de Seguridad Informática
- Principios de Seguridad Informática
- Factores de Riesgo
- Mecanismos de Seguridad Informática

Conceptos

Como consecuencia de la amplia difusión de la tecnología informática, **la información**:

Se almacena y se procesa en computadoras, que pueden ser independientes o estar conectadas a través de sistemas en red.

Puede ser confidencial para algunas personas o para instituciones completas.

No está centralizada y puede tener alto valor.

Conceptos

Como consecuencia de la amplia difusión de la tecnología informática, **la información**:

Puede utilizarse para fines poco éticos.

Puede divulgarse sin autorización de su propietario.

Puede estar sujeta a robos, sabotaje o fraudes.

Puede ser alterada, destruida y mal utilizada.

Conceptos

La **Seguridad Informática (S.I.)** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer **condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos**.

La decisión de aplicarlos es responsabilidad de cada usuario.

Las consecuencias de no hacerlo … también.

Principios de Seguridad Informática

Para lograr sus objetivos, la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

Confidencialidad

Integridad

Disponibilidad

Principios de Seguridad Informática

Confidencialidad

Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de seguridad informática deben proteger al sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados.

Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que usuarios, computadoras y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

Principios de Seguridad Informática

Integridad

Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

Este principio es particularmente importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadoras y procesos comparten la misma información.

Principios de Seguridad Informática

Disponibilidad

Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de Seguridad Informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Este principio es particularmente importante en sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente.

Factores de riesgo

Ambientales: factores externos, lluvias, inundaciones, terremotos, tormentas, rayos, suciedad, humedad, calor, entre otros.

Tecnológicos: fallas de hardware y/o software, fallas en el aire acondicionado, falla en el servicio eléctrico, ataque por virus informáticos, etc.

Humanos: hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, intrusión, alteración, etc.

Factores tecnológicos de riesgo

Virus informáticos: Definición

Un virus informático es un programa (código) que se replica, añadiendo una copia de sí mismo a otro(s) programa(s).

Los virus informáticos son particularmente dañinos porque pasan desapercibidos hasta que los usuarios sufren las consecuencias, que pueden ir desde anuncios inocuos hasta la pérdida total del sistema.

Factores tecnológicos de riesgo

Virus informáticos: Características

Sus principales características son:

Auto-reproducción: Es la capacidad que tiene el programa de replicarse (hacer copias de sí mismo), sin intervención o consentimiento del usuario.

Infección: Es la capacidad que tiene el código de alojarse en otros programas, diferentes al portador original.

Factores tecnológicos de riesgo

Virus informáticos: Propósitos

Afectar el software: Sus instrucciones agregan nuevos archivos al sistema o manipulan el contenido de los archivos existentes, eliminándolo parcial o totalmente.

Afectar el hardware: Sus instrucciones manipulan los componentes físicos. Su principal objetivo son los dispositivos de almacenamiento secundario y pueden sobrecalentar las unidades, disminuir la vida útil del medio, destruir la estructura lógica para recuperación de archivos y otras consecuencias.

Factores tecnológicos de riesgo

Virus informáticos: Clasificación

La inmensa **cantidad** de virus existentes, sus diferentes **propósitos**, sus variados **comportamientos** y sus diversas **consecuencias**, convierten su clasificación en un proceso complejo y polémico.

A continuación se presentan las categorías que agrupan a la mayoría de los virus conocidos. Sin embargo, es importante considerar que la **aparición diaria de virus** cada vez más sofisticados, puede llevar al surgimiento de nuevas categorías en cualquier momento.

Factores tecnológicos de riesgo

Virus informáticos: Clasificación

Virus genérico o de archivo: Se aloja como un parásito dentro de un archivo ejecutable y se replica en otros programas durante la ejecución.

Los genéricos acechan al sistema esperando que se satisfaga alguna condición (fecha del sistema o número de archivos en un disco). Cuando esta condición "catalizadora" se presenta, el virus inicia su rutina de destrucción.

Factores tecnológicos de riesgo

Virus informáticos: Clasificación

Virus mutante: En general se comporta igual que el virus genérico, pero en lugar de replicarse exactamente, genera copias modificadas de sí mismo.

Virus recombinables: Se unen, intercambian sus códigos y crean nuevos virus.

Virus "Bounty Hunter" (caza-recompensas): Están diseñados para atacar un producto antivirus particular.

Factores tecnológicos de riesgo

Virus informáticos: Clasificación

Virus específicos para redes: Coleccionan contraseñas de acceso a la red, para luego reproducirse y dispersar sus rutinas destructivas en todas las computadoras conectadas.

Virus de sector de arranque: Se alojan en la sección del disco cuyas instrucciones se cargan en memoria al inicializar el sistema. El virus alcanza la memoria antes que otros programas sean cargados e infecta cada nuevo disco que se coloque en la unidad.

Factores tecnológicos de riesgo

Virus informáticos: Clasificación

Virus de macro: Se diseñan para infectar las macros que acompañan a una aplicación específica.

Una macro es un conjunto de instrucciones que ejecutan una tarea particular, activada por alguna aplicación específica como MS – Word o MS – Excel.

Son virus muy fáciles de programar y se dispersan rápidamente a través de anexos a e-mail, copia de archivos usando disquetes, etc.

Factores tecnológicos de riesgo

Virus informáticos: Clasificación

Virus de Internet: Se alojan en el código subyacente de las páginas web. Cuando el usuario accede a esos sitios en Internet, el virus se descarga y ejecuta en su sistema, pudiendo modificar o destruir la información almacenada.

Son de rápida y fácil dispersión, puesto que se alojan y viajan en un medio de acceso multitudinario: Internet.

Factores humanos de riesgo

Hackers

Los hackers son personas con avanzados conocimientos técnicos en el área informática y que enfocan sus habilidades hacia la invasión de sistemas a los que no tienen acceso autorizado.

En general, los hackers persiguen dos objetivos:

- **Probar que tienen las competencias para invadir un sistema protegido.**
- **Probar que la seguridad de un sistema tiene fallas.**

Factores humanos de riesgo

Crackers

Los crackers son personas con avanzados conocimientos técnicos en el área informática y que enfocan sus habilidades hacia la invasión de sistemas a los que no tienen acceso autorizado.

En general, los crackers persiguen dos objetivos:

- **Destruir parcial o totalmente el sistema.**
- **Obtener un beneficio personal (tangible o intangible) como consecuencia de sus actividades.**

Mecanismos de Seguridad Informática

Conceptos

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático.

Existen muchos y variados mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan.

Mecanismos de Seguridad Informática

Clasificación según su función

Preventivos: Actúan **antes de que un hecho ocurra** y su función es **detener** agentes no deseados.

Detectivos: Actúan **antes de que un hecho ocurra** y su función es **revelar** la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.

Correctivos: Actúan **luego de ocurrido el hecho** y su función es **corregir** las consecuencias.

Mecanismos de Seguridad Informática

Ejemplos orientados a fortalecer la confidencialidad

Encripción o cifrado de datos: Es el proceso que se sigue para **enmascarar los datos**, con el objetivo de que sean incomprensibles para cualquier agente no autorizado.

Los datos se enmascaran usando una **clave especial** y siguiendo una secuencia de pasos pre-establecidos, conocida como "**algoritmo de cifrado**". El proceso inverso se conoce como descifrado, usa la misma clave y devuelve los datos a su estado original.

Mecanismos de Seguridad Informática

Ejemplos orientados a fortalecer la integridad

Software anti-virus: Ejercen control preventivo, detectivo y correctivo sobre ataques de virus al sistema.

Software "*firewall*": Ejercen control preventivo y detectivo sobre intrusiones no deseadas a los sistemas.

Software para sincronizar transacciones: Ejercen control sobre las transacciones que se aplican a los datos.

Mecanismos de Seguridad Informática

Ejemplos orientados a fortalecer la disponibilidad

Planes de recuperación o planes de contingencia: Es un esquema que especifica los pasos a seguir en caso de que se interrumpa la actividad del sistema, con el objetivo de recuperar la funcionalidad.

Dependiendo del tipo de contingencia, esos pasos pueden ejecutarlos personas entrenadas, sistemas informáticos especialmente programados o una combinación de ambos elementos.

Mecanismos de Seguridad Informática

Ejemplos orientados a fortalecer la disponibilidad

Respaldo de los datos: Es el proceso de copiar los elementos de información recibidos, transmitidos, almacenados, procesados y/o generados por el sistema.

Existen muchos mecanismos para tomar respaldo, dependiendo de lo que se quiera asegurar. Algunos ejemplos son: Copias de la información en dispositivos de almacenamiento secundario, computadoras ejecutando las mismas transacciones en paralelo , etc.

Mecanismos de Seguridad Informática

Seguridad física

¿Qué debemos proteger?

Todos los dispositivos que componen el hardware: Procesador, memoria principal, dispositivos de entrada y de salida, dispositivos de almacenamiento ...

... y los respaldos

Mecanismos de Seguridad Informática

Seguridad física

¿Cómo? (Algunos ejemplos)

- **Restringir el acceso a las áreas de computadoras**
- **Restringir el acceso a las impresoras**
- **Instalar detectores de humo y extintores (fuego)**
- **Colocar los dispositivos lejos del piso (agua)**
- **Colocar los dispositivos lejos de las ventanas (lluvia)**
- **Colocar pararrayos (rayos)**
- **Proteger las antenas externas (vientos)**

Tarea

- Investigar al menos tres ejemplares de virus informáticos de las clasificaciones vistas.
- Entregar un reporte en PDF por correo.