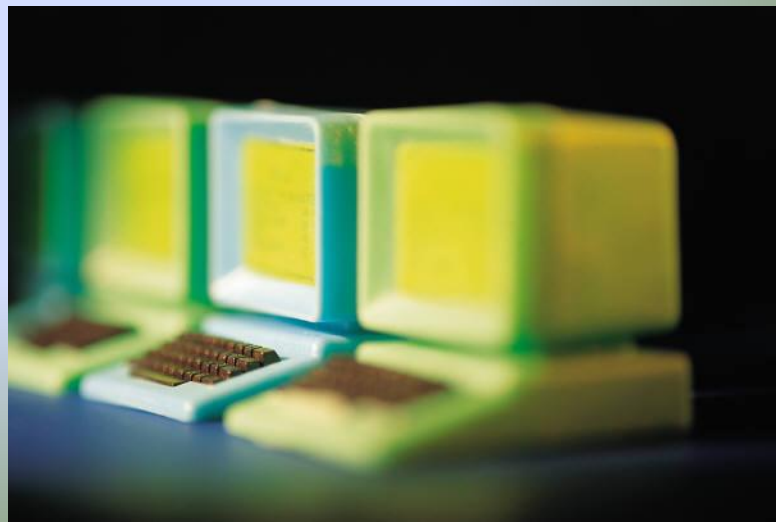
JAIME ANDRES GUACARAPARE
Tecnologia en Desarrollo de Software

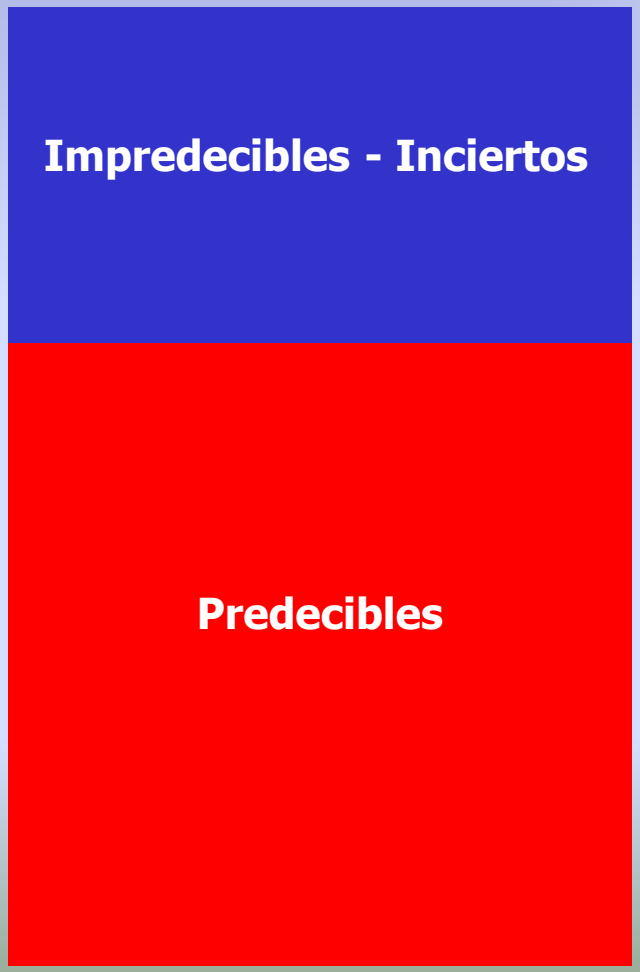
TEMA: SEGURIDAD INFORMÁTICA

La información como activo estratégico



Tema: Seguridad informática

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.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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 (FAT) y otras consecuencias.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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 todos los ordenadores conectados.

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 disquete que se coloque en la unidad.

Introducción a la Computación
Tema: Seguridad informática

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.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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.**

Tema: Seguridad informática

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.**

Tema: Seguridad informática

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.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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.

Tema: Seguridad informática

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, ordenadores paralelos ejecutando las mismas transacciones, etc.

Tema: Seguridad informática

Mecanismos de Seguridad Informática

Un mecanismo correctivo para factores de riesgo humano: Sanciones legales.

La legislación española se ocupa de sancionar a las personas que incurran en cualquier delito relacionado con sistemas informáticos a través de la

Ley Especial Contra Delitos Informáticos