SEGURIDAD INFORMATICA 2020
DELITOS IN FORMATICOS

Tipos de delitos informáticos más comunes

Los delitos informáticos los podríamos clasificar en :

- **Ataques contra el derecho a la intimidad:** Este tipo de delito informático es el descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados de ficheros informáticos privados.
- **Infracciones a la Propiedad Intelectual:** Se trata de proteger la Propiedad Intelectual de cualquier tipo de ataque informático a través de los derechos de autor. Se castigan acciones como la reproducción, distribución, plagio y otras prácticas relacionadas en obras literarias o de cualquier tipo sin la autorización del titular de los derechos de autoría.
- **Falsedades**: Posesión o creación de programas para cometer delitos de falsedad. Es la elaboración de documentos o medios de pago falsos. Las nuevas tecnologías han hecho que existan cada vez más maneras de delinquir de esta forma.

- **Sabotajes informáticos**: Supone destruir o hacer desaparecer información de bases de datos, equipos, soportes, etc. con la finalidad de suspender o paralizar una actividad laboral.
- **Fraudes informáticos**: Cometer estafa a través de la manipulación de datos o programas con un fin lucrativo. Se puede realizar a través de la piratería informática accediendo a un ordenador con información confidencial.
- **Amenazas**: Pueden realizarse desde cualquier medio de comunicación. Pueden ser también calumnias e injurias

además de amenazas. Realizar una calumnia es acusar falsamente a otra persona de haber cometido un delito. La injuria supone la deshonra o el descrédito, utilizando argumentos falsos sobre otra persona.

- **Pornografía infantil:** Cualquier tipo de acción que apoye la pornografía de menores. Distribución, venta posesión, etc. de material pornográfico en el que aparezcan menores o incapaces.
- **La inducción de menores a la prostitución.**

Delitos informáticos: Problemas de seguridad

- **Caballo de Troya**: Éste es un programa malicioso que se presenta como algo inofensivo al usuario, pero al ejecutarlo se generan daños en el sistema. Crean una puerta trasera que permite que un usuario no autorizado lo administre remotamente.
- **Puerta trasera**: Se envían de forma oculta a través de programas, normalmente en caballos de Troya. Suponen una brecha en un sistema de seguridad.
- **Bomba lógica**: Es una inserción de código en un programa informático que solo actúa de forma maliciosa si se cumplen una serie de condiciones.
- **Desbordamiento de pila y búfer:** Es un error de software que se produce cuando un atacante envía más datos de los que el programa está esperando. Se utiliza para acceder ilícitamente a un sistema.
- **Virus**: Son una inserción de código malintencionada que puede provocar problemas de seguridad. Existen millones de virus distintos y pueden realizar infinidad de acciones dentro del sistema.

- **Gusanos**: Es un proceso que utiliza un sistema de reproducción para afectar negativamente al rendimiento del sistema. El gusano crea copias de si mismo con recursos del sistema para impedir que otros procesos operen. Son muy peligrosos ya que pueden pasar a otro sistema y afectar a una red completa.
- **Escaneo de puertos**: Más que un ataque es un procedimiento para detectar vulnerabilidades del sistema. Se suele llevar a cabo de forma automatizada.
- **Denegación del servicio**: Se realizan a través de la red y lo que hacen principalmente es: Consumir recursos del sistema para que no se pueda trabajar en él o hacer caer la red.

Delitos informáticos para protegernos debemos:

- Tener siempre el **software actualizado** ya que los atacantes se aprovechan de las vulnerabilidades de un sistema. Descarga también los parches de seguridad para brechas de software del fabricante.
- **Utiliza firewall**: Se utiliza para mantener la conexión a internet lo más segura posible. Es un programa informático que controla el acceso de un ordenador a la red y a los elementos peligrosos de ésta.
- **Instalar un antivirus de calidad.** Este te protegerá de este tipo de elementos maliciosos mediante análisis constantes del sistema. Es recomendable que elijas un antivirus conocido ya que hay ciertos antivirus que no son realmente lo que dicen ser y podrían atacar tu ordenador.

Delitos informáticos ¿Cómo proteger un sistema?

Para proteger adecuadamente un sistema informático de delitos informáticos, se debe adoptar medidas de seguridad en cuatro niveles:

- **Físico**: En este ámbito son importantes dos tipos de medidas: los mecanismos de detección (sensores de calor, detectores de humos, etc.) y los sistemas de detección (huellas digitales, reconocimiento de vos, tarjetas, etc.)
- **Humano**: La autorización de los usuarios adecuados al sistema y el acceso al mismo.
- **Sistema operativo**: Autoprotección ante futuros peligros y fallos de seguridad informática.
- **La red**

Medidas para evitar delitos informáticos

- Cambie de contraseñas periódicamente y hazlas cada vez más complicadas: Tener la misma contraseña para cada suscripción es un auténtico peligro ya que si descubren una tendrán acceso a todas. Cuanto menos previsible sea más opciones tendrás de que esta no sea descubierta. Se recomienda cambiarlas además cada poco tiempo.
- Cierre sesión en todas sus cuentas al terminar de utilizarlas, sobre todo si comparte ordenador con otras personas.
- Instale un antivirus: Al igual que para prevenir el ataque de troyanos, el antivirus es una herramienta fundamental para su ordenador.

- Utilice un firewall o cortafuegos para tener un acceso seguro a internet.
- No realice transacciones en redes públicas. Por ejemplo, si se va de viaje y se ve en la necesidad de comprar un billete no lo haga en la red Wifi del hotel ya que podían intentar entrar en sus cuentas bancarias. Utiliza servidores VPN o de red privada más segura o páginas https.
- Realice copias de seguridad.
- Desconéctese de internet cuando no lo necesite.