DELITOS RELACIONADOS CON CIBERSEGURIDAD

Los avances tecnológicos han traído consigo un considerable aumento de los casos de delito en informática.

Fraudes que plantean desafíos únicos para la aplicación de la ley, que constantemente se ve obligada a adaptarse a nuevas formas de ciberdelincuencia.
En gran medida debido a la complejidad de los métodos empleados por los infractores.

Que es un delito informatico?

Un delito informático es cualquier actividad ilegal que involucre el uso de sistemas informáticos o redes, pudiendo abarcar desde intrusiones maliciosas hasta el robo de datos, la manipulación de información online, el acoso cibernético, la difamación online o la violación de la privacidad.

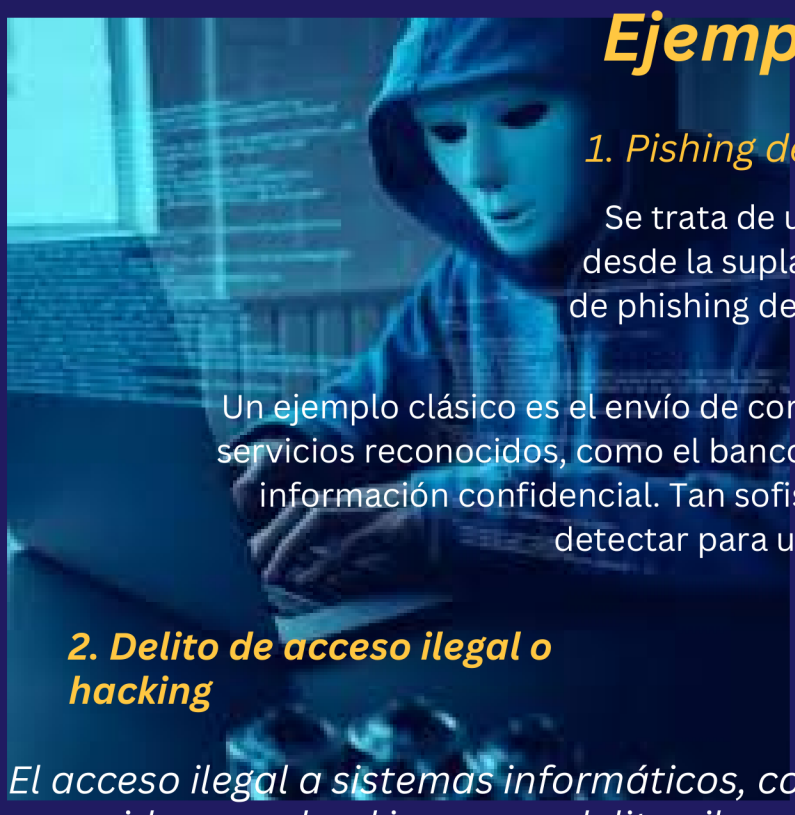
Quien regula los delitos informaticos?

Ley 1273 de 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

Tipos de delitos informáticos

La variedad y sofisticación de los delitos tecnológicos desafían constantemente la seguridad en Internet. Por eso, es fundamental entender cuáles son las diferentes amenazas que acechan en el ciberespacio para poder fortalecer nuestras defensas.



Ejemplos

1. Pishing de ingeniería social

Se trata de un fraude en informática que puede abarcar desde la suplantación de identidad online hasta esquemas de phishing destinados a engañar a los usuarios para revelar información confidencial.

Un ejemplo clásico es el envío de correos electrónicos falsos que aparentan ser de servicios reconocidos, como el banco o la compañía de la luz, en los que se solicita información confidencial. Tan sofisticados que incluso llegan a ser difíciles de detectar para usuarios experimentados.

2. Delito de acceso ilegal o hacking

El acceso ilegal a sistemas informáticos, comúnmente conocido como hacking, es un delito cibernético que puede tener consecuencias muy graves.

Un ejemplo habitual es el ataque a bases de datos gubernamentales, donde los hackers pueden obtener información sensible y llegar incluso a comprometer la seguridad nacional.

3. Delitos contra la propiedad intelectual

Es otro tipo de delito informático que ha ido ganando relevancia en los últimos años. Los ciberdelincuentes pueden copiar, distribuir o robar elementos relacionados con la propiedad intelectual, como software, diseños o datos exclusivos, generando pérdidas significativas tanto a particulares como a empresas.

Los ejemplos más habituales incluyen la piratería de software y la distribución no autorizada de contenidos protegidos por derechos de autor, afectando principalmente a la industria del entretenimiento y de la tecnología.

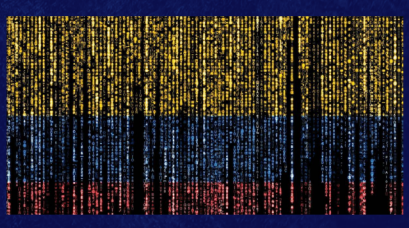
4. Ataques de denegación de servicio (DDoS)

Estos delitos cibernéticos tienen por objetivo incapacitar servicios online inundándolos con tráfico falso. Debido a ello, grandes plataformas y páginas web pueden ser inutilizados temporalmente, como ha ocurrido en algunas ocasiones en ataques a servicios financieros gubernamentales.

5. Amenazas de sextorsión

Los delincuentes amenazan con revelar información comprometedora, como imágenes íntimas, a menos que se pague un rescate. Este tipo de delito afecta la privacidad y la seguridad emocional de las víctimas.

Qué es ‘ransomware’?



El ransomware es un tipo de software malicioso que cifra la información de manera que los usuarios autorizados no pueden hacer uso de ella. El ciberdelincuente pide un rescate en criptomonedas (para no ser rastreado) con la promesa de entregarles la clave que les permita hacer uso nuevamente de la información.

Cómo funciona?

Funciona haciendo un pago con una criptomoneda, así que la víctima debe crear un monedero digital y comprar criptomonedas para transferirlas al atacante. Las indicaciones las muestra la misma pantalla de bloqueo que genera el ransomware donde informa que ha sido atacado y qué debe hacer para recuperar la información. En muchos casos de uso de ransomware, la información sigue estando en los dispositivos de la víctima, solo que al estar cifrada no la puede utilizar.

Consejos de Ciberseguridad

PROTEGE LOS DATOS

Eres responsable de la informacion que manejas!

01 UTILIZA CONTRASEÑAS SEGURAS

No cambies contraseñas sin autorizacion, utiliza solo claves controladas por la oficial de datos personales

02 NO GUARDES INFORMACION EN LUGARES NO AUTORIZADOS

Toda informacion debe ser guardada e el servidor, para mantener copias de respaldo en caso de perdida de informacion.

03 EVITA CONECTARTE A REDES WIFI PÚBLICAS

Mejor utiliza una red privada virtual (VPN) para mantener tu información segura.

04 NO REVELES INFORMACIÓN PERSONAL

Tus datos personales pueden usarse para el robo de identidad.

05 ANTE UN CORREO SOSPECHOSO!

- No abra ningun enlace.
- No eliminar el correo.
- Reportar inmediatamente al oficial de tratamiento de datos