- Programa : Control de la seguridad Digital
- Ficha:  2912068

- Ciberseguridad: Concepto, Generalidades.

Ciberseguridad: La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos



## SE DIVIDEN EN ALGUNAS CATEGORÍAS COMUNES.

- La **seguridad de red** es la práctica de proteger una red informática de los intrusos, software que restringe el ingreso de intrusos a al red.
- A tener en cuenta: Cambiar el usuario y la clave periódicamente, apagar o desconectar el ruoter wifi  o cable de red cuando no este en casa, actualizar los sistemas operativos y utilizar cortafuegos que son aplicaciones que previene a que posibles intrusos entren a nuestra red .
- La **seguridad de las aplicaciones** se enfoca en mantener el software y los dispositivos libres de amenazas.
- A tener en cuenta: no instalar aplicaciones desconocidas, aplicaciones que soliciten sus datos personales como numero de identidad, fotocopias de identidad, verificación de rostro, números de tarjeta de crédito.
- La **seguridad de la información** protege la integridad y la privacidad de los datos.
- Ley de Protección de Datos Personales o Ley 1581 de 2012. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento

## Tipos de ciberamenazas

El **delito cibernético** incluye agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros.

EJEMPLOS: El phishing es un delito informático que consiste en engañar a una persona para que proporcione información confidencial, como contraseñas, números de tarjetas de crédito o información personal. Los ciberdelincuentes suelen enviar correos electrónicos o mensajes de texto fraudulentos que parecen provenir de una fuente legítima, como un banco, una empresa o una institución gubernamental.

**Malware:** El malware puede utilizarse para robar datos, dañar sistemas informáticos o cometer otros delitos.

- **Virus:** Un virus es un tipo de malware que se replica y se propaga a otros sistemas informáticos.
- **Troyano:** Un troyano es un tipo de malware que se disfraza de software legítimo para engañar a los usuarios para que lo descarguen o ejecuten.
- **Worm:** Un gusano es un tipo de malware que se propaga a través de las redes.
- **Adware:** El adware es un tipo de malware que muestra anuncios no deseados en los navegadores web.
- **Spyware:** El spyware es un tipo de malware que recopila información personal sin el consentimiento del usuario.

Los **ciberataques**

El **ciberterrorismo** tiene como objetivo debilitar los sistemas electrónicos para causar pánico o temor.

buscan obtener ganancias financieras mediante el robo de dinero, el robo de datos o la interrupción del negocio. Los ciberdelincuentes pueden piratear una cuenta bancaria para robar dinero directamente o utilizar estafas de ingeniería social para engañar a las personas para que les envíen dinero. Los piratas informáticos pueden robar datos y utilizarlos para cometer robos de identidad o venderlos.

**sextorsión** es cuando un agresor accede a imágenes o videos íntimos de una víctima sin su consentimiento. Una vez que el agresor tiene las imágenes o videos, la amenaza con publicarlas o compartirlas si no cumple con sus demandas.

- **Consejos para protegerse de la sextorsión**

- **No envíe imágenes o videos íntimos de usted mismo a nadie que no conozca bien.**
- **Sea consciente de las personas con las que habla en línea.**
- **No haga clic en enlaces o abra archivos adjuntos de personas que no conoce.**
- **Actualice su software antivirus y firewall regularmente**
- **Estafa:** Una estafa es un engaño diseñado para robar dinero o información personal. Las estafas en línea pueden ser muy sofisticadas y pueden ser difíciles de detectar.
- **Ciber espionaje:** El ciber espionaje es la recopilación de información confidencial de una persona o empresa sin su consentimiento. El ciber espionaje puede utilizarse para obtener información comercial, robar secretos industriales o incluso chantajear a la víctima.
- **Ciberbullying:** El ciberbullying es el acoso o intimidación de una persona a través de Internet o de las redes sociales. El ciberbullying puede tener un impacto devastador en la víctima, tanto emocional como psicológicamente
- **El ciberacoso** es un delito que se comete a través de medios electrónicos, como internet, redes sociales, teléfonos móviles o videojuegos online. Se trata de cualquier acto o comportamiento de hostigamiento, intimidación, avergonzar, humillar, amenazar, agresión o abuso que se produzca a través de estos medios.

- **. Robo de identidad**: ocurre cuando alguien roba información personal y la usa para cometer un delito o fraude. Alguien puede usar tu número de seguro social para solicitar beneficios por desempleo, hacerse pasar por ti en línea o usar tu información para obtener acceso a las cuentas bancarias. El fraude con tarjetas de débito o crédito es una de los robos de identidad más frecuentes.

- **Ransomware**: es una forma de malware que bloquea dispositivos, redes y documentos importantes hasta que la víctima paga un rescate. Las personas que utilizan ransomware suelen dirigirse a organizaciones como hospitales y bufetes de abogados que no pueden permitirse el lujo de separarse de su tecnología ni siquiera durante un breve período de tiempo.

- **9. Pornografía infantil**: es uno de los delitos cibernéticos más monstruosos. Son imágenes de niños involucrados en actividades sexuales y que se comercializan en Internet las 24 horas del día. Los pornógrafos infantiles utilizan la facilidad de distribución de Internet para vender su material a pedófilos (adultos que se sienten atraídos sexualmente por los niños).
- **10. Qué es grooming?**
- La persona acosadora suele crear un perfil falso en redes sociales, aplicaciones, videojuegos multijugador u otro medio social. Se hace pasar por una persona menor de edad para generar confianza y tener una relación de amistad con niñas, niños o adolescentes.

# BIBLIOGRAFIA


- https://miconsultoriolegal.com/10-delitos-informaticos-en-colombia-protegete-en-la-era-digital/
- https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security