NOMBRE DEL DOCENTE: NATIVIDAD RÍOS **FECHA:**
CORREO: natividad.rios@medellin.edu.co **WHATSAPP:** 3054851130
AREA: TECNOLOGÍA E INFORMÁTICA **GRADO:** NOVENO **GRUPO:** 9°1, 9°2
NOMBRE DEL ALUMNO_____

TALLER # 10

¿QUE SON LOS DELITOS INFORMÁTICOS?

Los DELITOS INFORMÁTICOS son todos aquellos actos que permiten los agravios, daños o perjuicios en contra de las personas, grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio del uso de las computadoras y a través del mundo virtual del Internet.

Estos DELITOS INFORMÁTICOS no necesariamente pueden ser cometidos totalmente por estos medios, sino también a partir de los mismos.

Por otro lado, otros de los muchos ataques que pueden ser dañinos y hasta resultar destructivos siendo realizados por medio de las computadoras y en algunas ocasiones con la ayuda de terceros, estos son algunos casos para mencionar:

- Claves programáticas espías: conocidas como troyanos.
- Estafas a través de subastas en línea.
- Divulgación indebida de contenidos
- Pornografía infantil en Internet
- Violación a los derechos de autor
- Piratería en Internet.

Glosario sobre algunos de los delitos informáticos más comunes

Bluejacking: Es cuando se usan teléfonos celulares con tecnología Bluetooth para enviar mensajes anónimos a otros teléfonos.
Bluesnarfing: Es el acceso no autorizado a la información guardada en teléfonos celulares, computadores y tabletas electrónicas (fotos, vídeos, lista de contactos, mensajes de texto) usando una conexión de Bluetooth.
Ciberacoso (cyberbullying): Es un tipo de agresión psicológica que se da usando las nuevas tecnologías: teléfonos celulares e Internet. Por medio de correos, mensajes o imágenes que se envían se busca herir o intimidar a otra persona. Este tipo de acoso no se hace de frente, por ello la víctima desconoce la identidad de su agresor.
ESCNNA: Explotación Sexual Comercial de Niños, Niñas y Adolescentes.
Flaming: Es cuando una discusión que se lleva a cabo en línea (en correos electrónicos, redes, blogs o foros) toma un tono insultante, burlón o desagradable hacia una de las personas con el objetivo de enojarla e imponer los puntos de vista de la otra.
Grooming: Cuando un posible abusador o pedófilo trata de iniciar una relación en línea con un menor de edad, buscando involucrarlo en actos sexuales, intercambio de imágenes y en conversaciones con contenido sexual.
Hackear: Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.
Hacker: Es un experto informático especialista en entrar en sistemas ajenos sin permiso, con frecuencia para mostrar la baja seguridad de estos o simplemente para demostrar que es capaz de hacerlo.
Hacking: Es la acción de "robar" sistemas informáticos y redes de telecomunicación.
Malware: Programa creado con el fin de molestar o dañar los computadores que lo tienen instalado.
Pharming: Es un tipo de fraude que consiste en suplantar los nombres de dominio de la página que quiere navegar el usuario, para conducirlo a una página web falsa.
Phishing: Es un delito cibernético con el que por medio del envío de correos se engaña a las personas invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales. Allí se solicita que verifique o actualice sus datos con el fin de robarle sus nombres de usuarios, claves personales y demás

información confidencial.

Pornografía infantil: Es toda representación visual, gráfica, de texto, dibujos animados o videojuegos, que, de manera real o simulada, explícita o sugerida, involucran la participación de menores de edad o personas que aparenten serlo, en el desarrollo de actividades sexuales.

Sexting: Es cuando alguien toma una foto poco apropiada de sí mismo (sugestiva o sexualmente explícita), y la envía a alguien vía teléfono celular o Internet.

Sextorsión: Es la amenaza de enviar o publicar imágenes o vídeos con contenido sexual de una persona. Esto puede hacerse a través de teléfonos celulares o Internet.

Smishing: Es una variante del phising, pero a diferencia de este, usa mensajes de texto para engañar a los usuarios, Pidiéndoles información privada e invitándolos a que se dirijan a sitios web falsos que tienen spywares y softwares maliciosos que se descargan automáticamente, sin que el usuario lo note.

Software Espía o Spyware: Programa maligno que recolecta información privada de un computador. Generalmente, para robar la información no se necesita usar el computador, y el dueño de este no lo nota.

Virus: Programa que puede alterar o destruir el funcionamiento del computador. Normalmente ocurre sin el permiso o conocimiento del usuario.

Vishing: Similar al phising, pero con teléfonos. Consiste en hacer llamadas telefónicas a las víctimas, en las que, por medio de una voz computarizada, muy similar a las utilizadas por los bancos, se solicita verificar algunos datos personales e información bancaria.

ACTIVIDADES

1. Consulta cual es la ley de delitos informáticos en Colombia
2. Alguna vez has sido víctima cibernética, Justifica tu respuesta.
3. Realiza una cartelera en tu cuaderno sobre las medidas que se deben de tener en cuenta para no ser víctima de un delito informático.
4. Realiza un crucigrama sobre delitos informáticos.
5. Consulta 5 normatividad sobre delitos informáticos en Colombia