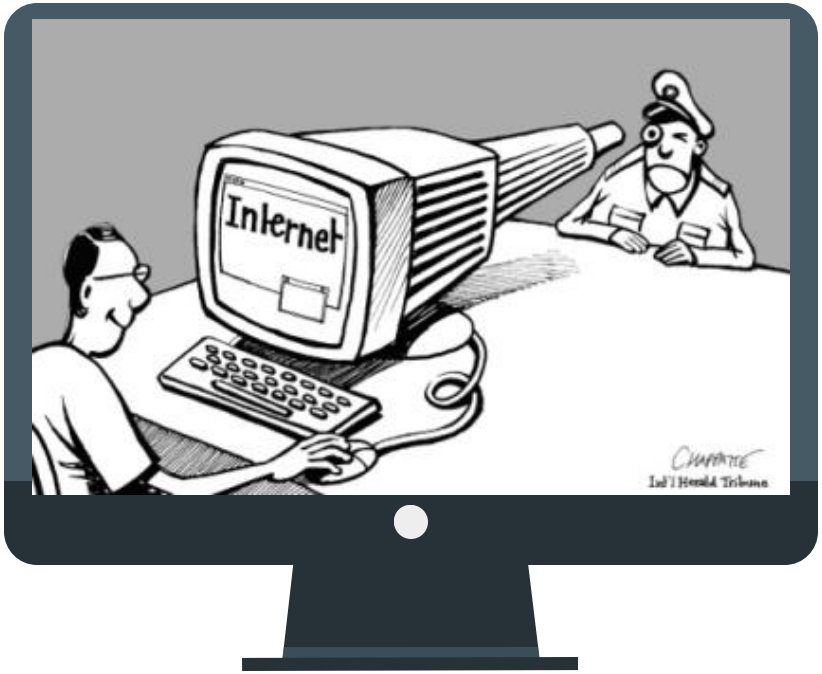
Tema 4. Ciberseguridad

- *Conocer los diferentes riesgos existentes en el internet, y que representen una amenaza para los usuarios.*
- *Conocer las mejores técnicas que se tienen al alcance para proteger la privacidad de los datos durante la navegación en internet.*
- *Utilizar de forma adecuada las herramientas de seguridad informática para minimizar los riesgos a los cuales se exponen en Internet.*

¿Qué es la ciberseguridad?



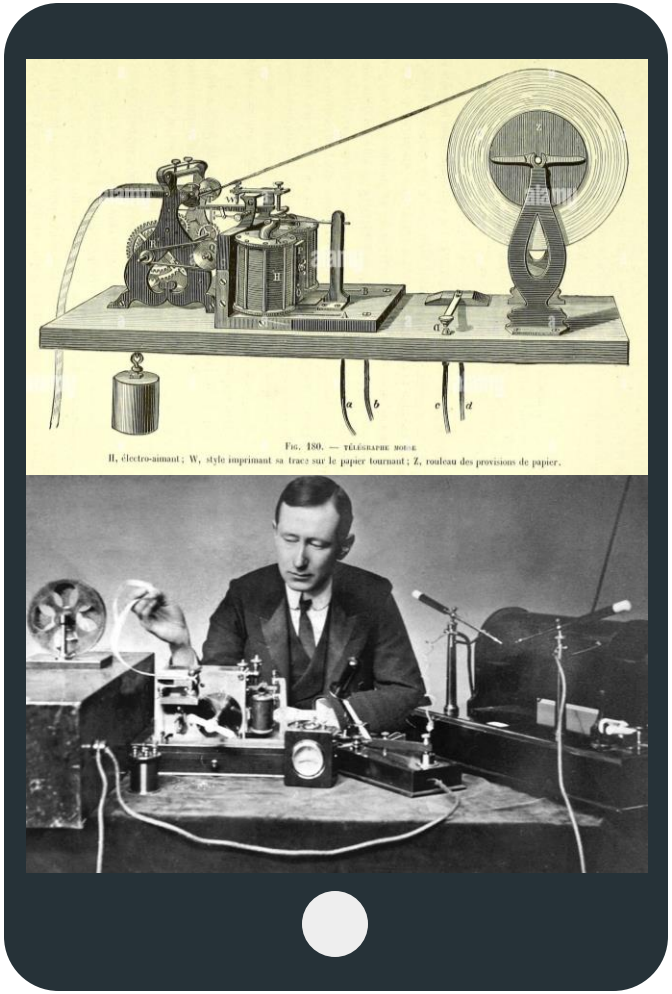
Ciberespionaje

El espionaje ha estado presente desde el inic
de la humanidad, lo cual ha implicado el acces
a la información de las actividades de persona
ciudades y países. Entre los métodos ma
antiguos del espionaje está la presencia d
cifrado y ocultamiento de información usand
códigos secretos.

Ciberespionaje

La llegada del telégrafo y la radio marcaron la evolución de las comunicaciones, y con ello; los procedimientos de intercepción y cifrado de la información; estos procesos van de la mano con el espionaje.

El ejemplo más significativo de esta evolución lo indica la máquina *Enigma*, que fue utilizada en la Segunda Guerra Mundial por el ejército alemán.



¿Qué es la Ciberseguridad?

Según la bSecure Conferenced, es “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados

¿Qué es la Ciberseguridad?

https://www.youtube.com/watch?v=odYdO3B_saE

Estadísticas de uso de Internet en Ecuador

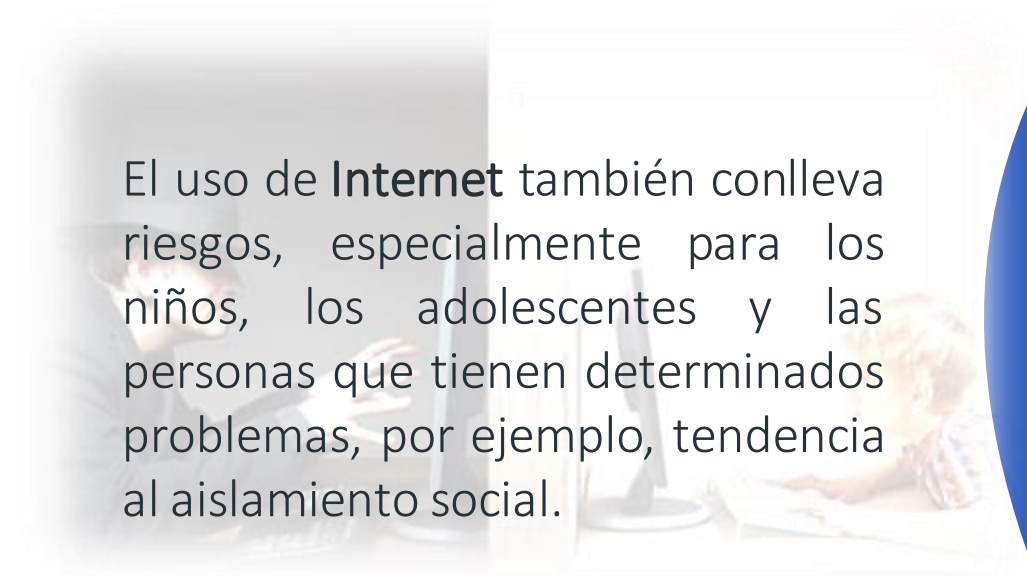
El Instituto Nacional de Estadística y Censos (INEC) como ente rector de la producción de información estadística oficial del Ecuador, desarrolló una encuesta "Nacional Multipropósito de Hogares (Seguimiento al Plan Nacional de Desarrollo)" – Encuesta Multipropósito.

Este estudio realizado con una muestra de 12072 viviendas distribuidas a nivel nacional, reflejó que el principal indicador de Tecnología de la Información y Comunicación (TIC) es el uso del internet en personas mayores a 5 años (INEC, 2020).

Tipo de encuesta	Encuesta por muestreo probabilístico
Periodo de levantamiento	Diciembre 2020
Cobertura geográfica	Nacional Urbana/Rural
Población objetivo	Población de 5 años y más.
Muestra total	12.060 viviendas

¿Que son los riesgos en internet?

El uso de **Internet** también conlleva riesgos, especialmente para los niños, los adolescentes y las personas que tienen determinados problemas, por ejemplo, tendencia al aislamiento social.



Riesgos en internet asociados con la comunicación personal

Riesgos activos en el us internet

Los riesgos activos son las acciones vol conductas conflictivas que pueden ser nocivas usuarios involucrados, por ejemplo:

- *Propagación de malware.*
- *Apropiación fraudulenta de datos pers*
- *Pornografía infantil.*
- *Acoso sexual.*
- *Búsqueda y acceso a sitios con conten drogas, pornografía, apuestas online y descarga de archivos infectados con v malware.*

Riesgos pasivos en el uso del internet

s riesgos pasivos son aquellos que olucran a menores en el uso de internet sin ervisión adulta, por ejemplo:

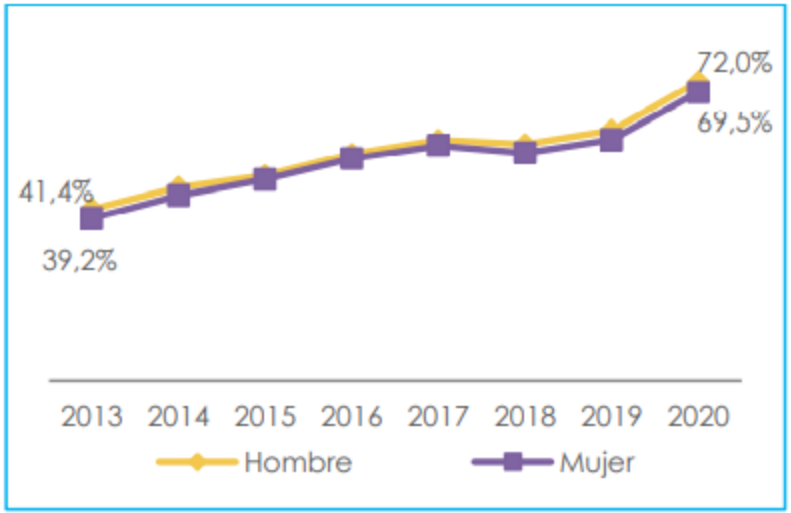
olescentes o personas adultas.

- *Consumo de contenidos potencialmente nocivos como pornografía.*
- *Violencia y situaciones humillantes como racismo, conductas alimentarias disfuncionales como la anorexia o bulimia.*
- *Ciberbullying.*
- *Acoso sexual.*

Estadísticas de uso de internet en Ecuador

Porcentaje de personas que utilizan internet, por sexo

HOMBRE



MUJER

En la siguiente muestra que fue tomada en el año 2020 indica que el 72% de los hombres utilizó internet a diferencia del 69,5% de las mujeres, como se puede evidenciar que el uso del internet entre hombre y mujeres es solo del 2.5%.

Lugar de uso del internet, por área

Lugar de uso de Internet a nivel nacional	2019	2020	Variación significativa 2019 y 2020
Hogar	68,1%	86,1%	Si
Trabajo	11,7%	6.5%	Si
Institución Educativa	5,1%	0.4%*	-
Centros de acceso público	9,0%	1,9%	Si
Casa de otra persona	4,5%	4,6%	No
Otros	1,5%	0.3%*	-

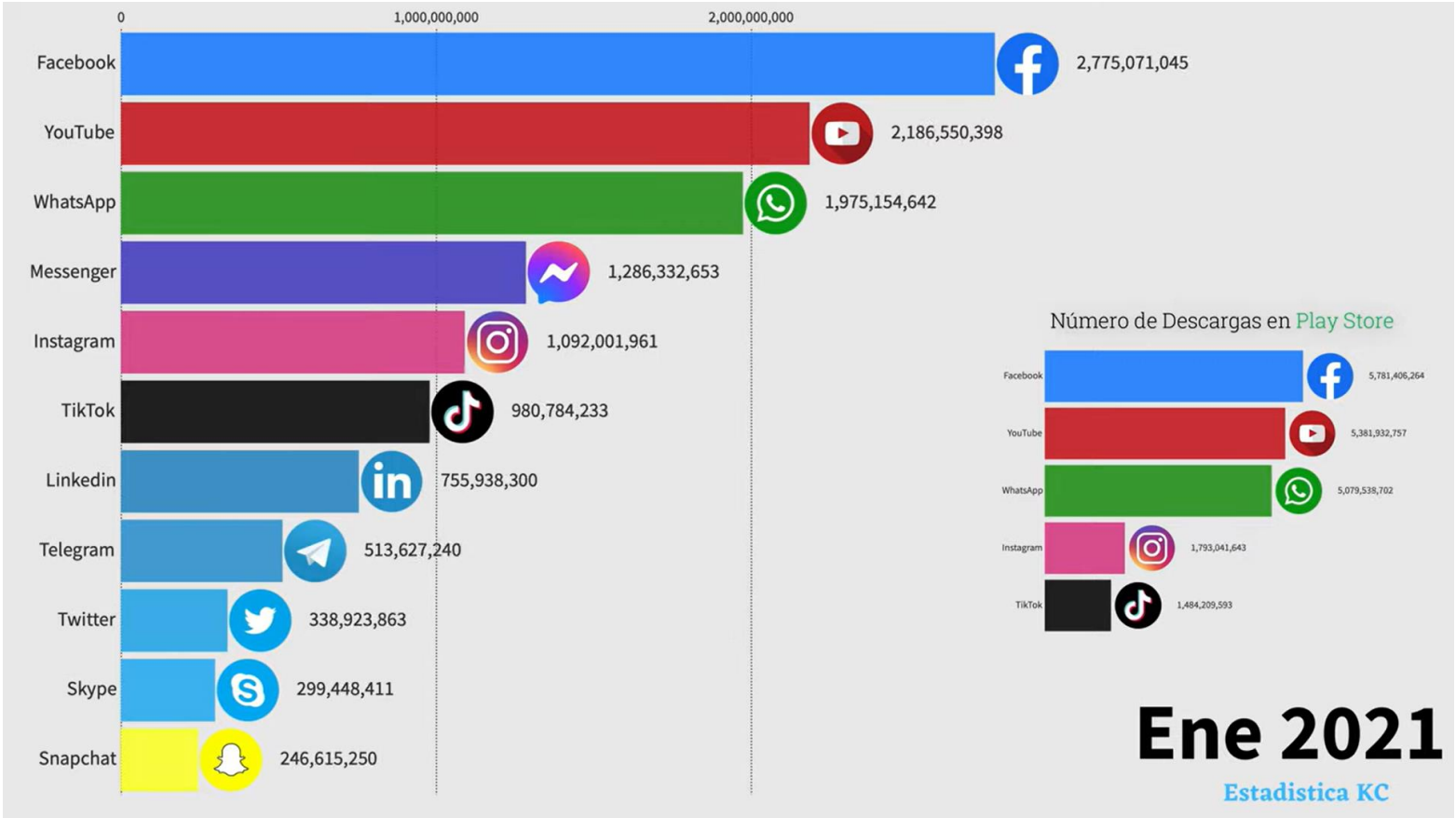
En la siguiente tabla se muestra la variación entre el periodo 2019 y 2020, del lugar de mayor uso de internet a nivel nacional. La mayor variación se visualiza en la categoría hogar con un incremento del 18% respecto al 2019.

Lugar de uso del internet a nivel nacional

Frecuencia de uso del Internet	2019	2020	Variación significativa 2019 y 2020
Al menos una vez al día	86,0%	92.1%	Si
Al menos una vez a la semana	11,8%	6.7%	Si
Al menos una vez al mes o al año	2,1%	1.0%	Si

La siguiente tabla indica la variación en el periodo 2019 y 2020 de la frecuencia de uso de internet a nivel nacional. Las personas que usan internet al menos una vez al día incrementa 6,1% mientras que las que utilizan al menos una vez a la semana disminuyen 5,1% (INEC, 2020).

Estadística de redes sociales con más usuarios en el mundo



Fuente: https://www.youtube.com/watch?v=dFRPltzDpgg

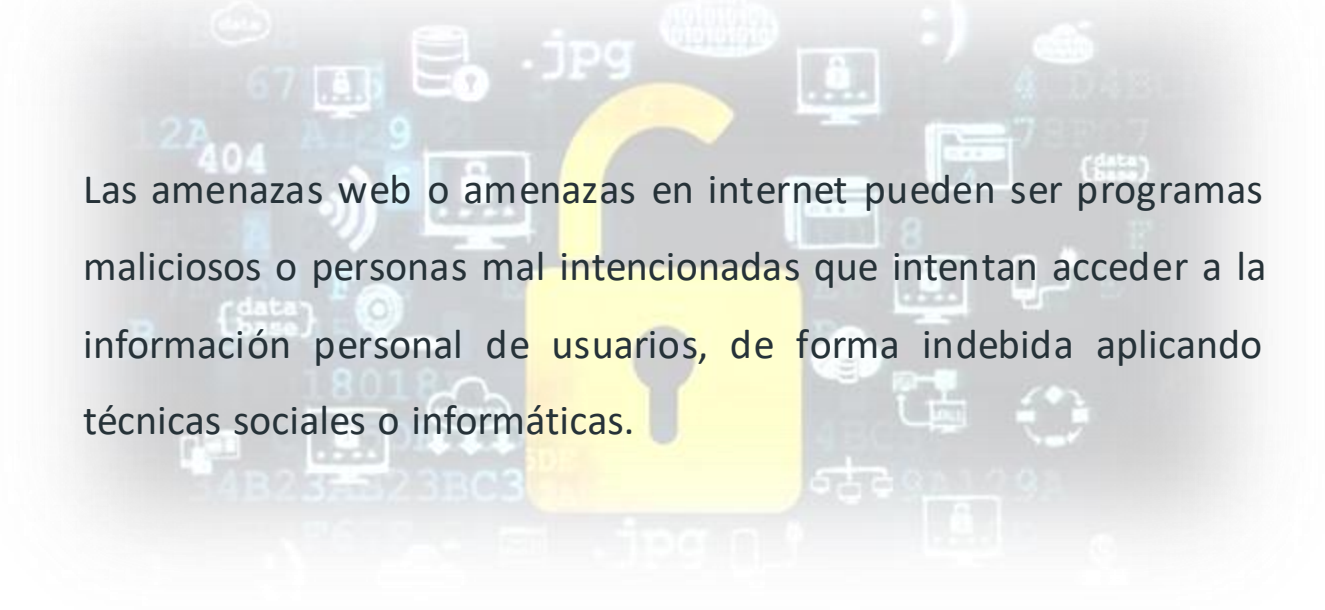
Orientaciones generales para la prevención de riesgos en el uso del internet

https://www.youtube.com/watch?v=NRY6W3uMs2Y

Trabajo Practico 1

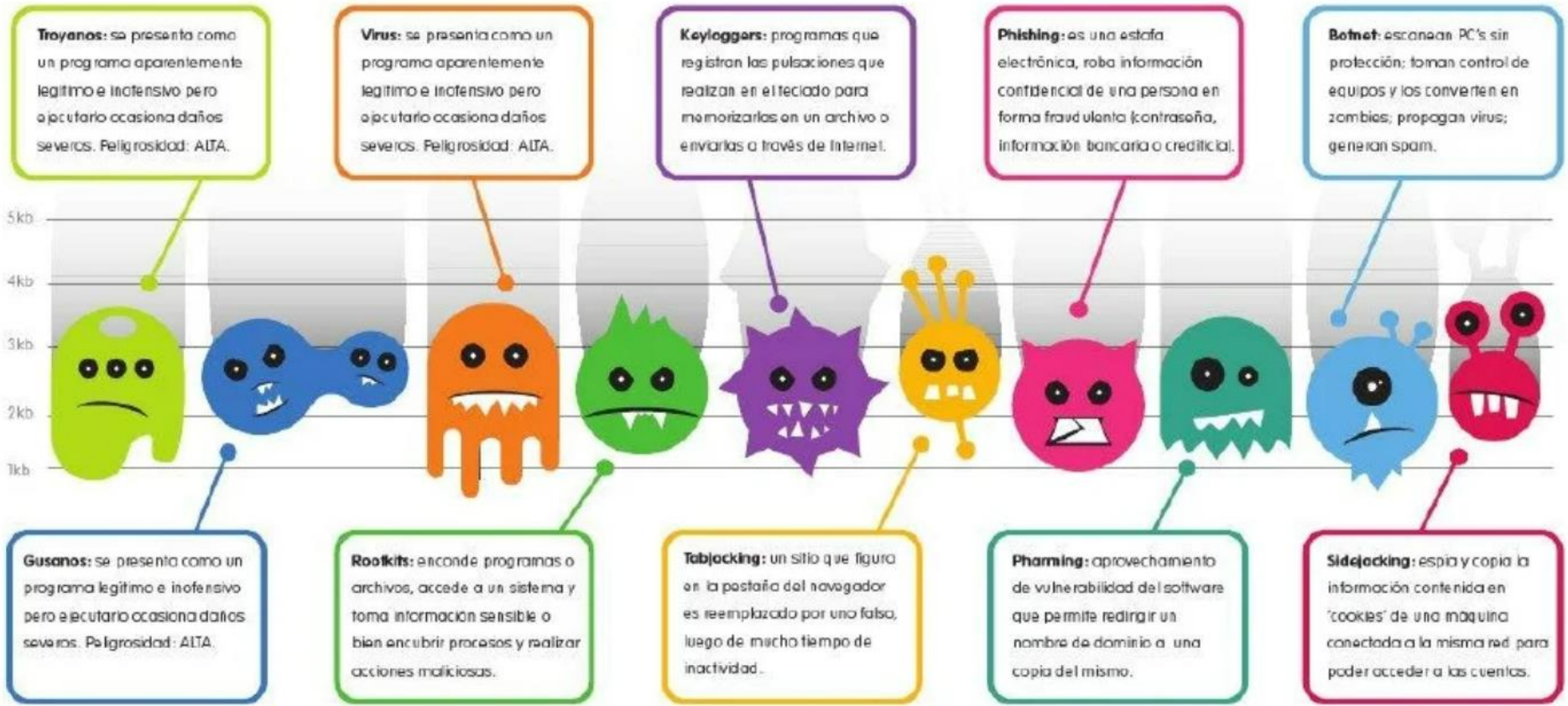
Instalación de antivirus

Amenazas en internet



Las amenazas web o amenazas en internet pueden ser programas maliciosos o personas mal intencionadas que intentan acceder a la información personal de usuarios, de forma indebida aplicando técnicas sociales o informáticas.

Amenazas más peligrosas en internet



¿Qué es el malware?

https://www.youtube.com/watch?v=RoE9T9KjxMw

Malware

- *Malware es un software malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento.*
- *Hay muchos tipos de malware y cada uno busca sus objetivos de un modo diferente.*
- ***Adware**, **spyware**, **virus**, **redes de robots** (botnets), **troyanos**, **gusanos**, **rootkits** y **ransomware** entran en la definición de malware.*
- *Los malwares no solamente atacan a los ordenadores sino también a los dispositivos móviles.*

Riesgos en las relaciones afectivas en línea

https://www.youtube.com/watch?v=eZO0XG3cWKY

Falsas relaciones afectivas en línea

Se usan sitios web que ofrecen servicios como: eDarling, Meetic, Latin american cupin, Badoo, Loventine, Bumble, etc.

Entre los riesgos más comunes en estos tipos de sitios son: perfiles falsos, estafas, pérdida de privacidad de datos o trata de personas.

Las amenazas de mayor nivel son: tráfico de personas, secuestros, violaciones, chantaje, suplantación de identidad, acoso sexual, pornografía, apropiación de datos personales.

Motivos de uso de estos sitios: falta de tiempo en el mundo real para establecer comunicaciones y relaciones con otras personas, cualquier circunstancia que haga que el usuario desee salir de su lugar de origen, captar principalmente a mujeres para ser sometidas voluntaria e involuntaria a servicios de carácter sexual.

Compras fraudulentas online

Hoy en día la compra de artículos a través de internet se ha vuelto muy común debido a su facilidad

Algunas de las consecuencias de realizar compras online no deseadas son:

- *Gasto excesivo, total o parcial de dinero.*
- *Robo de claves.*
- *Duplicación de tarjetas de crédito.*
- *Robo de información personal.*

Exposición de datos personales en internet

La publicación de información personal en internet conlleva varios riesgos ya que no sabemos en su totalidad a que personas pueden llegar nuestros datos.

Algunos de los riesgos que corremos al realizar este tipo de acción son:

- *Robo de datos.*
- *Nuestra información llega a desconocidos.*
- *Los jóvenes están más expuestos a hackers.*
- *Se facilita el rastreo.*

Contraseñas vulnerables

La administración de contraseñas por parte de los usuarios, en algunos casos es inadecuado, pues pone en alto riesgo el acceso no autorizado a los sistemas informáticos e información confidencial.

Trabajo Practico

Gestión de contraseñas mediante herramientas informáticas

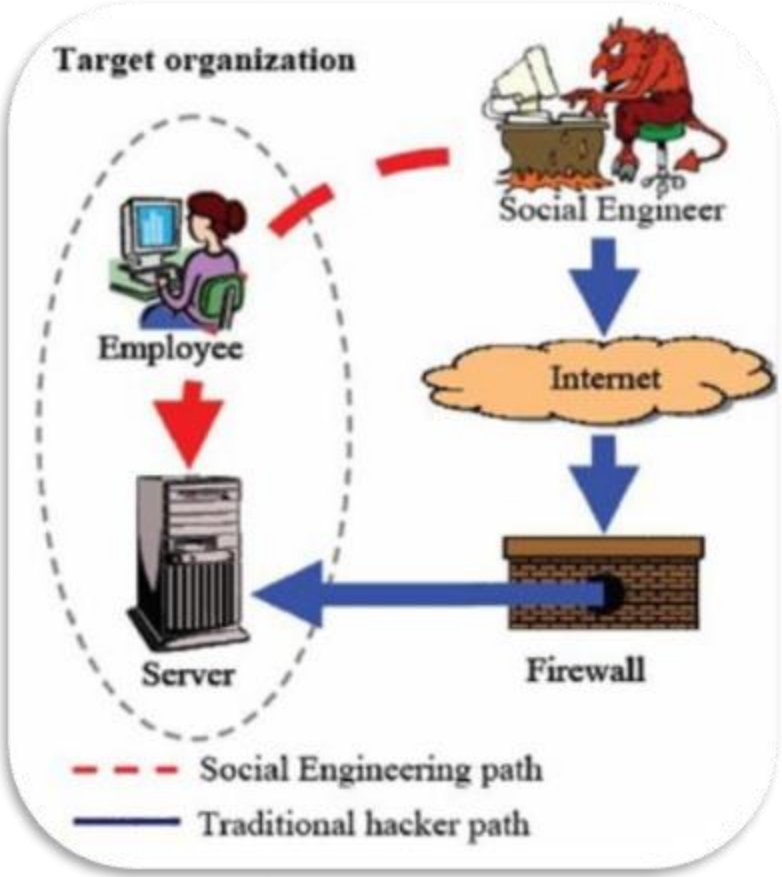
¿Qué es la ingeniería social?

https://www.youtube.com/watch?v=SSjdJgINu2E

Ingeniería social

La ingeniería social consiste en la **manipulación** de las **personas** para que voluntariamente realicen actos que normalmente no harían.

Referido a técnicas de violación que se sustentan en las debilidades de las personas más que en el software. El objetivo es engañar a la gente para que revele contraseñas u otra información que comprometa la seguridad del sistema objetivo.



Técnicas de ingeniería social

- Llamadas telefónicas mediante la personificación falsa y persuasion.
- El sitio de trabajo, acceso físico no autorizado; robar, fotografiar o copiar documentos sensibles; pasearse por los pasillos buscando oficinas abiertas; intentos de ganar acceso al data center.
- El internet - intranet, repetición de claves; anexos con troyanos, exploits, spyware.
- Fuera de la oficina, almuerzos “De Negocios” de viernes que terminan en sesiones de confesión de contraseñas, extensiones, direcciones de correo electrónico; conexiones “de oficina a oficina”.

Privacidad en internet

https://www.youtube.com/watch?v=Lcrvgby_8E8&t=58s

Privacidad en internet

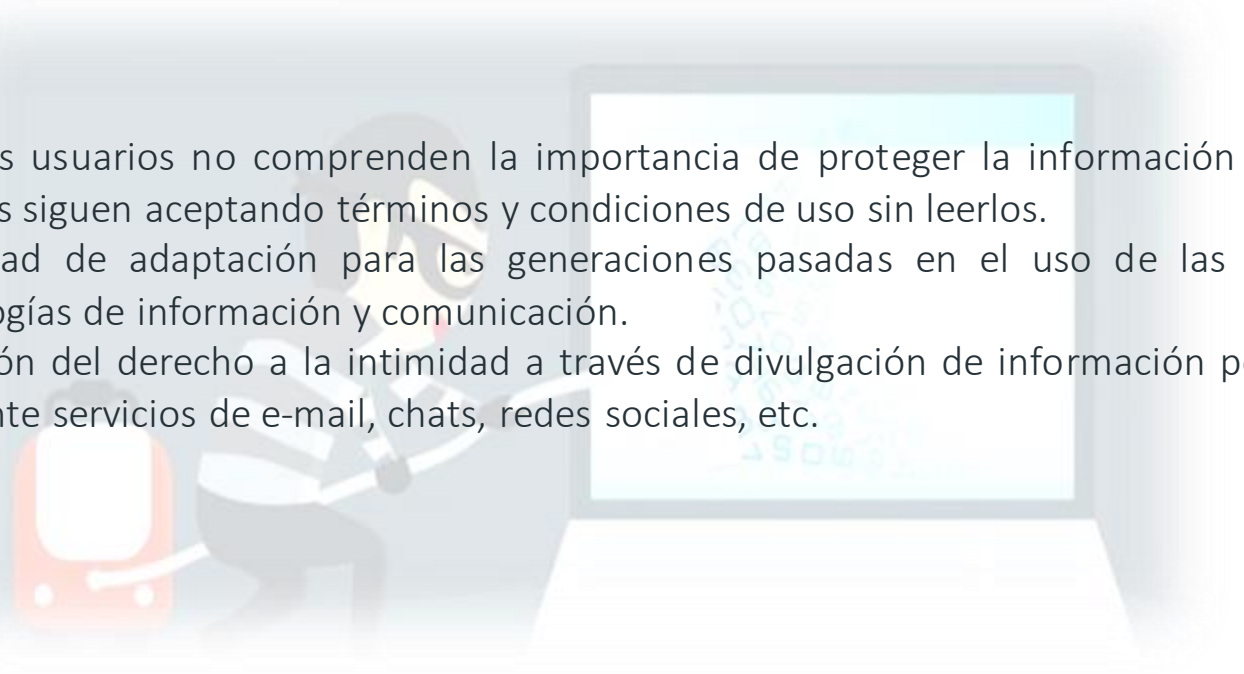
La **privacidad** es una de las principales preocupaciones de los usuarios en internet. En diversas redes circulan datos personales, direcciones de domicilio, correos electrónicos, cuentas bancarias, etc. Por lo que, es necesario conocer técnicas y herramientas que ayuden a mentener un perfil privado.

Ventajas de la privacidad en internet

- Decidir cuál es nuestra identidad digital, es decir, la imagen que internet proyecta de nosotros al resto de usuarios.
- Permitir que solo accedan a nuestros datos aquellos usuarios, empresas o proveedores de servicios que hayamos otorgado nuestro consentimiento.
- Adecuar a nuestro perfil e intereses los contenidos, productos o servicios que se ofrecen en internet.

Desventajas de la privacidad en internet

- Muchos usuarios no comprenden la importancia de proteger la información digital; muchos siguen aceptando términos y condiciones de uso sin leerlos.
- Dificultad de adaptación para las generaciones pasadas en el uso de las nuevas tecnologías de información y comunicación.
- Violación del derecho a la intimidad a través de divulgación de información personal mediante servicios de e-mail, chats, redes sociales, etc.



Técnicas y consejos para mejorar la privacidad y seguridad en internet

Técnicas de privacidad

Presta atención a las condiciones de uso.

- Revisar detalladamente la información que solicitan para utilizar ciertos dispositivos con conexión a Internet o descargar una nueva aplicación. Investigar la veracidad y legalidad del proveedor, y no dar ningún tipo de información que no sea necesario.

Contraseñas

- Administrar las contraseñas de modo responsable e inteligente. No usar la misma contraseña para todos los sitios que frecuenta. Crear contraseñas con mínimo 12 caracteres y combine con letras, números y caracteres especiales.

VPN

- Utilizar un servicio de red privada virtual (VPN) cuando navegue por redes públicas poco seguras; de esta forma, asegura que la conexión esta cifrada y los datos no estarán expuestos.

Técnicas de privacidad

Siempre cerrar las sesiones

- Si utiliza un dispositivo que no es el suyo, acuérdese siempre de cerrar las sesiones luego de concluir su actividad. De lo contrario, facilitará a cualquier persona el ingreso a sus cuentas y accederá a sus datos personales.

Actualizaciones

- Mantener actualizado el sistema operativo, de su computador y dispositivos móviles. Las últimas versiones son más seguras, porque corrigen las vulnerabilidades (fallos de programación) que facilitan a los hackers infiltrarse en los equipos a través de malware.

Navegadores seguros

- Actualizar el navegador; existen complementos que permiten una navegación más segura, por ejemplo, Firefox tiene extensiones que permiten comprobar la fiabilidad de la página e impedir que ejecute códigos sin consentimiento del usuario.

Consejos para mejorar la privacidad

Tener cuidado con las redes wifi públicas.

Actualizar las contraseñas.

Borrar el historial de búsqueda periódicamente.

Desconectar el GPS cuando no se esté utilizando.

No compartir demasiada información en redes sociales.

¿Qué son los navegadores web?

https://www.youtube.com/watch?v=dvBBDcuqwLY

Top de navegadores Seguros

- *Mozilla Firefox*
- *DuckDuckGo*
- *Epic Privacy Browser*
- *Cómodo IceDragon*
- *Google Chrome*

Mozilla Firefox

- Considerado el navegador gratuito mas seguro actualmente, utiliza una fuerte criptografía mediante el protocolo https; además, cuenta con protección antivirus integrada.
- Link de descarga:
- https://www.mozilla.org/es-ES/firefox/new/

DuckduckGo

- La mayor ventaja es la privacidad que proporciona al usuario durante el uso del navegador, no almacena ninguna información personal como direcciones IP.
- Link de descarga:
- https://duckduckgo.com/

Epic Privacy Browser

- Es un navegador web privado que bloquea anuncios, rastreadores, huellas digitales, criptomineria, señalización y mas.
- Link de descarga:
- https://epic-browser.uptodown.com/windows

Cómodo IceDragon

- Esta basado en Firefox, de modo que cuenta con algunas de las características del navegador principal.
- Tiene un sistema de detección de malware (SiteInspector) el cual permite verificar si una pagina web es maliciosa antes de entrar en ella.
- Link de descarga:
- https://icedragon.comodo.com/

Google Chrome

- Tal vez el más utilizado y el más conocido, al igual que los demás, este cuenta con grandes ventajas de seguridad, incluye protección de descargas, verificación de sitios fraudulentos que pueden tratar de robar información.
- Link de descarga:
- https://www.google.com/intl/es-419/chrome/

Extensiones de navegadores

Una **extensión** de navegador es un **pequeño módulo de software** para personalizar un navegador web. Los navegadores permiten variedad de extensiones; incluida la modificación de la interfaz de usuario, bloqueo de publicidad y la administración de las cookies.

Extensión para navegador, Privacy Badger

Privacy Badger es una extensión de navegador gratuita creada por la Electronic Frontier Foundation (EFFF).

Características:

- Realiza listas de acuerdo al sitio (blanca/negra)
- Compatible con los navegadores Google Chrome, Mozilla Firefox y Opera.
- Bloquea recursos de terceros como publicidad.

Link de descarga:
https://chrome.google.com/webstore/detail/privacy-badger/pkehgijcmpdhfbdbbnkijodmdjhbjlgp?hl=es

Extensión para navegador, Cookies Autodelete

Cookies Autodelete es una extensión web que permite el borrado de los elementos generados durante la navegación, cuando el usuario cierra el navegador o una pestaña del mismo.

Características:

- Es compatible con Firefox a partir de la versión 57.
- Borra automáticamente las cookies no utilizadas

Link de descarga:
https://chrome.google.com/webstore/detail/cookie-autodelete/fhcgjolkccmbidfldomjliifgaodjagh

Extensión para navegador, Ghostery

Ghostery es una extensión de navegador relacionada con la privacidad y la seguridad para una aplicación de navegador móvil.

Características:

- Ghostery permite a sus usuarios detectar y controlar fácilmente las «etiquetas» y los «rastreadores» de JavaScript.
- Actualización continua de una "biblioteca de scripts" que identifica cuando se encuentran nuevos scripts de seguimiento en Internet.

Link de descarga:
https://chrome.google.com/webstore/detail/ghostery-%E2%80%93-privacy-ad-blo/mlomiejdfkolichcflejclcbmpeaniij?hl=es

Trabajo Practico

Instalación de una extensión de navegador

¿Cómo nos protegen los antivirus?

https://www.youtube.com/watch?v=f8FWKR7YUq0

Antivirus

Un **antivirus** es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora. Existen diferentes tipos de antivirus, algunos cuentan con licencia de pago y otros en versión gratuita.

Plataformas de funcionamiento:

- Móvil
- S.O. Android
- S.O. iOS
- S.O. Windows
- S.O. Linux
- S.O. MacOS

Criterios para seleccionar un antivirus

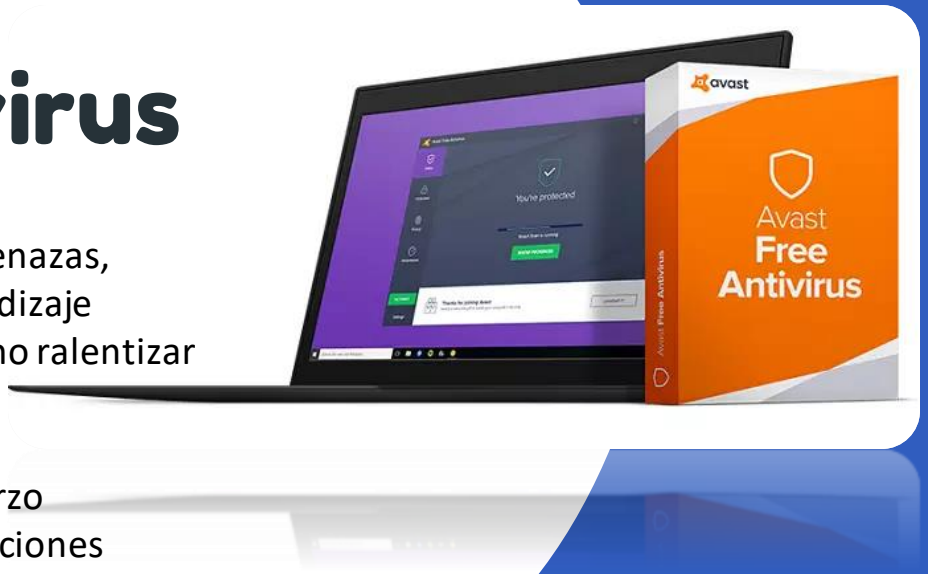
Existen diferentes tipos de antivirus, que de acuerdo con las funciones a desarrollar se escogerá la mejor opción:

- ***Antivirus gratuitos:*** son utilizados para equipos de uso doméstico.
- ***Antivirus de pago:*** añade algo más de seguridad con funciones únicas del antivirus.
- ***Antivirus corporativos:*** protección de cuentas, correos electrónicos, bases de datos corporativas.

Top 5 de antivirus gratuitos

- Avast Free Antivirus
- Avg Free Antivirus
- Avira Free Antivirus
- Bitdefender Antivirus
- Kaspersky Antivirus Free

Avast Free Antivirus



Equipado con la mayor red de detección de amenazas, protección contra virus con capacidad de aprendizaje automático y seguridad de red doméstica para no ralentizar la computadora.

Características:

- Diseñado para una protección sin esfuerzo
- Ver películas, jugar en línea sin interrupciones
- Escudo de comportamiento

Link de descarga: www.avast.com

AVG Free Antivirus

Eficaz para detectar amenazas y eliminarlas, es capaz de interrumpir cualquier programa que sea malicioso y esté intentando situarse en el disco duro.

Características:

- Protección para smartphone.
- Solución integral de antivirus y optimización.
- Privacidad y protección premium.

Link de descarga: https://www.avg.com/es-ww/homepage#pc

Avira Free Antivirus

Detecta virus, adware, spywares, entre otros. También es capaz de reparar los archivos afectados por los malware, bloquea sitios web que pueden estar infectados.

Características:

- Protección en tiempo real contra ataques de virus.
- Detección y remoción de virus, antispam y malware.
- Consume pocos recursos del computador.

Link de descarga: https://www.avira.com/es/free-antivirus

BitDefender Antivirus

Proporciona soluciones antivirus, firewall, antispyware, antispam y control parental para usuarios corporativos y domésticos. Tiene un impacto mínimo en los recursos del computador, es rápido y no agresivo.

Características:

- Seguridad para todos sus datos
- No invasivo
- Protege transacciones online
- Protege mediante cortafuegos

Link de descarga:
https://www.bitdefender.com/solutions/free.html

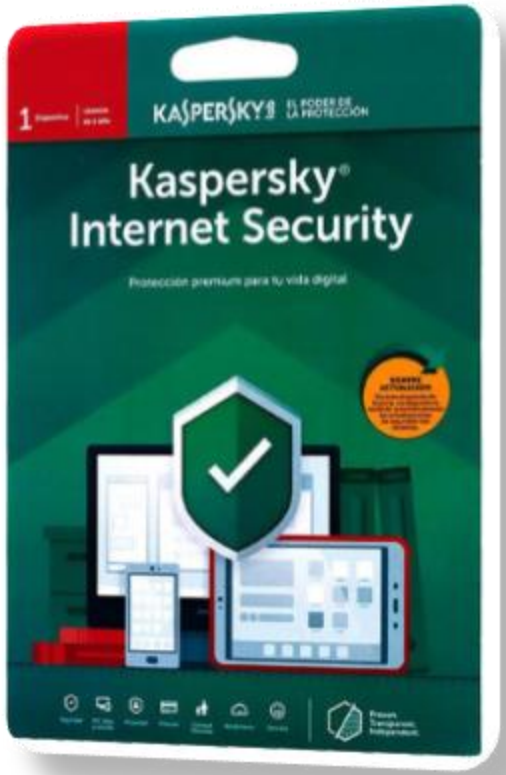
Kapersky Antivirus Free

Incluye tecnologías de seguridad de primera categoría y permite analizar automáticamente datos en tiempo real.

Características:

- Protección anti-malware en tiempo real, te protege frente a amenazas nuevas y emergentes.
- Tecnología con asistencia en la nube que permite la protección en tiempo real.
- Detiene los procesos peligrosos.

Link de descarga:
https://latam.kaspersky.com/free-antivirus



Trabajo Practico

Instalación de antivirus