COMISIÓN INSTITUCIONAL DE TELETRABAJO

Aspectos Tecnológicos en el Teletrabajo

Presentado por:

Maykol Phillips Seas (maykol@una.cr)

3 de Setiembre de 2020

- Aspectos de Ingeniería Social
- Protección de contraseñas
- Protección de la información
- Protección del dispositivo de trabajo
- Firma digital
- Capacidad de internet
- Reuniones virtuales

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

❑Aspectos de Ingeniería Social

Engaños y fraudes

10 min.

Según la firma Kaspersky la ingeniería social se define como el "*conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados*"

Para Oracle, un malware se entiende como "*un término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software*"

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

UNA
UNIVERSIDAD
NACIONAL
COSTA RICA

ÚLTIMA NOTICIA: Carlos Alvarado Ofrece un Sistema 100% Seguro para Generar Ingresos desde Casa mientras dure el COVID-19

Los ciudadanos de Costa Rica no deben arruinarse por el CODVID-19, deben de generar ingresos desde sus casas gracias a este sistema que ofrece resultados seguros y garantizados.

Carlos Alvarado ofrece soluciones para generar ingresos desde casa mientras dure la Pandemia

GANANCIAS: ₡3,992,478 colones

"Invierto desde hace más de 7 años, pero el mejor sistema hasta la fecha es sin duda Bitcoin-Dolar, ya que te facilita mucho el trabajo y puedes tener mucho tiempo libre"

Elías Peña (Costa Rica)

GANANCIAS: ₡1,070,447 colones

"Ya hice ₡1,649,067 colones en ganancias después de usar Bitcoin-Dolar durante apenas un mes. ¡Ahora trabajo desde casa apenas 1 o 2 horas al día!"

Sora Carrillo (Costa Rica)

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

ATAQUES DE INGENIERÍA SOCIAL

1 **PRETEXTING**

Obtención de datos personales a través de llamadas telefónicas simulando ser otra persona.

2 **DUMPSTER DIVING**

Explorar la basura con el fin de obtener información valiosa de la víctima.

3 **SHOULDER SURFING**

Espiar físicamente a las personas para conseguir información privada de la víctima.

4 **BAITING**

Poner un cebo a la víctima para que coja el pendrive e infecte el ordenador.

LISA Institute

5 **PHISHING**

Enviar masivamente correos con archivos maliciosos para obtener información confidencial.

6 **SMISHING**

Enviar SMS con enlaces maliciosos para obtener información privada de la víctima.

7 **VISHING**

Engañar a las víctimas mediante llamadas telefónicas para obtener sus datos personales.

8 **SEXTORSIÓN**

Amenazar a la víctima para no publicar imágenes comprometidas a cambio de dinero.

https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

UNA UNIVERSIDAD NACIONAL COSTA RICA

Corresponde a métodos y técnicas que pueden utilizar – o no – medios tecnológicos para engañar y estafar.

Puede utilizar llamadas telefónicas, correos electrónicos sospechosos, llamadas por WhatsApp, llamadas por Facetime (Apple), entre otros.

No en vano, muchas personas reciben llamadas telefónicas de países tan lejanos como Guyana, Tokelau, Madagascar, Rusia, Kiribati, Papúa, entre otros.

Pretenden la obtención de nombres de usuario y contraseñas, información confidencial, números de cuentas bancarias, contraseñas de Internet Banking, e información relevante que en la mayoría de los casos tiene un valor económico.

Recomendación general: Una sana desconfianza ante este tipo de situaciones. No proceder, ni dejarse intimidar si no hay seguridad en un 100% de lo que se va a hacer.

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

❑ Protección de contraseñas

20 min.

La utilización de contraseñas (passwords) forman parte de nuestra cotidianeidad ya sea de forma directa o indirecta, ya que estas nos permiten la interacción con facilidades y servicios que anteriormente requerían nuestra presencialidad.

Anteriormente, íbamos a cobrar el cheque al banco, hacíamos filas para pagar servicios de agua, electricidad y teléfono, acudíamos al banco para pagar la tarjeta de crédito, entre otros. Los trámites eran presenciales …

¿ Qué servicios y facilidades, requieren el uso de contraseñas ?

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Nuestra vida cotidiana, está compuesta por muchas contraseñas …

En términos generales, tenemos 2 modalidades para definir contraseñas de servicios y aplicaciones:

Una misma contraseña para todo; solución rápida y fácil. Pero si se pierde u olvida, el ingreso a todas las facilidades se ve comprometido por igual.

Diferentes contraseñas para todas las facilidades. Implica una mayor complejidad y esfuerzo para administrarlas y gestionarlas.

Solución: Utilizar un software gestor de contraseñas, que almacene, proteja y encripte todas las contraseñas a almacenar.

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Sin embargo, el tema tiene su complejidad media:

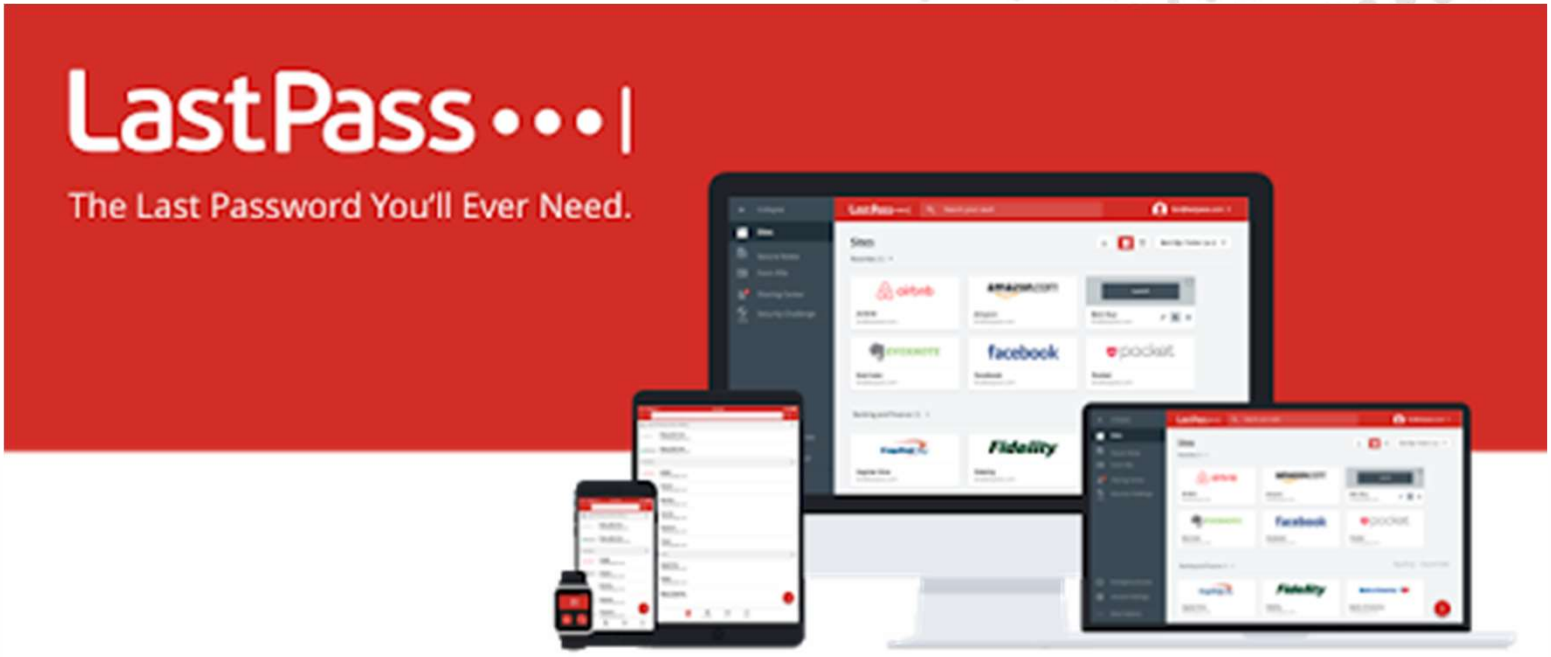
Puede utilizarse un software que utilice una clave maestra para para ingresar a las contraseñas almacenadas. Sin embargo, esta clave estará encriptada y será irrecuperable en caso de extravío. Ej: la firma digital.

O se puede usar una solución que utiliza una clave maestra, encriptada, que puede recuperarse por correo electrónico o SMS en caso de extravío. Esto es lo más habitual.

Advertencia: Debe decidirse, si nuestras contraseñas van a almacenarse en la nube o de forma local en nuestro computador o dispositivo móvil.

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Ejemplo de gestor de contraseñas:



https://www.lastpass.com/es

UNA
UNIVERSIDAD
NACIONAL
COSTA RICA

Fortaleza de las contraseñas:

Entre más extensas sean mejor. Que incluyan números, letras mayúsculas y minúsculas y caracteres especiales.

Si se tiene el conocimiento y facilidad de habilitar un segundo factor de autenticación, mejor (Ej: **Token bancario, SMS, correo de autenticación, llamada telefónica**).

Rotar las contraseñas periódicamente.

Se recomienda, almacenar en lugar seguro. No olvidar, ya que su recuperación puede ser costosa en tiempo o dinero (firma digital).

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Lista de las 25 contraseñas más usadas en 2013

1. 123456 (Sube 1)
2. password (Baja 1)
3. 12345678 (Sin cambios)
4. qwerty (Sube 1)
5. abc123 (Baja 1)
6. 123456789 (Nuevo)
7. 111111 (Sube 2)
8. 1234567 (Sube 5)
9. iloveyou (Sube 2)
10. adobe123 (Nuevo)
11. 123123 (Sube 5)
12. Admin (Nuevo)
13. 1234567890 (Nuevo)
14. letmein (Baja 7)
15. photoshop (Nuevo)
16. 1234 (Nuevo)
17. monkey (Baja 11)
18. shadow (Sin cambios)
19. sunshine (Baja 5)
20. 12345 (Nuevo)
21. password1 (Sube 4)
22. princess (Nuevo)
23. azerty (Nuevo)
24. trustno1 (Baja 12)
25. 000000 (Nuevo)

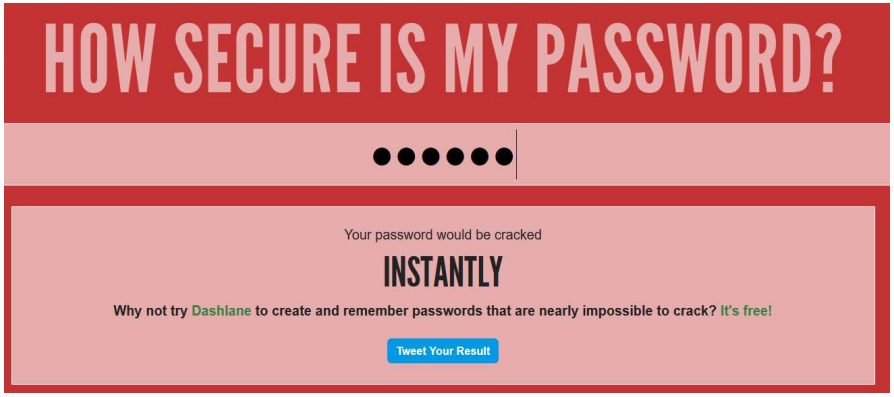
Esto es lo que hay que evitar

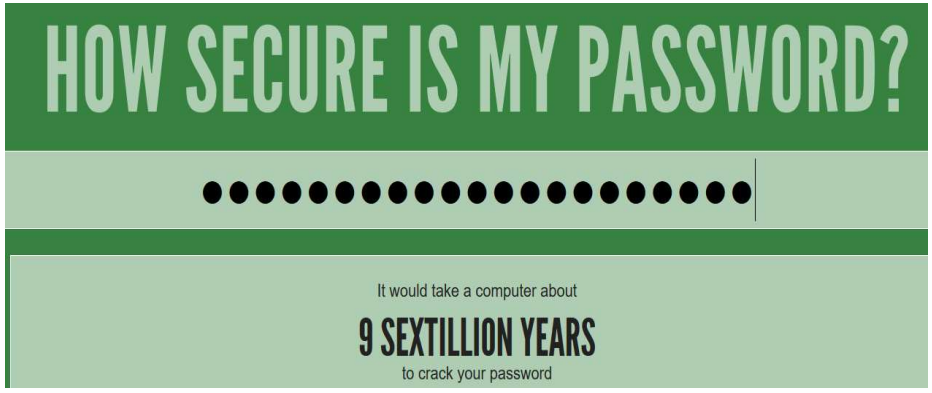
1Gb de información

Universidad Rey Juan Carlos

UNA UNIVERSIDAD NACIONAL COSTA RICA

https://howsecureismypassword.net/



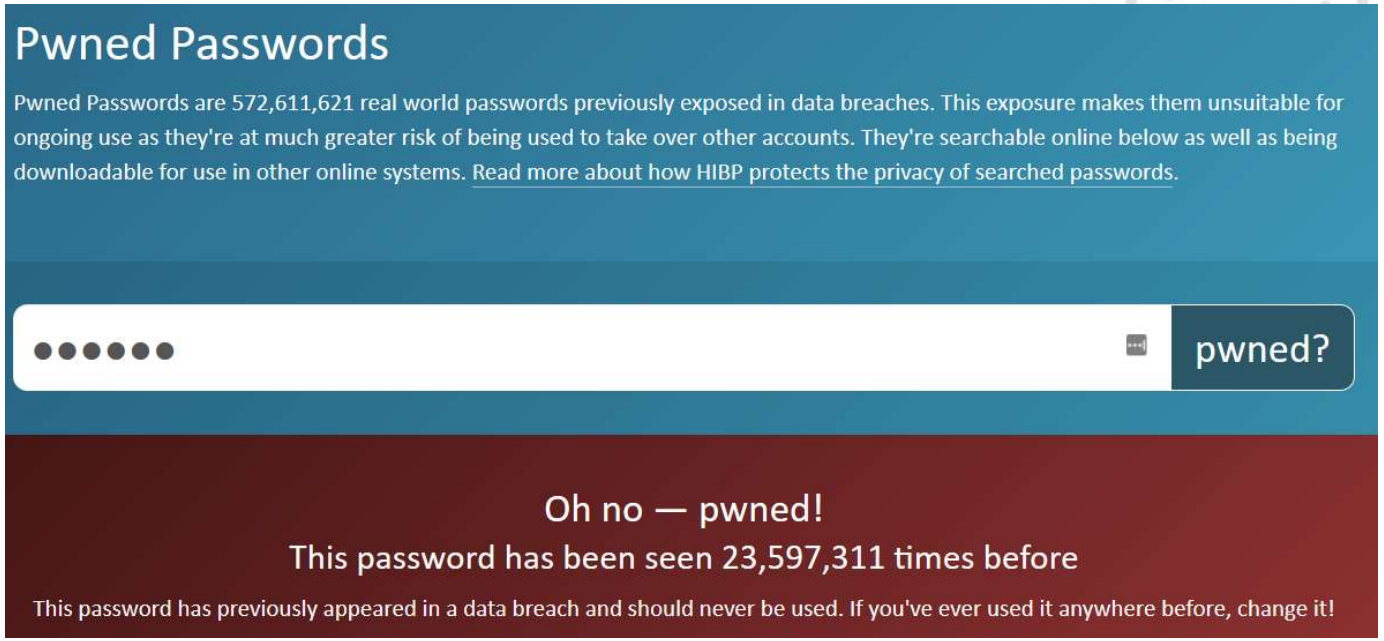


Contraseña: 123456

Contraseña: Vieneelloboferoz2020.

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

https://haveibeenpwned.com/Passwords



Contraseña: 123456

UNA
UNIVERSIDAD
NACIONAL
COSTA RICA

Generadores de contraseñas:

https://www.lastpass.com/es/password-generator

https://www.pandasecurity.com/es/homeusers/passwords-generator/

UNA UNIVERSIDAD NACIONAL COSTA RICA

En resumen:

¿ El tema para gestionar y administrar contraseñas, es fácil y automático ? No, su complejidad es media.

¿ Requiere claridad de la temática, aprendizaje y pruebas previas ? Sí

¿ Hay que invertir tiempo para experimentar y aprender ? Sí

Generalmente, ¿ deben cambiarse las contraseñas con regularidad ? Sí

¿ Debemos utilizar contraseñas complejas ? De preferencia sí, para los servicios críticos, puede ser basado en frases y no en palabras de diccionario, fechas o nombres particulares.

¿ Debemos compartir nuestras contraseñas ? No

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

❑ Protección de la información

5 min.

La UNA no maneja información secreta, pero esta información puede ser pública, restringida o confidencial: correos electrónicos institucionales vs. correos electrónicos personales, números de teléfono personales, salarios, deducciones, estados financieros, investigaciones internas, entre muchas otras.

En Teletrabajo, podemos estar trabajando eventualmente con información que debe ser protegida. El computador puede ser utilizado por terceros, puede ser objeto de hurto, puede llevarse al técnico para su reparación, etc.

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Encripción de la información:

- Permite utilizar una contraseña maestra, irrecuperable en la mayoría de los casos
- Existen soluciones gratuitas y comerciales
- Almacenar los datos o discos duros enteros – encriptados – en un *sitio alterno seguro*: disco duro portátil o soluciones en la nube
- Pruebe y aprenda, antes de usar
- Asegúrese de tener un plan B en caso de desastre.

VeraCrypt

AxCrypt
www.axcrypt.net

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Protección del dispositivo de trabajo

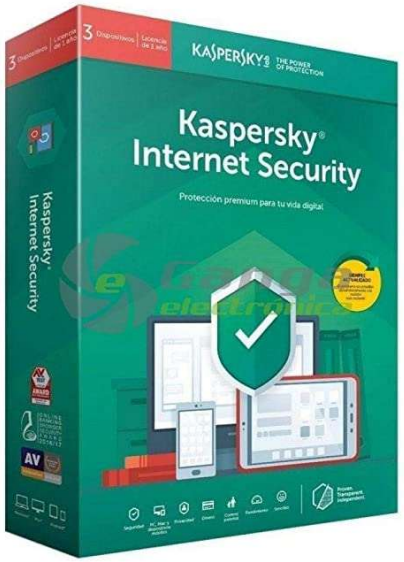
10 min.

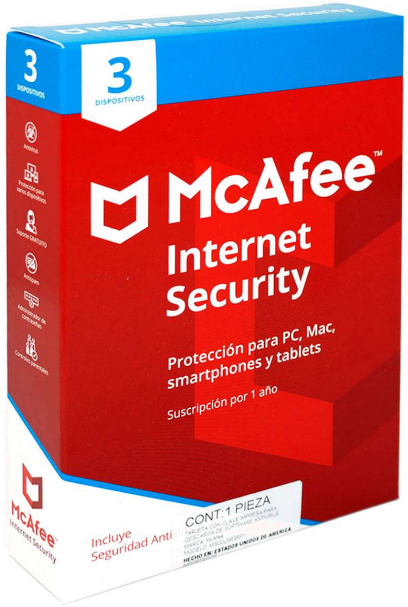
Para proteger el computador, un antivirus ya no es suficiente

Se requiere una solución de seguridad informática más robusta, completa y compleja. Generalmente, esta solución es un software comercial

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Hay varias opciones en el mercado:

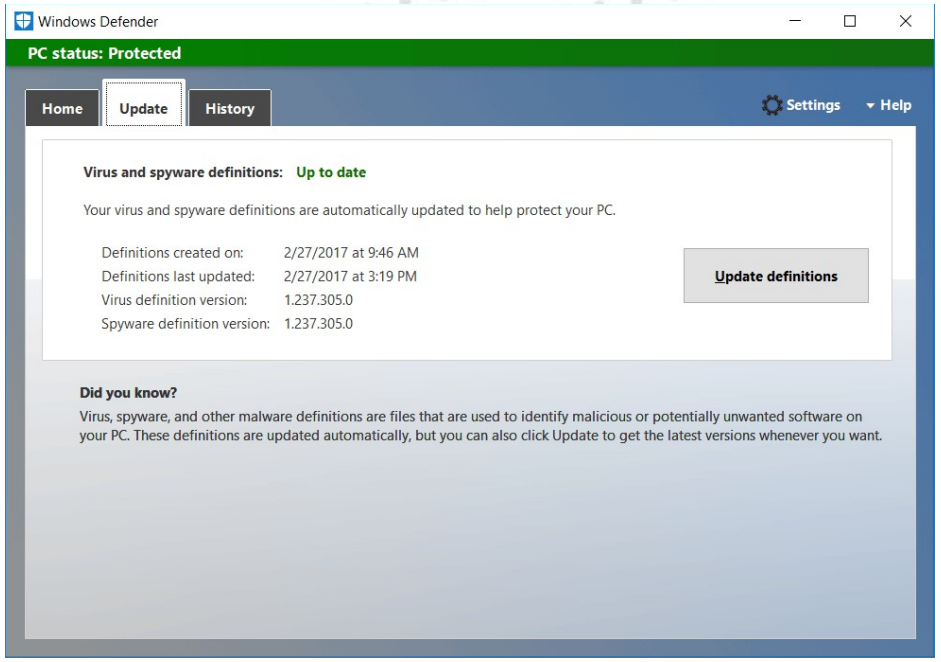




UNA
UNIVERSIDAD
NACIONAL
COSTA RICA

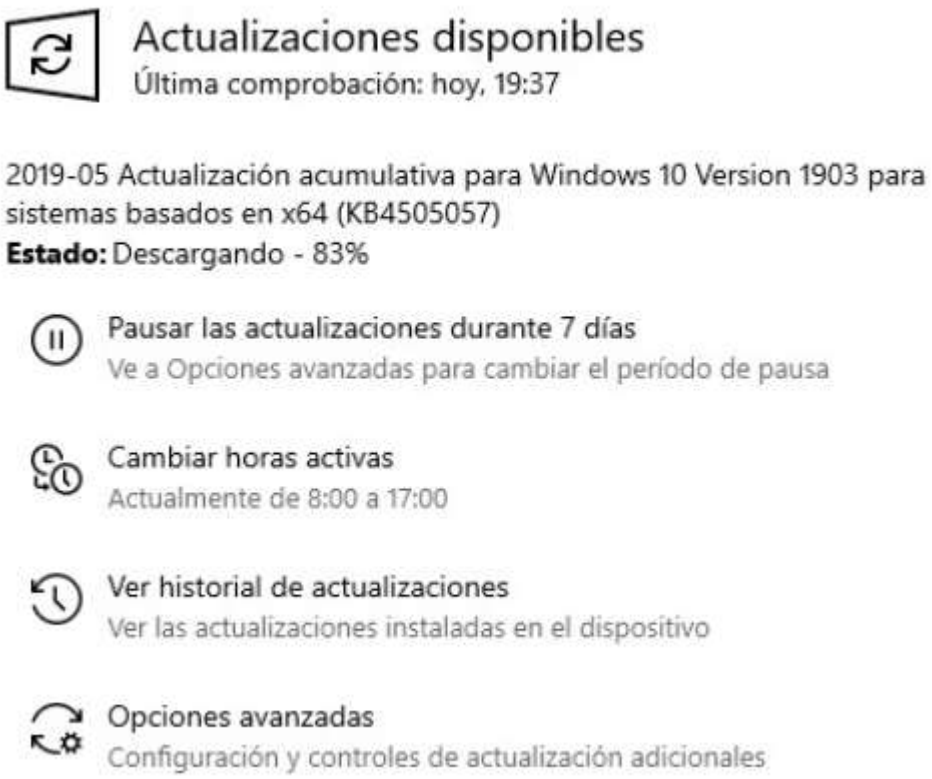
Implementar como mínimo:

Windows Defender



UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Otras consideraciones:



Actualización constante de sistemas operativos y aplicaciones en computadores, tabletas y celulares

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Más consideraciones:

Respaldar datos en dispositivos alternos

No compartir el WiFi con terceros, o crear al menos una red WiFi para invitados. Utilizar encriptación WPA2 como mínimo

No instalar software pirata o desconocido, no contestar correos sospechosos, no visitar páginas web sospechosas

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

❑Firma Digital

5 min.

En la mayoría de los casos, nuestros procesos no requieren firma física.

En la UNA, la gestión documental que utiliza la firma digital permite el envío electrónico de documentos formales.

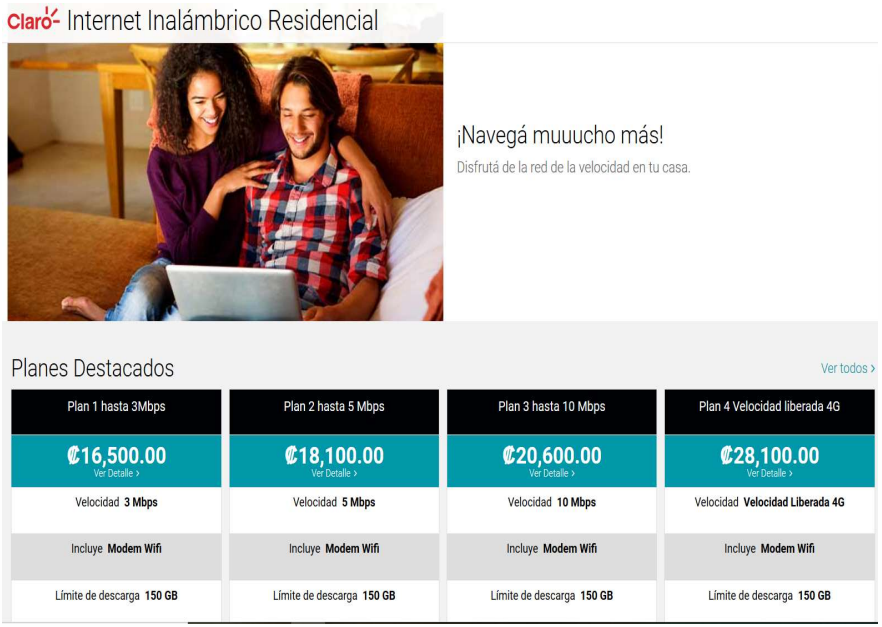
La firma digital tiene repercusiones legales en caso de un uso incorrecto.

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

❑Capacidad de internet

(fijo – residencial - hogar)

10 min.



UNA
UNIVERSIDAD NACIONAL
COSTA RICA

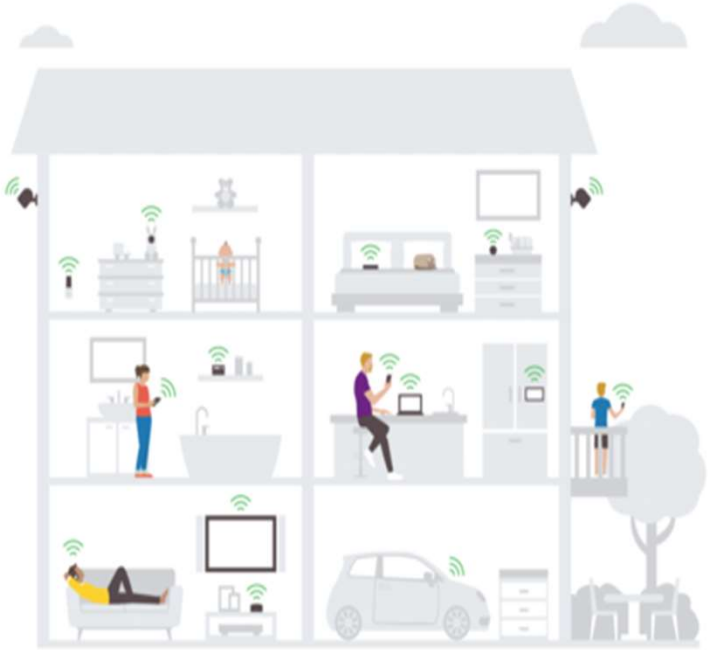
Preguntas a realizar:

¿ Cuánto es la velocidad de internet contratada en mi hogar ?

¿ Cuántas personas utilizan el internet de forma diaria ?

¿ Qué tipo de aplicaciones utilizan estas personas de forma frecuente ? ¿ Zoom, Teams u otras plataformas sincrónicas educativas o de trabajo ? ¿ Youtube, Facebook o similares ? ¿ Juegos en línea ? ¿ Netflix, Amazon Prime o Apple Tv ?

Todo lo anterior afecta la disponibilidad y el acceso a internet



UNA
UNIVERSIDAD NACIONAL
COSTA RICA

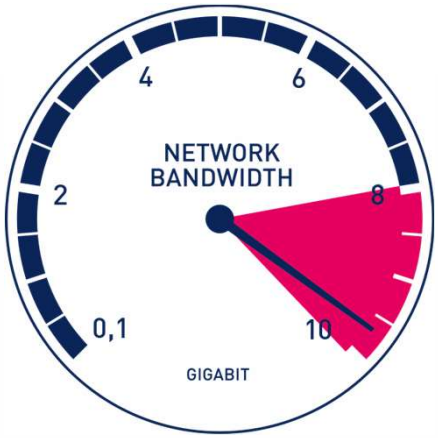
En el caso de Zoom:

Ancho de banda recomendado para Reuniones y panelistas de seminarios web:

- Para video llamada 1:1: 600 kbps (subida/bajada) para video de alta calidad y 1.2 Mbps (subida/bajada) para video HD
- Para llamada de video grupal: 600 kbps/1.2 Mbps (subida/bajada) para video de alta calidad. Para Vista de galería: 1.5 Mbps/1.5 Mbps (subida/bajada).
- Para compartir pantalla únicamente (sin miniatura de video) 50-75 kbps
- Para compartir pantalla con miniatura de video: 50-150 kbps
- Para audio VoIP: 60-80 kbps

Ancho de banda recomendado para asistentes al seminario web:

- Para video llamada 1:1: 600 kbps (bajada) para video de alta calidad y 1.2 Mbps (bajada) para video HD
- Para compartir pantalla únicamente (sin miniatura de video): 50-75 kbps (bajada)
- Para compartir pantalla con miniatura de video: 50-150 kbps (abajo)
- Para audio VoIP: 60-80 kbps (abajo)



https://support.zoom.us/hc/es/articles/201362023-Requisitos-del-sistema-para-PC-Mac-y-Linux

UNA
UNIVERSIDAD
NACIONAL
COSTA RICA

En el caso de Teams:

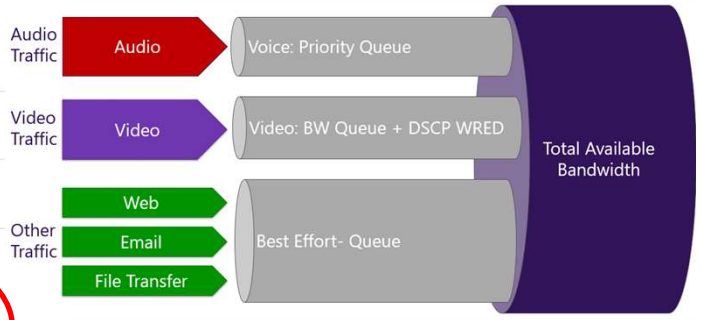
Bandwidth requirements

Teams is designed to give the best audio, video, and content sharing experience regardless of your network conditions. That said, when bandwidth is insufficient, Teams prioritizes audio quality over video quality.

Where bandwidth *isn't* limited, Teams optimizes media quality, including up to 1080p video resolution, up to 30fps for video and 15fps for content, and high-fidelity audio.

This table describes how Teams uses bandwidth. Teams is always conservative on bandwidth utilization and can deliver HD video quality in under 1.2Mbps. The actual bandwidth consumption in each audio/video call or meeting will vary based on several factors, such as video layout, video resolution, and video frames per second. When more bandwidth is available, quality and usage will increase to deliver the best experience.

Bandwidth(up/down)	Scenarios
30 kbps	Peer-to-peer audio calling
130 kbps	Peer-to-peer audio calling and screen sharing
500 kbps	Peer-to-peer quality video calling 360p at 30fps
1.2 Mbps	Peer-to-peer HD quality video calling with resolution of HD 720p at 30fps
1.5 Mbps	Peer-to-peer HD quality video calling with resolution of HD 1080p at 30fps
500kbps/1Mbps	Group Video calling
1Mbps/2Mbps	HD Group video calling (540p videos on 1080p screen)



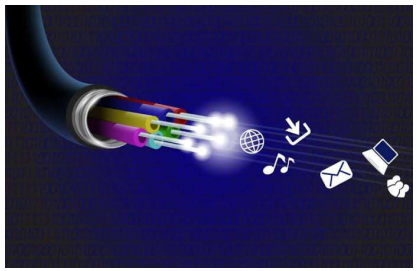
UNA
UNIVERSIDAD NACIONAL
COSTA RICA

En el caso de Netflix:

Recomendaciones sobre la velocidad de conexión a Internet

A continuación se presentan las recomendaciones de velocidad de descarga de Internet por stream para reproducir series y películas a través de Netflix.

- 0,5 megabits por segundo: velocidad de conexión de banda ancha requerida
- 1,5 megabits por segundo: velocidad de conexión de banda ancha recomendada
- 3 megabits por segundo: velocidad recomendada para calidad SD
- 5 megabits por segundo: velocidad recomendada para calidad HD
- 25 megabits por segundo: velocidad recomendada para calidad Ultra HD



UNA
UNIVERSIDAD NACIONAL
COSTA RICA

En resumen:

- Debe valorarse la oferta técnica y comercial existente en mi región
- ¿ Qué tanto afecta a mis actividades teletrabajables, el uso de internet por parte de otros miembros de mi hogar ?
- ¿ Debo limitar el uso de ciertas aplicaciones que utilizan internet durante mi horario laboral ?
- ¿ Debo aumentar la velocidad contratada con mi proveedor de servicio ? ¿ Es técnica, y económicamente factible ?

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

❑ Reuniones virtuales

Incidentes y errores comunes

10 min.

En los últimos meses, se han suscitado eventos que interfieren una sesión de trabajo, o en su defecto generan situaciones jocosas o comprometedoras:

- Personas desconocidas que transmiten pornografía
- Personas semidesnudas que transitan durante la transmisión
- Inexistencia de un control que permita coordinar la gestión del audio y video de los participantes

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

UNA
UNIVERSIDAD
NACIONAL
COSTA RICA

- Agendar reuniones o eventos en los que se distribuya de forma pública las contraseñas de ingreso

- Desconocer la facilidad técnica de habilitar o deshabilitar las funcionalidades de audio y video de su propio equipo

- En reuniones con múltiples participantes, "dejar a la libre" la activación del video, y particularmente del audio, en donde no exista un encargado de la reunión que conozca y regule la habilitación de estas facilidades.

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

- Utilizar la última versión de software (Zoom, Teams)
- Configurar una contraseña para ingresar a la reunión
- Configurar la sala de espera o equivalente
- Iniciar con el audio y el video apagados
- Establecer de previo la logística para permitir a los participantes utilizar el audio y el video.
- Estar preparado para silenciar o expulsar a "invitados no deseados"

UNA
UNIVERSIDAD
NACIONAL
COSTA RICA

UNA
UNIVERSIDAD
NACIONAL
COSTA RICA