

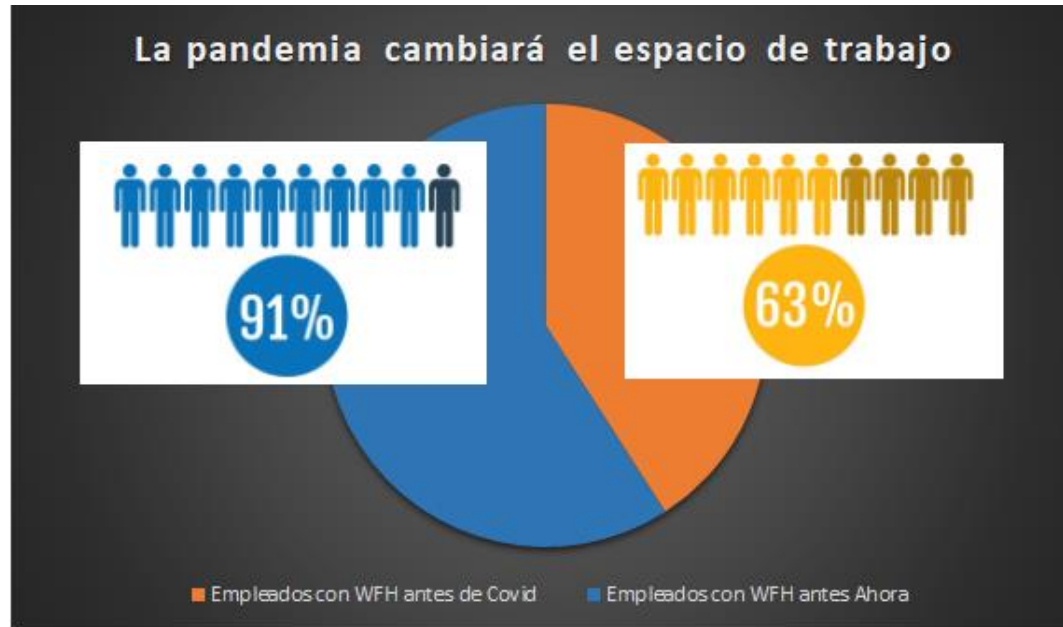
3 de Octubre

Ciberseguridad en ambientes de teletrabajo

Ing. Arnoldo Altamirano

Senior Audit Manager en Scotiabank de Costa Rica
Ingeniería en Sistemas de Información, UNA
Certified Information System Auditor, ISACA

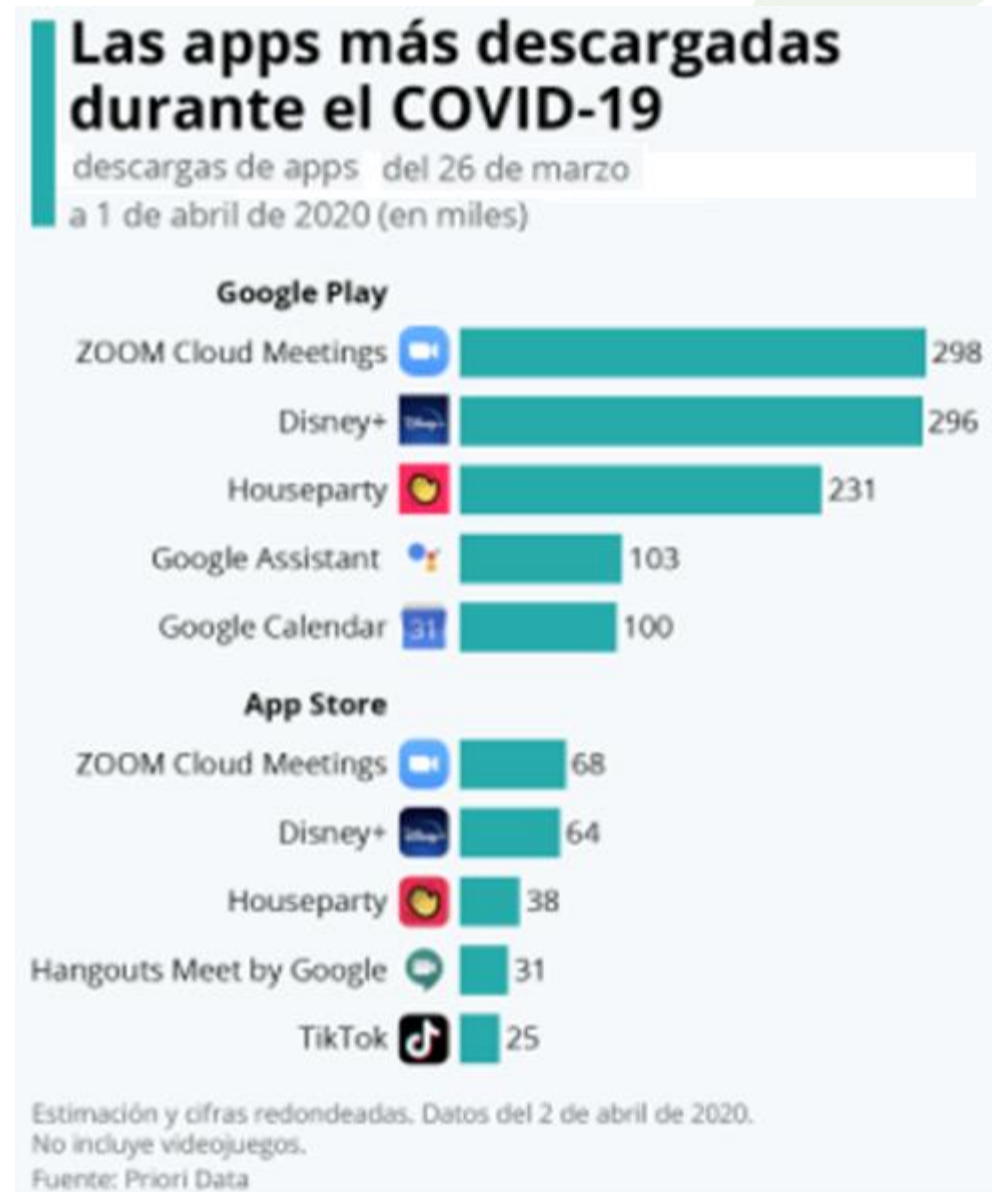
Datos interesantes del trabajo desde la casa



Qué les permitirá a los empleados continuar con el trabajo desde la casa?

- 1 Mejoran su Calidad de vida
- 2 Preparación para futuros desastres
- 3 Mejoran su Calidad de vida

Datos interesantes del trabajo desde la casa



Conectividad

Recomendaciones para los empleados y miembros del hogar

1. La conectividad (Tu red y el VPN)

Siempre utilizá conexión VPN (Red Privada Virtual): te permite el acceso seguro a la red propia de tu trabajo utilizando la conexión a Internet de tu casa.

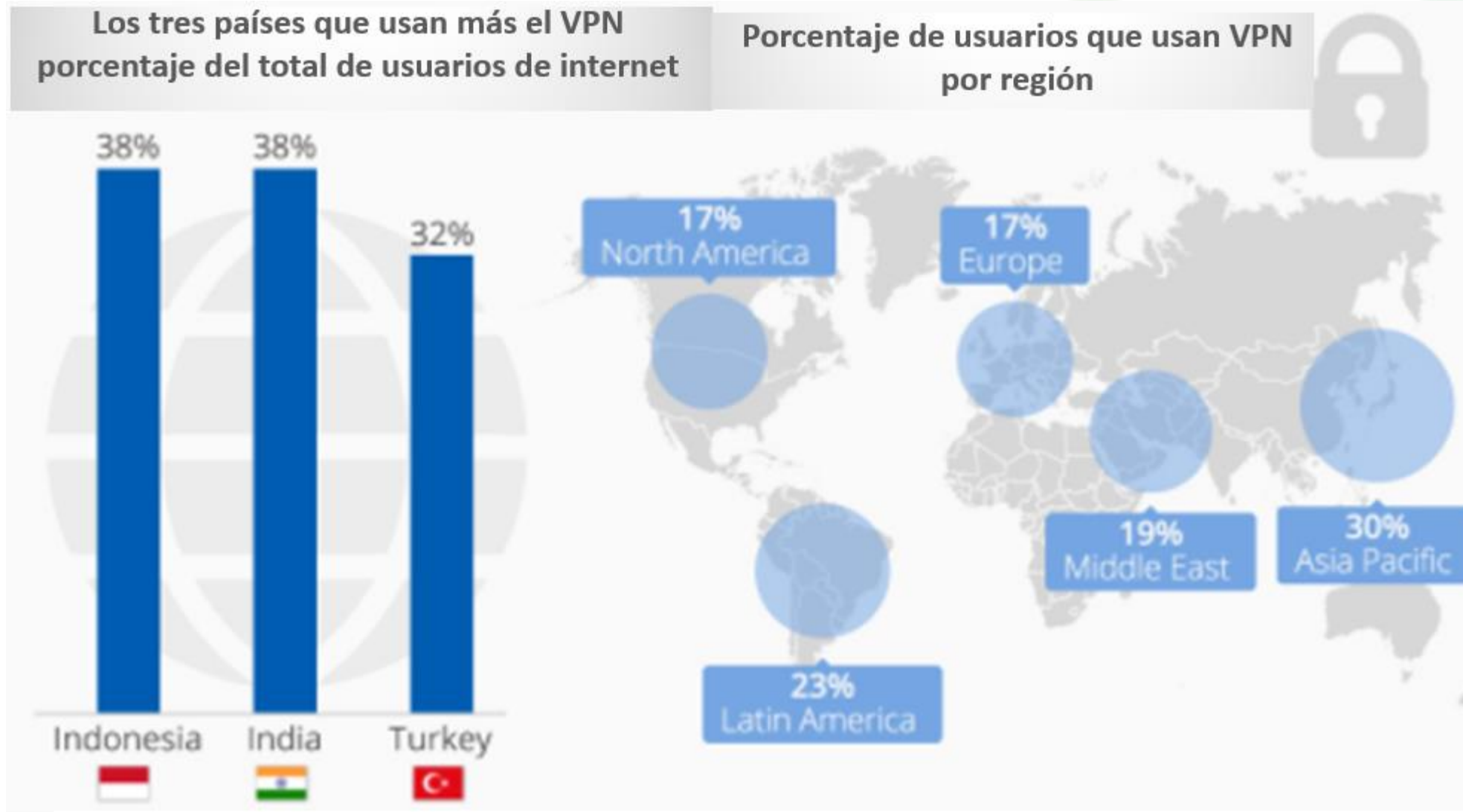
Esto evita que el tráfico sea interceptado por un ciberatacante.

Evitá conectarte a Internet desde redes Wi-Fi públicas como las de un restaurante o espacio de trabajo colaborativo (coworking).

Verificá tu Wi-Fi hogareño: asegurate que tu router esté adecuadamente configurado con el estándar llamado WPA2 (Wi Fi Protected Access) el cual obliga a que se requiera de una contraseña.



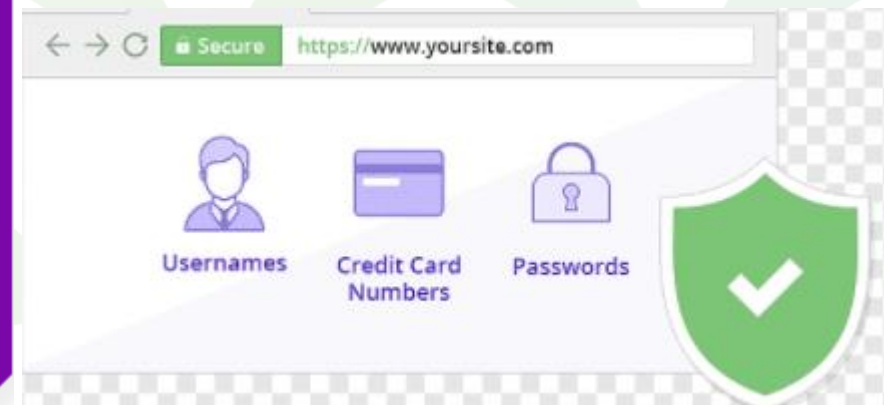
Datos interesantes del trabajo desde la casa



Las contraseñas

2. Selecciona una contraseña robusta

- Configurar una contraseña o activar datos biométricos para acceder al dispositivo. Este último siempre se debe bloquear cuando no estemos trabajando en él.
- Para que sea robusta:
 - 8 caracteres o más,
 - una mayúscula,
 - un número y un carácter especial.
 - Es fundamental que no utilices la misma contraseña para todos los perfiles/cuentas.
- Activar el Múltiple Factor de Autenticación en todos los servicios y apps que permitan esta configuración, sobre todo si tenés instaladas aplicaciones con información laboral en tu celular personal.
- Verifica que la dirección URL del sitio al que queramos acceder esté bien escrita y que comience con **HTTPS**.



Las contraseñas más débiles, el rankin de las peores...

Los passwords más populares del mundo

	2019	Cambio desde El ultimo año		2018	Cambio desde El ultimo año
1.	123456*	0		123456*	0
2.	qwerty	+3		password	0
3.	password	-1		111111	new
4.	iloveyou	+2		sunshine	+51
5.	111111	-2		qwerty	-2
6.	123123	+6		iloveyou	0
7.	abc123	+4		princess	new
8.	querty123	+12		admin	-1

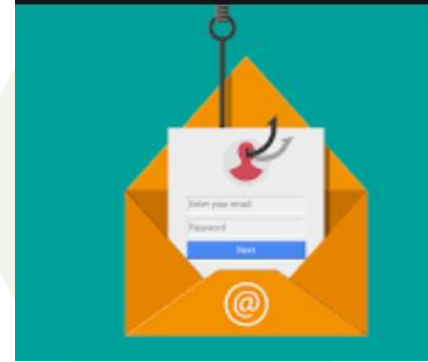
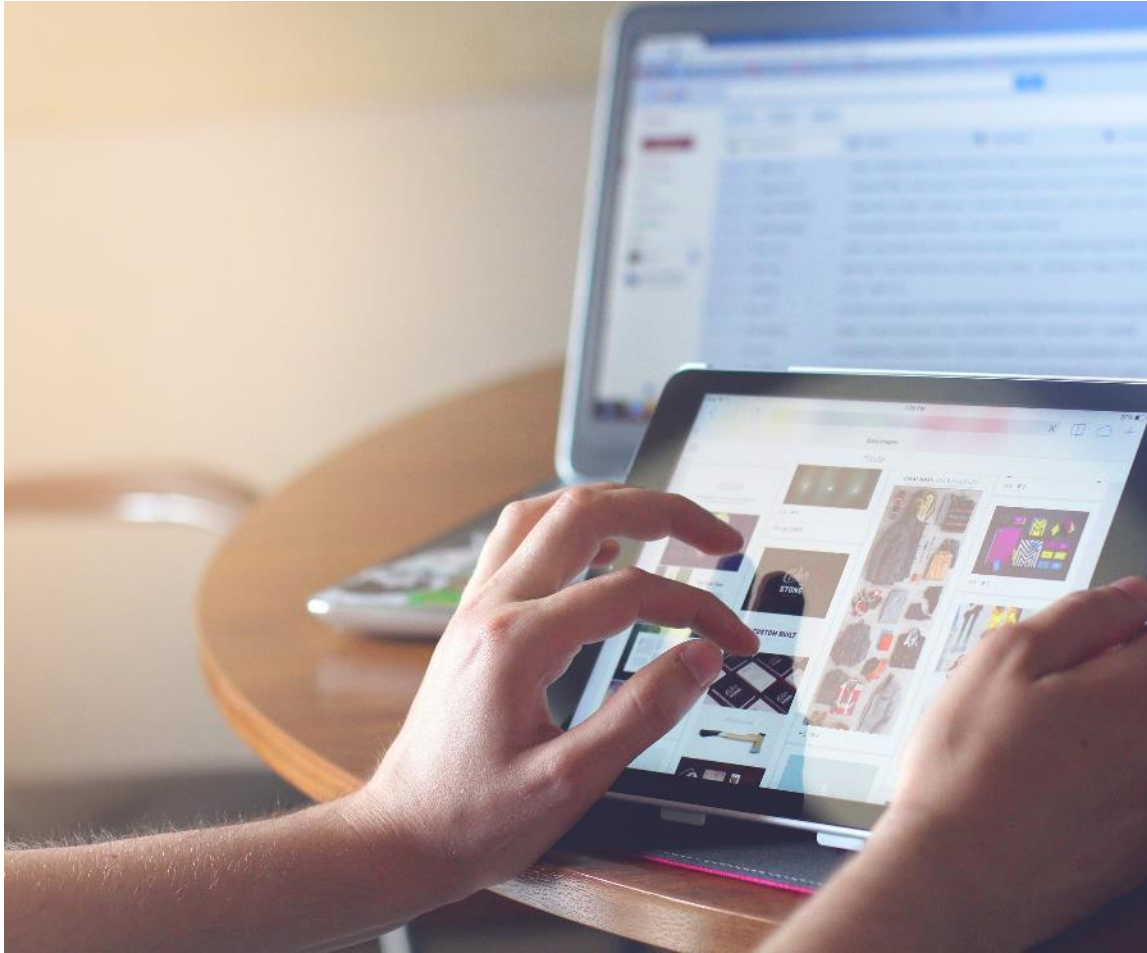
Source: SplashData

Algunos sitios que recomendamos de generación de contraseñas robustas...

<https://www.lastpass.com/es/password-generator>,
<https://www.dashlane.com/es/features/password-generator>,
<https://www.roboform.com/es/password-generator>,
<https://www.avast.com/es-ww/random-password-generator>,
<https://www.pandasecurity.com/es/homeusers/passwords-generator/>,

entre otros.

3. Uso del correo electrónico (ojo con el phishing)



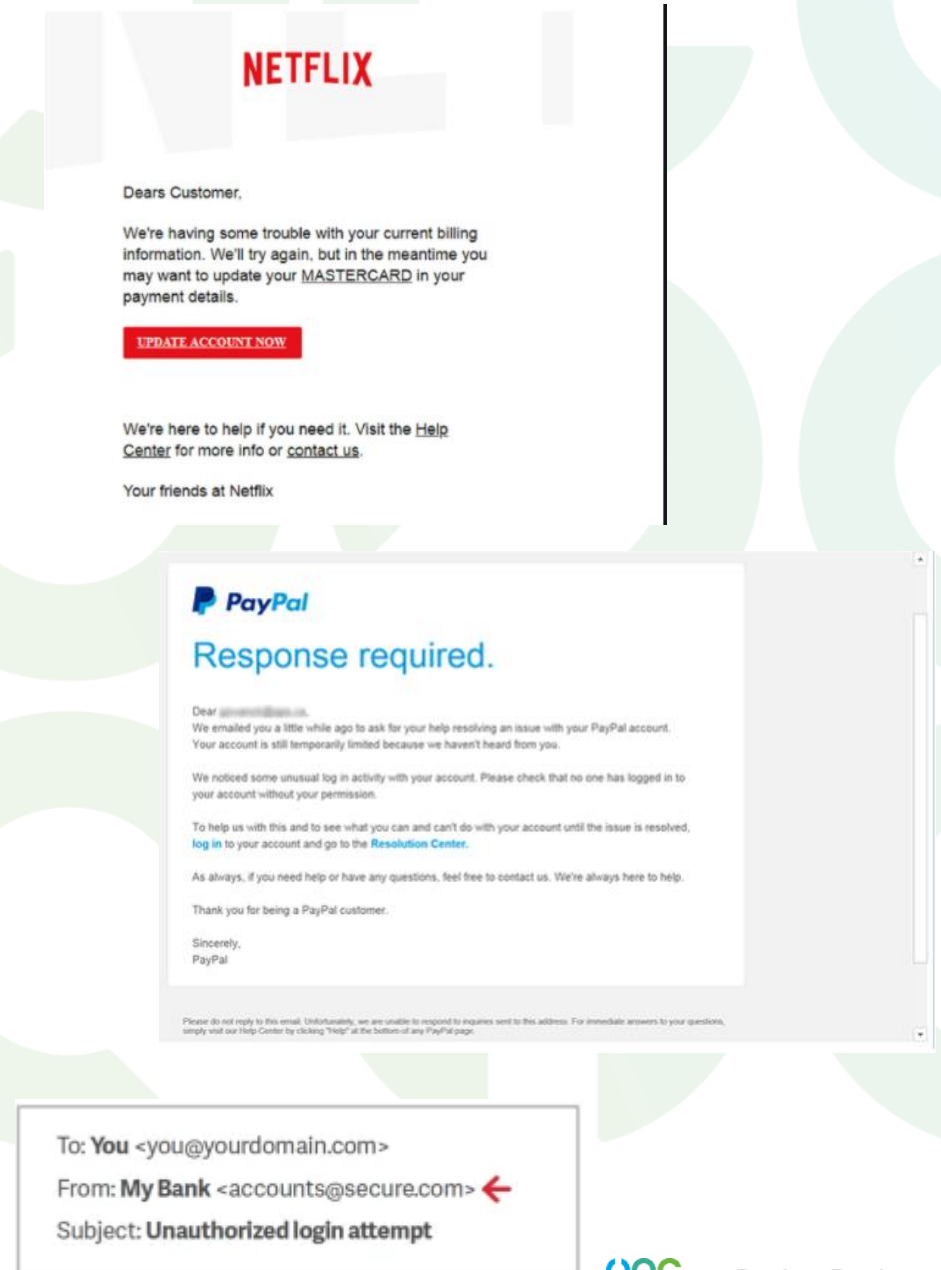
Prestá atención respecto a correos electrónicos fraudulentos, es decir campañas de phishing. A través de estos podríamos infectar el equipo con un malware o generar una fuga de información. O incluso que hagan uso de tus cuentas bancarias.

Algunas formas de reconocer el phishing

Recordá no hacer click en enlaces ni descargar archivos adjuntos que provengan de un remitente desconocido o sospechoso.

Utilizá el mail institucional, sobre todo para realizar intercambio de archivos oficiales. Si no poseés una cuenta, recomendamos que la solicites cuanto antes al sector correspondiente.

- 1) ¿El mensaje realmente demuestra que el remitente sabe algo acerca tuyo?
- 2) Espera lo peor de los archivos adjuntos y los vínculos integrados, No hagas clic.
- 3) No confíes en el nombre para mostrar.
- 4) Cuidado con el lenguaje urgente o amenazante en la línea de asunto.
- 5) Los mensajes **solicitan verificar información personal**, como detalles de tus bancos o una contraseña.
- 6) El mensaje **está mal escrito y suele contener faltas de ortografía**.



4. Seguridad de la información

Siempre que sea posible trabajá los archivos desde la Nube, es decir, no los descargues localmente a tu dispositivo para editarlos. La mayoría de los servicios de este tipo cuentan con editores online.

- Asegurate de sincronizar bien todos los archivos para así evitar pérdidas de información.
- No almacenes información sensible y/o confidencial en memorias USB o discos extraíbles personales.
- No publiques información personal en las redes sociales.



Tu información personal ¡cuidala...!



FUENTES

<https://www.csirt.gob.cl/media/2020/03/Protocolo-de-seguridad.pdf>
<https://www.welivesecurity.com/la-es/2020/03/16/recomendaciones-seguridad-teletrabajo-covid-19>
<https://espacionegocios.com.ar/6-medidas-de-seguridad-home-office-15233>
<https://www.facebook.com/OEAoficial/videos/2924929580883612>
<https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene>

EVITA PUBLICAR EN INTERNET

1 Tu domicilio y cuando estés o no en casa.

Mañana vacaciones. ¡Una semana fuera de casa!

Así no se lo pondrás tan fácil a delincuentes como ladrones.



 de Octubre

¡MUCHAS GRACIAS!



CLICK TO EDIT MASTER SUBTITLE STYLE



CLICK TO EDIT MASTER SUBTITLE STYLE



CLICK TO EDIT MASTER SUBTITLE STYLE



CLICK TO EDIT MASTER SUBTITLE STYLE