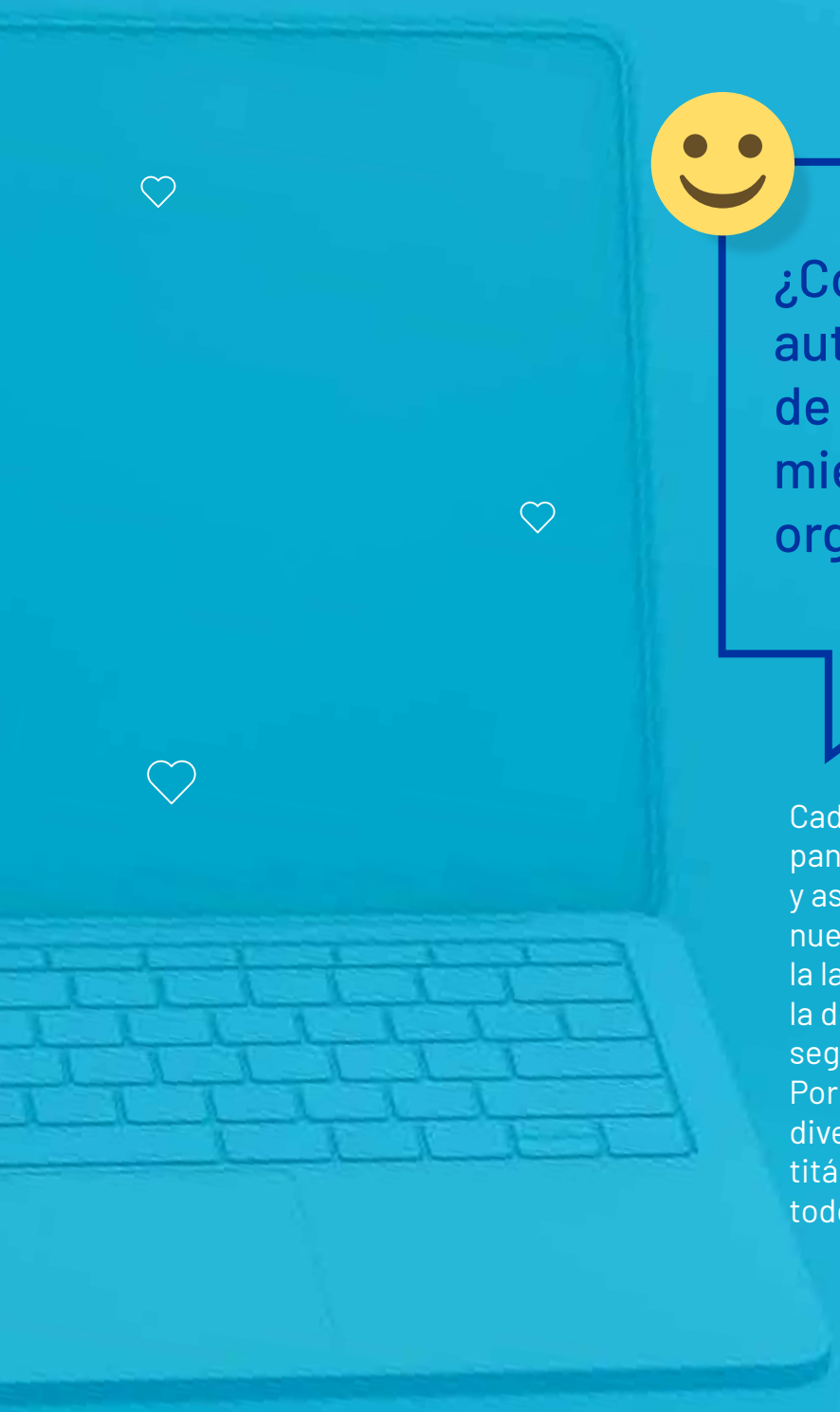


# ¿Cómo podemos autogestionar la prevención de riesgos cibernéticos como miembros de una organización?

Cada día, cuando nos sentamos frente a una pantalla para comenzar nuestras labores diarias y asumir el rol que tenemos al interior de nuestra compañía, debemos ser conscientes de la labor a realizar en pro de nuestra seguridad y la de nuestra empresa: ser guardianes de la seguridad y protectores de la información. Por esto, es fundamental tener presente las diversas recomendaciones para lograr esta titánica tarea, pues la seguridad es tarea de todos.

# Uso seguro de nuestras redes sociales

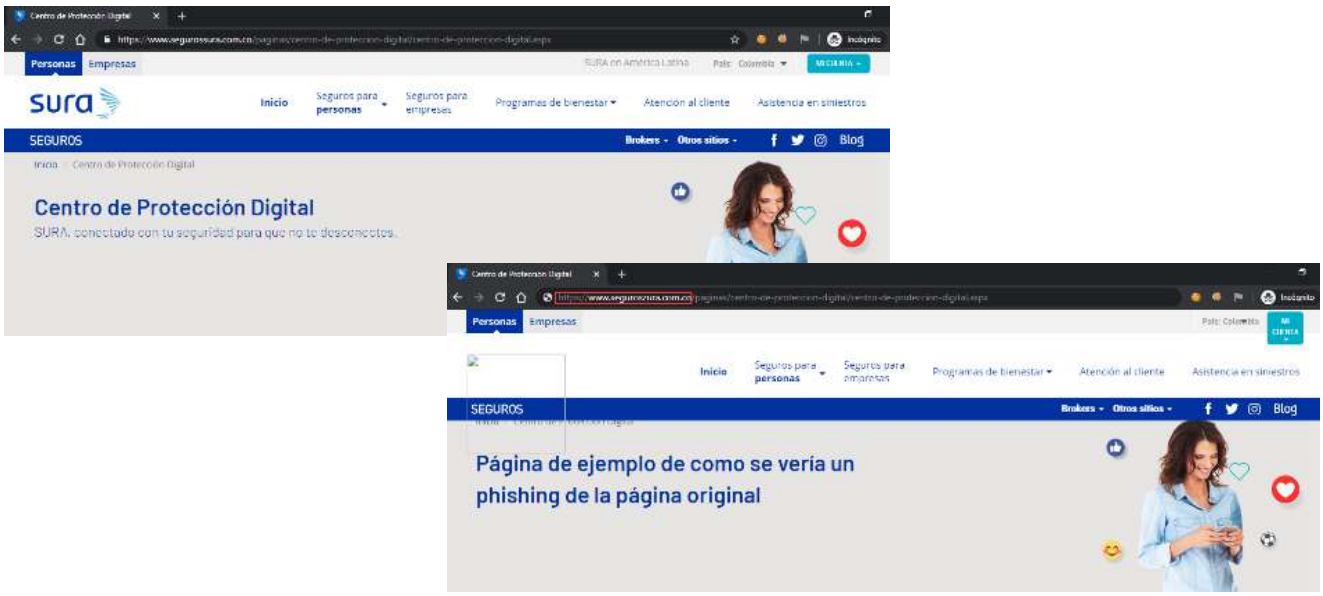
Es muy probable que empecemos el día dedicando un momento en la mañana para revisar nuestras redes sociales y WhatsApp para enterarnos de lo nuevo que ha sucedido en el mundo desde la última vez que las revisamos o, incluso para ver si ya recibimos respuesta de algo en lo que estamos interesados.

De manera muy desprevenida, es posible que nos estemos exponiendo a diversos riesgos cibernéticos. Estos ataques no solo van detrás de conseguir acceso a las grandes infraestructuras tecnológicas, sino que también van por la información de las compañías y ***su conocimiento construido (Know-How)***, la información de sus clientes (como nombre y número de identificación, información financiera, información de su salud o algún otro dato que se pueda considerar como sensible o incluso confidencial) y, por supuesto, nuestra información como empleados, nuestras credenciales para acceder a los recursos de la compañía o, incluso, algo tan básico como nuestra computadora o celular y su capacidad de procesamiento para luego ser utilizados en otros ataques. Por esto, es importante conocer cómo protegernos y enfrentar estos ataques para evitar ser víctimas de los cibercriminales.

Al dedicar un tiempo en redes sociales, recuerda que no toda la información allí compartida será verídica. Por lo tanto, verifica primero su veracidad en fuentes confiables que tengas identificadas al compartirla, ya que puedes terminar compartiendo noticias falsas o fake news, o algún enlace malicioso con el que puedan robarle información a otra persona.

Para validar el origen de un enlace, pasa el cursor por encima del vínculo si estás en un computador. Si estás en un dispositivo móvil, deja tu dedo sobre el enlace sin hacer clic y valida que la ruta que te aparece en la esquina inferior izquierda de tu dispositivo es un dominio que conoces y no uno malformado.

Con dominio nos referimos a la dirección que aparece en la parte superior izquierda de nuestros navegadores cuando queremos navegar hacia alguna página. Por ejemplo, si navegamos hacia la página del Centro de Protección Digital de SURA, veremos lo siguiente: *https://www.segurossura.com.co/cpd* con lo que nuestro dominio será segurossura.com.co. El dominio será entonces aquello que esté entre **https://** y el siguiente **/**. Si, por ejemplo, el dominio que visualizaras fuera seguroszura.com.co, sabrías que alguien te quiere engañar pues tiene una **Z** en vez de una **S** y no se corresponde con el dominio real de la Compañía. Por lo tanto, no deberías entrar a dicho dominio ni compartir esta noticia. Estos casos se deben de reportar a la entidad que están intentando suplantar para que esté atenta.




## 1

Una recomendación esencial a la hora de acceder a nuestras redes sociales es la de fortalecer nuestra contraseña, de modo que para los ciberdelincuentes sea lo más complejo posible llegar a la misma, o incluso imposible. Para ello, te recomendamos la siguiente ***guía de construcción para una contraseña segura*** que hemos desarrollado para este fin.

**Tus contraselas deben ser:**

- Secretas
- Aa1Bc25*
- Robustas
- ***
- No repetidas
- Cambiarlas periódicamente

## 2

Otra recomendación para asegurar el acceso en nuestras redes sociales es habilitar el segundo factor de autenticación, que será como una doble chapa en una puerta, con lo que deberemos tener dos llaves para acceder a nuestra casa. Esta doble protección se basa en algo que conocemos (nuestra contraseña) y en algo que tenemos (nuestro dispositivo móvil), aunque también podría agruparse con algo que somos (nuestra huella dactilar). Con esto, un cibercriminal que desee acceder a nuestras redes sociales deberá conocer nuestra contraseña, pero también deberá tener nuestro dispositivo o nuestra huella dactilar. Para realizar estas configuraciones en las redes sociales, te recomendamos:

Consultar los ***manuales*** que hemos construido para ello.

Acceder a tus redes sociales desde dispositivos y redes de confianza como por ejemplo tu red WiFi o red celular, evitando acceder desde redes en las que no confíes como una WiFi abierta que encuentres en la calle o la red pública del centro comercial. Con esto evitarás que un cibercriminal pueda acceder a la información que tienes en las redes sociales.

# USO SEGURO DE NUESTRAS APLICACIONES Y EL CORREO CORPORATIVO

Después de haber hablado de la seguridad en nuestras redes sociales, nos detendremos ahora para revisar diferentes mecanismos que podemos utilizar a la hora de protegernos de los cibercriminales en el ejercicio de nuestra actividad laboral:

## 1

Igual que en las redes sociales, es vital que la contraseña de tu usuario corporativo sea una contraseña robusta. Incluso, si tu empresa te ofrece la posibilidad de fortalecer el acceso por medio de doble factor de autenticación, procede a configurarlo o acceder al servicio de soporte dispuesto para ello. Este factor podrá apalancarse desde nuestro celular con un código que nos llegue cada vez que ingresamos nuestra contraseña, hasta el lector de huellas que tal vez tenga tu equipo de trabajo. De esta manera, evitamos que un cibercriminal conociendo solamente nuestra contraseña pueda acceder a las aplicaciones de la empresa.

## 2

En caso de que tengamos un acceso **VPN (Red Privada Virtual)** lo mejor será utilizarlo, dado que, si estamos en una red que no es confiable, al utilizarla **ciframos (aseguramos)** las comunicaciones entre nuestro dispositivo y la empresa, de tal forma que el cibercriminal que se encuentre en dicha red no será capaz de obtener información sensible de la empresa.

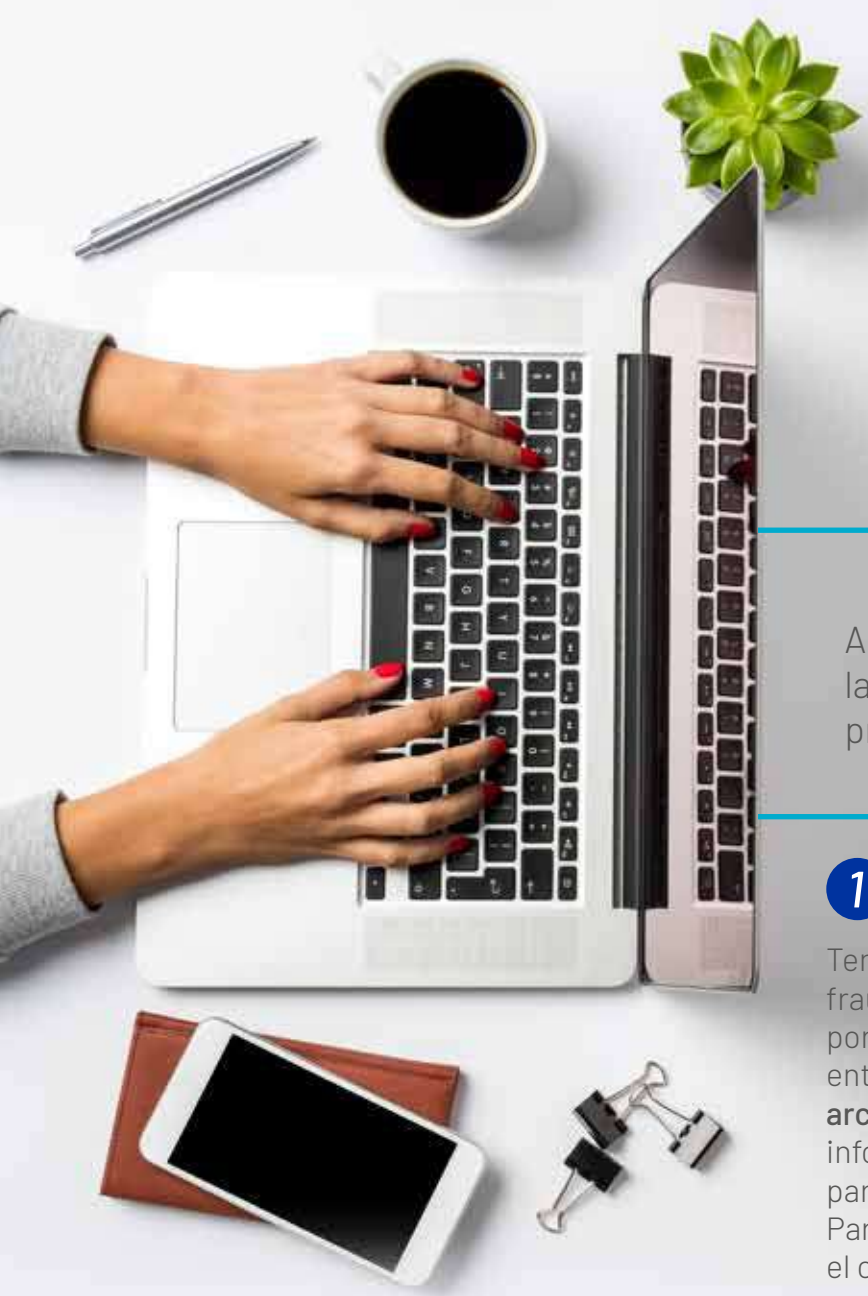
3

Cuando navegues en Internet, verifica siempre la presencia del candado en la barra de direcciones y evita hacerlo en sitios que presenten el siguiente mensaje de alerta ⚠ No es seguro | ~~https://~~ o si te aparece la frase de *"No es seguro"* ⓘ No es seguro | , ya que en estos últimos dos casos un cibercriminal podría interceptar lo que escribas en esas páginas y, por ejemplo, conocer tus credenciales o modificar lo que estés haciendo para suplantarte y robarte información sensible (como información bancaria o de los clientes). Si el dominio (dirección electrónica) hacia el cual navegas es de confianza porque lo conoces, habla con la línea de soporte de tu compañía o con las personas encargadas del área tecnológica, ya que puedes estar siendo objetivo de un ciberataque.



*Página con https no válido*


*Página sin https*

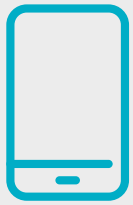


Al usar tu correo electrónico laboral, ten las siguientes precauciones:

**1**

Ten cuidado con correos malintencionados y fraudulentos (Phishing), que intentan hacerse pasar por personas de tu organización o de otras para que entres a **dominios fraudulentos** o descargues **archivos adjuntos** que posibiliten robos de información o instalación de programas indeseados para capturar credenciales o adueñarse de tu equipo. Para hacerle frente a este tipo de ataques, valida que el correo de la persona que te escribe es de confianza, por ejemplo, si el correo de tu jefe es *tujefe@sura.com.co* y te llega un correo de *tujefe@zura.com.co* sabrás que no es un correo válido y que, por el contrario, los cibercriminales quieren robar tu información. Reenvía dicho correo en modo adjunto al área de tecnología o seguridad de tu organización para que puedan tomar acciones al respecto y evitar que alguno de tus compañeros caiga en dicha estafa.

Igualmente, si dudas si una persona fue la que realmente te envió un correo, una llamada puede ser la mejor opción para validar que efectivamente dicho correo es seguro. Otra forma de validar la veracidad del correo es revisar, al igual que lo hicimos en redes sociales, los links o vínculos que se encuentran en él. Antes de hacer clic sobre ellos, valida que efectivamente te lleven al dominio correcto.



2

Evita vincular tu correo corporativo con aplicaciones que no se relacionan con tu trabajo (como LinkedIn u otra red social personal), de tal forma que los cibercriminales no tengan un gran campo de aplicaciones sobre el cual recabar información de tu empresa.

3

En tu entorno laboral, evita utilizar las mismas contraseñas de otras aplicaciones que salen de dicho ámbito, de tal forma que si por ejemplo un cibercriminal logra hallar una contraseña que utilizabas en una aplicación de juegos, no sea posible que con la misma contraseña logre entrar a tu correo corporativo.

4

Al momento de descargar archivos adjuntos que te envíen, valida que efectivamente quien lo envió es quien dice ser y que te dé la certeza de que es un correo seguro. Desconfía en especial cuando te envían un archivo comprimido con contraseña, es posible que contengan virus. Si por algún motivo descargaste dicho archivo, llama al equipo de tecnología para que te ayude. Si descargaste un archivo que creías confiable y al abrir el comprimido te encuentras con una extensión desconocida, no prosigas, los ciberdelincuentes suelen esconder malware en ellos e incluso lo suelen hacer también al interior de archivos de Word, Excel, PDF, y otras extensiones comunes. Por ejemplo, si descargas un archivo Excel y te pide habilitar las macros, solo hazlo en caso de estar seguro de que así debe ser. Hay macros diseñadas para el robo de información y captura de tu equipo.

5

Ten cuidado con los correos que utilizan términos que denotan urgencia o que despiertan curiosidad. Los cibercriminales se aprovechan de la cualidad del ser humano de ser colaborativos y curiosos, y nos llevan a descargar archivos o a hacer clic en vínculos maliciosos. Por ejemplo, hablan del cierre de tus cuentas bancarias y te proporcionan un enlace para recuperarlas, te hablan sobre una infidelidad y te proporcionan un archivo comprimido con contraseña o te escriben por una multa de tránsito cuando ni siquiera tienes vehículo. En estos casos recuerda, ante todo, mantener la calma y analizar lo que sucede, de tal forma que lo puedas validar con el equipo de tecnología de tu compañía. En ocasiones, hasta te podrán escribir correos con tu propio nombre, como si efectivamente fuera algo para ti. Te compartimos la siguiente página, en la cual podrás practicar tus habilidades reconociendo un correo malicioso: https://phishingquiz.withgoogle.com/

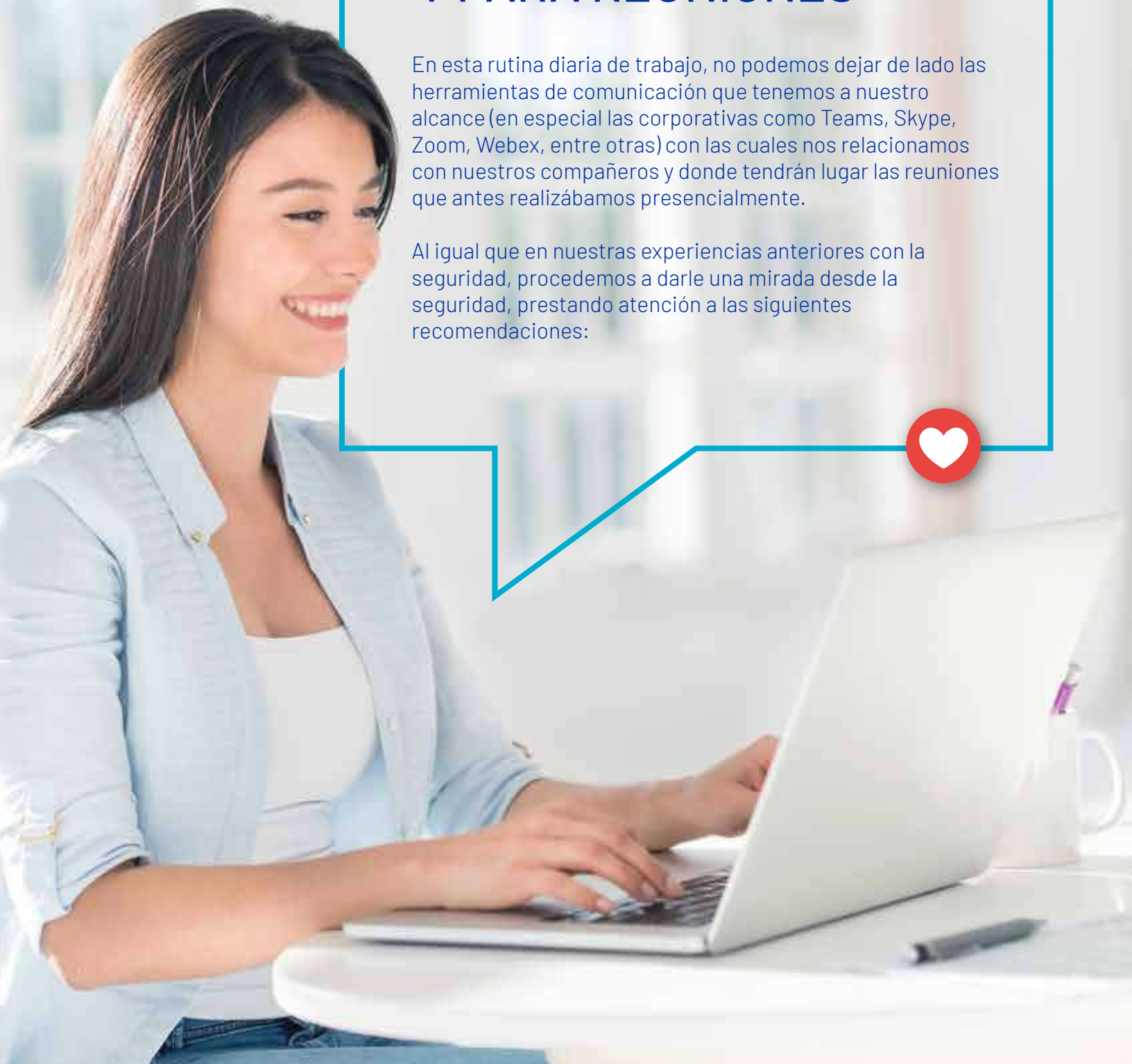
6

Recuerda validar con el equipo de tecnología si cuentan con un respaldo de la información. Es importante que la información sensible de la compañía tenga dicho respaldo en caso de alguna pérdida.

# USO SEGURO DE HERRAMIENTAS COLABORATIVAS Y PARA REUNIONES

En esta rutina diaria de trabajo, no podemos dejar de lado las herramientas de comunicación que tenemos a nuestro alcance (en especial las corporativas como Teams, Skype, Zoom, Webex, entre otras) con las cuales nos relacionamos con nuestros compañeros y donde tendrán lugar las reuniones que antes realizábamos presencialmente.

Al igual que en nuestras experiencias anteriores con la seguridad, procedemos a darle una mirada desde la seguridad, prestando atención a las siguientes recomendaciones:



1

Asegúrate de tener una contraseña robusta y habilitar el segundo factor de autenticación en tus herramientas colaborativas.

2

Ten cuidado con los vínculos y los archivos que te envían a través de las plataformas colaborativas cuando estás con personas desconocidas en una reunión, ya que podrían ser maliciosos.

3

Si depende de ti, ten actualizadas las versiones de dichas aplicaciones, pues frecuentemente los profesionales de la seguridad encuentran brechas en dichos sistemas que pueden ser utilizadas por los cibercriminales. Si no depende de ti, solicita al equipo de tecnología que actualicen las versiones de las mismas, ya que sobre ellas puede gestionarse información crítica de la compañía.

4

Procura generar una contraseña robusta para tus reuniones de tal forma que un cibercriminal no sea capaz de entrar a la reunión y extraer información útil de la misma o generar malestar a los asistentes.

5

Instala las aplicaciones de conectividad y colaboración que utilices desde las plataformas oficiales destinadas para ello (Microsoft Store, Google Play, App Store, Galaxy Store, entre otras) pues existen páginas dedicadas a implantar malware (software malicioso) en dichas aplicaciones y, si bien es posible que la aplicación te funcione, también es posible que te terminen robando información. A veces es mejor pagar un poco por la aplicación que utilicemos, a que sean nuestros datos o los de la empresa con los que terminemos pagando el uso de la aplicación.

6

Si sospechas que tu equipo ha sido infectado con algún malware o que tus credenciales han sido robadas, recuerda reportarlo al equipo de tecnología. Ellos te ayudarán a protegerte y a proteger a tus compañeros para que este no se replique.

7

Cuando recibas llamadas telefónicas de números que no tengas identificados, actúa con la mayor cautela posible. Si preguntan "¿Con quién hablo?", devuelve la pregunta indicando "¿A quién necesita?", ya que si nos llaman es porque deben saber a quién están buscando. Si luego de indicar tu nombre se identifican como personal de la Mesa de ayuda o del equipo de tecnología indicando nombres conocidos, asegúrate de que efectivamente son quien dicen ser, ya que muchos ataques de este tipo, llamados Vishing, intentan recopilar la mayor cantidad de información posible sobre tu contexto para parecer creíbles y permitir que a la final le entregues información valiosa sobre tu compañía.

Asegúrate, por tanto, que te escriban por un medio corporativo antes de proceder con cualquier requerimiento y tener las garantías de quien te llama es efectivamente la persona que dice ser.

8

Los equipos de tecnología o Mesa de ayuda no requieren conocer tu contraseña para poder ejecutar acciones sobre tu equipo. Si son quienes dicen ser, podrán ayudarte sin necesidad de que les reveles una contraseña.

9

Cuando te llegue un mensaje de texto, ten cuidado con los vínculos que te envíen o "cupones" para redimir en domicilios u otros beneficios, ya que podrían ser maliciosos o, incluso, ir acompañados de una llamada en la cual te soliciten dicho código para hacer efectivo el cupón, pero realmente lo que estarán haciendo será robarte el acceso a una cuenta por medio de la recuperación del doble factor de autenticación. Esta técnica se llama Smishing. Tu equipo técnico o la Mesa de ayuda no deberían de solicitarte dicho número.

10

Con estas recomendaciones harás un gran trabajo, le harás la vida más difícil a los cibercriminales y más fácil a tu equipo de tecnología para que puedan protegerte de mejor manera a nivel técnico. Recuerda que eres la primera barrera frente a un ciberataque y, por más tecnología que tenga una organización, si como empleados que somos no hacemos frente a estos ciberataques, estaremos todos expuestos. Te invitamos entonces a que protejamos nuestras organizaciones y evitemos ser víctimas de los cibercriminales. La seguridad es una tarea de todos.

sura



segurossura.com.co