

# Cómo mantener la seguridad de su organización dentro y fuera de la oficina

La seguridad de su organización debe ser siempre una de sus prioridades, tanto si trabaja desde casa como si lo hace en una oficina. Aunque a priori diríamos que existen muchas diferencias entre ambas modalidades, en realidad las precauciones que debe tener con el trabajo local o remoto son las mismas. Veamos algunas normas importantes de ciberseguridad y cómo pueden aplicarse tanto en la oficina como cuando se trabaja en casa.

## Use solo dispositivos seguros

- Recuerde que el nivel de seguridad de su dispositivo lo marcan las aplicaciones que tiene instaladas. No instale nunca una aplicación o un complemento sin consultar antes con el Departamento de Informática.
- Para trabajar, use solo dispositivos de trabajo. Si utiliza un ordenador personal para trabajar, le recomendamos que cree otra cuenta de usuario con un nombre de usuario y una contraseña únicos.
- En la oficina, es probable que la seguridad de la red sea responsabilidad del Departamento de Informática. Para mantener segura una conexión a Internet doméstica, configure una contraseña compleja en el router. Si la organización ofrece acceso a una red privada virtual (VPN), conéctese también a ella.

## Proteja su espacio de trabajo físico

- En la oficina, tenga cuidado con las credenciales «prestadas» y la infiltración. Hablamos de credenciales «prestadas» cuando alguien que dice formar parte de la organización le sigue hasta una zona segura sin utilizar una tarjeta de identificación o un código de entrada. La infiltración consiste en esperar a que alguien entre o salga de una zona segura y luego colarse mientras la puerta sigue abierta. Sospeche de cualquier persona que no reconozca y no tenga reparo en pedirle una identificación.
- En casa, instátese en un espacio de trabajo privado y cómodo, donde nadie pueda ver la pantalla mientras trabaja. Debe impedir que la información confidencial de la empresa quede a la vista de personas no autorizadas, lo que incluye a su pareja, sus hijos y sus amigos.
- Bloquee siempre el equipo cuando se levante de la mesa de trabajo. Si no bloquea el ordenador, cualquiera podría utilizarlo para acceder a información confidencial, robar las credenciales de inicio de sesión o incluso instalar malware.

## Piense antes de hacer clic

- No haga nunca clic en ningún enlace ni descargue ningún adjunto de un correo electrónico que no esperara recibir. Aunque el remitente parezca ser de una organización conocida, es posible que la dirección de correo electrónico haya sido suplantada.
- Cuando se le solicite en un correo electrónico que inicie sesión en una cuenta o servicio en línea, navegue hasta ese servicio con un explorador. No haga nunca clic en el enlace del correo electrónico. Vaya al sitio web directamente y, de esa manera, se asegurará de iniciar sesión en el sitio web real y no en uno que imite su apariencia.
- En caso de duda, llame al remitente del correo electrónico para confirmar que la solicitud, el enlace o el archivo adjunto son legítimos. No llame al número de teléfono incluido en el correo electrónico, porque podría ser falso.

