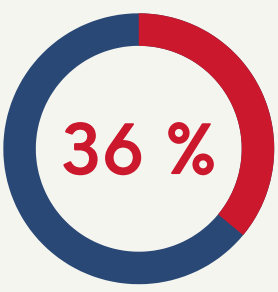
Trabajar desde casa

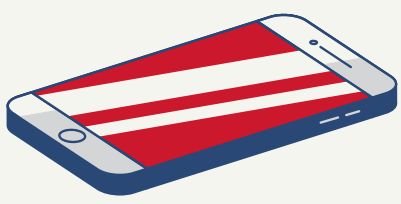
Precauciones, riesgos y posibles consecuencias

¿Sabías que trabajar desde casa conlleva riesgos adicionales?

Casi tres millones de empleados en España trabajan a distancia, un millón más que hace un año.



El incremento de CIBERDELITOS subió un 35,8% con respecto al 2018



Precauciones de seguridad para tu oficina en casa

En tu Router:

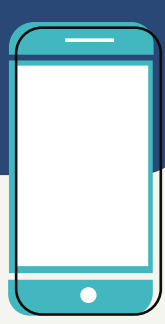
- Cambia la contraseña de administrador predeterminada de tu router WiFi por una contraseña única y segura.
- Activa la actualización automática del firmware de tu router WiFi.
- Crea una red de invitados para visitantes y dispositivos que no sean de confianza.

En tus Conferencias virtuales:

- Utiliza únicamente software autorizado para conferencias virtuales y asegúrate de que siempre está actualizado a la última versión.
- Asegúrate de no tener información personal o sensible visible al compartir tu pantalla, o cuando la cámara esté habilitada.
- No compartas tus invitaciones a reuniones con terceros.

En tu móvil :

- Mantén actualizados el sistema operativo y las aplicaciones de tu dispositivo móvil.
- Habilita el bloqueo de pantalla para proteger tu dispositivo móvil.
- No respondas a ninguna notificación sospechosa de aplicaciones de móvil o mensajes de texto SMS solicitando de forma urgente que hagas clic en un enlace, envíes dinero o compartas información confidencial.
- Cuelga inmediatamente si recibes una llamada sospechosa o urgente presionándote para que tomes algún tipo de acción inmediata.



En tu ordenador:

- Habilita la actualización automática siempre que sea posible en todos tus dispositivos personales.
- Avisa inmediatamente al departamento de Tecnología si sospechas que tu sistema se ha visto comprometido; no intentes arreglar por tu cuenta un equipo hackeado.
- No permitas que los miembros de la familia usen tu dispositivo de trabajo.

En tu conexión VPN:

- Nunca compartas con nadie la información de tu acceso por VPN (por ejemplo, la contraseña de tu usuario).
- Asegúrate de seguir las políticas de la empresa sobre el uso correcto del acceso vía VPN.

En tus passwords :

- Habilita y usa Autenticación Multi-Factor siempre que sea posible.
- Crea para cada cuenta una contraseña única, fuerte y larga, mediante el estilo frase de contraseña (o "passphrase").

TOP 3

RIESGOS

PARA TRABAJADORES REMOTOS

1

Passwords débiles

Se trata de una de las principales causas de ciberincidentes a escala global. Contraseñas cortas u obvias, y usar la misma contraseña para múltiples cuentas, puede hacerte vulnerable a los ciberdelincuentes.

2

Ataques de ingeniería social

Los trabajadores en remoto pueden ser especialmente vulnerables a ataques de phishing o llamadas telefónicas maliciosas, dado que a menudo son responsables de su propia seguridad.

3

Sitemas o software desactualizados

Es posible que, mientras trabajes en remoto, no tengas acceso al parcheado automático software o firmware, y por tanto estés trabajando con dispositivos desactualizados. Una red inalámbrica doméstica puede ser menos segura, y no puede ser protegida por la empresa en todo momento.