La ciberseguridad es responsabilidad de todos

Trabajamos juntos para proteger nuestro negocio y a nuestros clientes

USO ACEPTABLE

PARA ACTIVOS DIGITALES

No intente eludir o desactivar

las medidas de seguridad de su ordenador para acceder a contenidos que puedan poner en riesgo a la empresa, como visitar sitios web bloqueados.

No instale

ni utilice aplicaciones no autorizadas por la empresa.

No comparta

su nombre de usuario y contraseña corporativos con nadie, ni siquiera con compañeros de trabajo o terceros.

No haga clic

en enlaces o archivos adjuntos sospechosos en correos electrónicos. En caso de duda, informe.

Recuerde

- Los ciberdelincuentes se aprovechan de los **errores humanos o del incumplimiento de las normas** en sus ciberataques.
- **Desconfigurar** su antivirus, instalar **software pirata** o **utilizar VPN** para eludir los controles de su ordenador son algunas de las acciones que ponen en peligro la seguridad de su empresa.

- Utilice el instalador de aplicaciones corporativas para acceder de forma segura a las herramientas proporcionadas por la empresa.
- Si necesita otras aplicaciones o programas específicos para su trabajo, **utilice ITNow** para solicitar una **autorización individual para cada uno de ellos**.
- **No utilice navegadores alternativo**s ni acceda a Internet para descargar o entrar en sitios web prohibidos y no seguros. Estos sitios web son visitados con frecuencia por **ciberdelincuentes** y ponen en grave peligro su ordenador.

- Tu nombre de usuario y contraseña corporativos son **privados y nunca deben compartirse**. Son para tu uso y protección: **no los reveles**.
- Está **prohibido reutilizar** las credenciales y el correo electrónico corporativo en otros sistemas y servicios personales.
- No olvides que **no debes anotar** tus contraseñas de bloqueo ni tus credenciales corporativas en notas adhesivas o cuadernos.

- Los **ataques de phishing** por correo electrónico son la principal vía de entrada de los **ciberataques a las empresas**.
- **Compruebe** siempre la **autenticidad del remitente**. En caso de duda, verifíquelo poniéndose en contacto con el remitente a través de otro canal, por ejemplo, llamándole por teléfono.
- Reconozca las **señales de alerta** de estos intentos de estafa, como mensajes con solicitudes urgentes o amenazas, y errores gramaticales o de diseño.