Recomendaciones de seguridad informática

recomendaciones | prácticas desaconsejables | peligros
incidentes que deben notificarse | cómo mantenerse seguro

SOPHOS

La seguridad es responsabilidad de todos. Siga los consejos incluidos en este manual para protegerse
y proteger tanto a sus compañeros como la empresa.

La seguridad nos ofrece la libertad para hacer bien nuestro trabajo. Es muy fácil
y, en la mayor parte de los casos, cuestión de sentido común.

Informe a sus familiares y amigos para que naveguen por Internet de forma segura.

No caiga en la trampa de revelar información confidencial

1

No conteste a mensajes de correo electrónico ni llamadas telefónicas que soliciten información confidencial de la empresa, incluidos datos de los empleados, resultados financieros o secretos corporativos.
Cualquiera puede llamarnos y hacerse pasar por un empleado o un socio.

Esté atento para no caer en este timo e informe al departamento informático sobre cualquier actividad sospechosa.
Y proteja su información personal con el mismo cuidado.

2 No utilice equipos sin proteger

Al acceder a información delicada desde un equipo sin proteger como, por ejemplo, en un cibercafé o un equipo doméstico compartido, estará poniendo en peligro la información visualizada.

Asegúrese de que el equipo cuenta con los parches de seguridad aprobados más recientes, antivirus y cortafuegos. Y utilice el equipo en modo de usuario siempre que sea posible, en lugar de en modo de administrador.

No deje información delicada a la vista en la oficina

3

No deje documentos impresos que contengan información privada encima de la mesa. Guárdelos en un cajón o tritúrelos. Cualquiera que pase por allí podría verlos fácilmente.

Mantenga el escritorio ordenado y los documentos guardados en un lugar seguro. De esta forma, la oficina tendrá un aspecto más ordenado y correrá menos riesgos de que se produzcan filtraciones de datos.

4 Bloquee el ordenador y el teléfono móvil cuando no los esté utilizando

Bloquee siempre los equipos y los teléfonos móviles cuando no los esté utilizando.
Su trabajo es importante y queremos asegurarnos de que la información está segura.

Al bloquear los teléfonos y los ordenadores, los datos y los contactos estarán a salvo de

Esté pendiente y notifique cualquier actividad sospechosa

5

Informe siempre al departamento informático sobre cualquier actividad sospechosa. Bloquear ataques informáticos y asegurarnos de que sus datos no sufren robos ni extravíos es parte de nuestro trabajo.

Todos nuestros puestos dependen de que la información esté segura. Si pasa algo, cuanto antes lo sepamos, antes podremos ponerle solución.

6 Proteja con contraseñas los archivos delicados y los dispositivos

Proteja siempre con contraseñas los archivos delicados almacenados en ordenadores, unidades USB, teléfonos inteligentes, etc.

Cualquiera puede perder un teléfono, una memoria USB o un portátil. Al protegerlos con contraseñas seguras, es mucho más difícil que alguien consiga robar datos.

Utilice siempre contraseñas difíciles de averiguar

7

No utilice contraseñas obvias como "contraseña" o "gato", ni secuencias del teclado como "asdfg" o "12345". Es mejor utilizar contraseñas complejas* que incluyan mayúsculas y minúsculas, números e incluso signos de puntuación.

Intente utilizar contraseñas diferentes en cada sitio web y en cada equipo. De esta forma, si una cuenta sufre un ataque, las demás estarán a salvo.

*$i3t3O$O$enMi|<@$^
(siete osos en mi casa)

8 Tenga cuidado con los mensajes y enlaces sospechosos

No deje que le pierda la curiosidad.

Elimine siempre los mensajes y los enlaces sospechosos.
Con solo abrirlos o visualizarlos, puede poner en peligro su equipo y provocar problemas sin saberlo.

Recuerde que, si algo parece demasiado bonito para ser cierto, probablemente lo sea.

No conecte dispositivos personales sin la autorización del departamento informático

9

No conecte dispositivos personales como unidades flash USB, reproductores de MP3 o teléfonos inteligentes sin el permiso del departamento informático.

Estos dispositivos pueden infectarse con código listo para iniciarse en cuanto los conecte a un ordenador.

Hable con el departamento informático sobre los dispositivos y siga nuestras recomendaciones.

10 No instale programas no autorizados en el ordenador del trabajo

Las aplicaciones maliciosas suelen presentarse como programas legítimos, por ejemplo, juegos, herramientas o incluso programas antivirus.

Su intención es engañar a los usuarios para infectar los equipos o la red.

Si le gusta una aplicación y cree que puede serle útil, póngase en contacto con el departamento informático para que la investiguen antes de instalarla.

Una tarea constante

Los ordenadores no van a desaparecer y, por lo tanto, tampoco las amenazas. Por eso, esta lista cambiará con el tiempo, a medida que encontremos y superemos nuevas amenazas.

No se pierda las actualizaciones del Manual de recomendaciones de seguridad informática para empleados para no verse en situaciones comprometidas ni poner a la empresa en peligro.