

Reducir el riesgo del teletrabajo

Un mejor equilibrio entre la vida profesional y personal, el aumento de la productividad, la seguridad de los empleados y el ahorro de tiempo y dinero son solo algunas de las razones por las cuales las empresas están adoptando el teletrabajo. Este cambio en la forma de trabajar conlleva un riesgo: un mayor riesgo de fuga y violación de datos.

Mantenga su empresa y sus empleados seguros y protegidos con estos 7 consejos.

1. Establecer reglas

Definir un conjunto de reglas claras para el teletrabajo, también teniendo en cuenta la destrucción segura de información confidencial que puede producir mientras se trabaja fuera del lugar habitual.

2. Informe a sus empleados

Informe a sus empleados sobre las mejores prácticas de gestión de la información segura y su destrucción. Asegúrese de que todos los empleados tienen conocimiento acerca de lo que se considera información confidencial y las consecuencias para su negocio si se produce una violación o fuga de datos.

3. Limite el acceso a datos confidenciales

Asegúrese de que los empleados tengan el acceso correcto a los archivos correctos, según las necesidades.

4. Seguridad del dispositivo

Verifique que todos los archivos, dispositivos y conexiones a Internet están protegidos por contraseñas seguras y refuerce la seguridad en configuraciones y cortafuegos.

5. Teletrabajo seguro

Anime a los empleados a trabajar regularmente fuera del lugar de trabajo habitual, para que creen una caja de almacenamiento protegida para guardar los documentos importantes y confidenciales y que estén seguros.

6. Proteger documentos en papel

Asegúrese de que los empleados que trabajan fuera del sitio habitual retornan todos los documentos en papel al regresar a la oficina, ya sea para almacenamiento o para destrucción segura.

7. Implemente una política Shred-it All

Para garantizar que todos los documentos o la información confidencial se destruyen, implemente de forma segura una política Shred-it All para ayudar a evitar el riesgo de violación o fuga de datos.