FICHA INFORMATIVA

Guía de Shred-it para mantener sus datos seguros después de las vacaciones de verano

Los meses de verano son el período preferido por los empleados para disfrutar de sus merecidas vacaciones. Sin embargo, cuando regresan, es una buena práctica corporativa recordarles cómo manejar los datos confidenciales, lo cual es esencial para reducir el riesgo de una filtración de datos.

SABÍA QUE... ¿El coste medio de una filtración de datos es de 4,3 millones de euros? [1] Y que el 31% de los consumidores ¿perdería la confianza en una empresa que sufriera una filtración de datos? [2]

Estas son algunas sugerencias de seguridad que los empleados deben seguir, consideradas buenas prácticas, al regresar de sus vacaciones.

1. **Reducir la cantidad de datos almacenados en un dispositivo móvil,** conservando sólo lo imprescindible para sus funciones.
2. **Esté atento cuando trabaje de forma remota en una cafetería, aeropuerto o autobús.** Guarde los materiales de trabajo o muévase si alguien parece sospechoso.
3. **Evite compartir dispositivos electrónicos con familiares, amigos y extraños.** Bloquearlos cuando no estén en uso. Guarde los documentos sensibles y confidenciales en un lugar seguro.
4. **Tenga cuidado con los correos electrónicos de phishing y los sitios web maliciosos.** Algunos elementos que pueden alertarlo incluyen faltas de ortografía, errores gramaticales, direcciones de correo electrónico sospechosas y llamadas a la acción urgentes. Nunca envíe por correo electrónico datos personales como nombres, direcciones o detalles de tarjetas de crédito.
5. **Siga los procedimientos de su empresa para la destrucción segura de datos en papel y digitales.** No arroje papel en contenedores de basura o contenedores de reciclaje. No tire a la basura los dispositivos electrónicos inútiles. Llévalos a la oficina después del verano y entrégalos para su destrucción segura y definitiva.
6. **No conecte dispositivos USB desconocidos.** Utilice únicamente dispositivos aprobados por la empresa.
7. **En un lugar público,** no deje dispositivos móviles desatendidos o visibles en el automóvil.
8. **Actualice el software e instale los parches lo antes posible.** Los estudios confirman que el 82% de las filtraciones de datos registradas se debieron a una falla en la actualización de los parches. [3]
9. **Reforzar las contraseñas en todos los dispositivos y cuentas** (contraseñas de caracteres que incorporen números, letras y símbolos). Más del 60% de las infracciones involucran contraseñas de acceso. [4]
10. **Desactivar Wi-Fi y Bluetooth cuando no sean necesarios.** Para enviar o recibir elementos de información confidencial o conectarse a la red de la oficina, usar puntos de acceso personales, una red privada virtual (VPN) o redes Wi-Fi protegidas por contraseña. La conexión a través de Bluetooth cifra los datos.

[1] https://www.ibm.com/security/data-breach
[2] Shred-it Data Protection Report 2020
[3] Voke Media, Secure Operations Automation Market Snapshot report
[4] https://www.verizon.com/business/resources/reports/dbir/

Para obtener más información sobre las mejores prácticas de seguridad, visite Shredit.es o llame al 900 170 500

Protegemos lo que importa.

Shred-it®
Una Solución Stericycle®