¿ **La nueva forma de trabajar** está poniendo a las empresas en mayor riesgo de **sufrir una brecha de seguridad?**

Fellowes Encuesta **"Protege tus datos Confidenciales" 2022 .** Un informe sobre la **DESTRUCCIÓN** en un mundo laboral híbrido

Prólogo

> “Muchas empresas que se cambiaron a un modelo de trabajo remoto a principios de 2020 se dieron cuenta de que, simplemente, no tenían tiempo suficiente para llevar a cabo un análisis de riesgos en seguridad de datos para adaptarse a la nueva situación.”

“A inicios de la pandemia la atención de todo el mundo estaba centrada en garantizar que sus servicios pudieran continuar funcionando en vez que plantearse riesgos de seguridad que comportaban esos cambios necesarios. Además, los empleados tampoco tuvieron tiempo para adaptarse a la nueva forma de trabajar y en varios estudios se pusieron de relieve las malas costumbres en cuanto a la seguridad de los datos que se han detectado durante el periodo de teletrabajo de la pandemia.

En 2022 podemos ver que la forma en la que trabajamos ha evolucionado rápidamente y cada vez somos más los que hemos pasado a una forma de trabajar híbrida cuando se ha decidido regresar a las oficinas tras la pandemia. Sin embargo, las empresas han tomado medidas y han ajustado los procesos, ¿o es que la nueva forma de trabajar está poniendo a las empresas en mayor riesgo de sufrir una filtración de datos?

La respuesta a esa pregunta es sí. La mitad de los participantes de nuestro estudio creen que esta forma híbrida de trabajar puede haber aumentado la cantidad de información sensible que se pierde o que incumple las disposiciones del RGPD. Los documentos en papel no fueron precisamente lo primero por lo que se preocuparon las empresas a la hora de redactar sus políticas de seguridad, pero la rápida transición a este modelo híbrido ha implicado que se muevan miles de documentos más de la oficina a casa cada semana. Esto plantea importantes preguntas sobre la documentación confidencial en formato físico y la forma de protegerla en un mundo en el que los empleados ya no solo trabajan en la oficina de la empresa.

En nuestro afán de aumentar el conocimiento de Fellowes sobre destructoras de papel —que se remonta 40 años atrás—, queríamos conocer la forma en la que las personas protegen y destruyen los documentos en esta coyuntura laboral híbrida cada vez mayor, así como la forma en la que las organizaciones están cumpliendo con el RGPD (Reglamento General de Protección de Datos) 4 años después de su entrada en vigor. Siempre hemos desarrollado nuestras destructoras para que cumplan cada necesidad en el lugar de trabajo, desde el primer día. Nos comprometimos a proteger a las empresas y a las personas en cualquier lugar de trabajo ayudándolas a prevenir que los documentos físicos cayeran en las manos equivocadas.

Nuestro estudio, en colaboración con B2B International, incluyó a 605 usuarios de destructoras de Francia, Alemania y el Reino Unido que trabajaban en servicios financieros, el sector público y sanidad.

En este informe llevamos a cabo un estudio en profundidad sobre las tendencias y las conductas relativas a la seguridad de los datos en esta coyuntura laboral en constante cambio y esperamos que pueda servir de guía para las empresas en esta época de cambio, ya que destruir la documentación sensible, sea cual sea el lugar de trabajo, es esencial para mantener a raya los riesgos de seguridad a los que se enfrenta cada organización”.

Steven Hickey
Fellowes Head of European Marketing – Workspace Solutions

Cronología de las destructoras Fellowes

1982
DESTRUCTORAS COMERCIALES

Fellowes formaliza un contrato de licencia con una empresa alemana para fabricar destructoras comerciales

1990
LA PRIMERA DESTRUCTORA PERSONAL

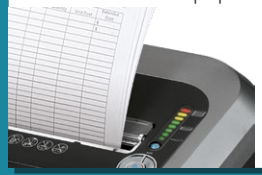
se desvela la destructora de papel personal como nueva invención

2005
DESTRUCTORAS CON SEGURIDAD SAFESENSE™:

Fellowes presenta la tecnología SafeSense™ para destructoras, lo que hace que sean mucho más seguras para su uso

2008
DESTRUCTORAS 100 % A PRUEBA DE ATASCOS

Fellowes presenta la gama de destructoras “100 % anti-atascos” que elimina los atascos de papel



2014
DESTRUCTORAS AUTOMÁTICAS AUTOMAX™:

Fellowes presenta las destructoras automáticas AutoMax™, que mejoran la productividad de la destructora en la oficina

2020
DESTRUCTORAS SERIE LX:

Fellowes presenta las destructoras con microcorte más avanzadas, diseñadas para integrarse en cualquier espacio de trabajo.

El RGPD y la protección de datos en un mundo laboral híbrido

Nuestro estudio ha revelado que **8 de cada 10** encuestados se ha pasado al teletrabajo, ya sea total o parcialmente. El trabajo híbrido —una combinación de trabajo in situ y de forma remota— quizá haya dado más flexibilidad y variedad de elección en lo que se refiere al entorno laboral pero también plantea el reto constante de garantizar que todos respeten la confidencialidad mientras trabajan y aplican buenos principios de protección de datos en cualquier lugar de trabajo.

Ya sea personal que trabaja en la oficina, en casa, en espacios de trabajo compartidos o en cualquier otro lugar, debe gestionar los riesgos de seguridad. El primer paso es garantizar que revisa los ámbitos que puedan plantear nuevos riesgos a la organización. Por ejemplo, debe disponer de políticas estrictas que rijan el uso que hace el personal de sus propios ordenadores, tabletas y teléfonos móviles para fines laborales ya que el control corporativo que puede ejercer sobre la forma de configurar y utilizar dichos dispositivos es menor. Otro motivo de preocupación es el uso de redes wifi públicas o domésticas, así como las contraseñas débiles o reutilizadas. Ambos supuestos tienen un punto común de intrusión para los ataques informáticos, y deben darse instrucciones claras a los empleados para garantizar que la empresa está protegida.

No sorprende a nadie que los documentos en papel supongan uno de los retos más infravalorados para las empresas. Dado que ahora todo es digital, a menudo las empresas se olvidan de reflejar el supuesto de los datos en papel en su política de seguridad. No obstante, cabe señalar que la mayoría de empresas **(el 68 %)** que han participado en el estudio han indicado que tratan una gran cantidad de información sensible impresa a diario. **El 70 %** de los encuestados se ha llevado documentos de trabajo impresos a casa, ha imprimido documentos de trabajo en casa o ambas y poco menos de la mitad de este grupo ha tirado dichos documentos

¿No tiene clara las implicaciones del RGPD? Nosotros le echamos una mano...

El Reglamento General de Protección de Datos entró en vigor en mayo de 2018 y consiste en un amplio conjunto de requisitos de protección de datos para el tratamiento de los datos personales de los ciudadanos europeos. Toda organización que trate este tipo de datos personales deberá recopilarlos únicamente conforme a unas condiciones estrictas y para fines legítimos y protegerlos frente a usos indebidos.

Los datos personales deben procesarse de forma que se garantice que estén adecuadamente protegidos frente a tratamientos no autorizados o ilegales, pérdida accidental, destrucción o daños, utilizando para ello las medidas técnicas y organizativas necesarias.

¿Qué son los datos personales?

Son datos que guardan relación con una persona a la que se puede identificar a partir de dichos datos. Pueden ser nombres, direcciones, números de la seguridad social, información de las redes sociales, contenido de videovigilancia o fotografías. Los datos personales pueden estar en formato físico o digital.

¿Cuáles son las consecuencias de incumplir el RGPD?

Una filtración de datos personales puede comportar multas de hasta el **4 % de la facturación global o 20 millones de €**, así como los daños infligidos a la reputación de la empresa.

Los seis principios de la protección de datos

Cada estrategia de protección de datos debe hacer constar los principios, según los cuales los datos deben tratarse de la siguiente forma:

- **Deben tratarse de forma lícita, justa y transparente**
- **Deben recopilarse para fines específicos, explícitos y legítimos y no tratarse de formas ulteriores que contravengan dichos fines**
- **Deben ser adecuados, relevantes y limitarse a aquellos que sean necesarios**
- **Deben ser concisos y estar actualizados. Las inconsistencias deben procesarse, eliminarse y rectificarse**
- **No deben conservarse más tiempo del necesario**
- **Deben tratarse de forma segura**

Puede encontrar más información aquí: Reglamento General de Protección de Datos - Fellowes®

a una papelera o contenedor de reciclaje sin destruirlos. Además, el **46 %** de los encuestados ha visto cómo la gente deja desatendidos documentos confidenciales relacionados con la empresa. Esto debería preocupar a las organizaciones y mucho. Aunque parece haber políticas estrictas para que se destruyan la información sensible en las empresas europeas, a menudo estas directrices no se siguen cuando se trabaja fuera. Los datos sensibles en papel deben guardarse a buen recaudo cuando no se utilicen y destruirse cuando ya no se necesiten para el fin en cuestión, ya sea en una oficina o en el espacio de trabajo en casa.

Nuestro estudio también ha revelado que aunque ya han pasado 4 años, solamente el **60 %** conoce bien el RGPD y tan solo **1 de cada 4** empresas ha adaptado sus políticas para que incluyan el trabajo desde casa o el teletrabajo en general. Las autoridades reguladoras, como la Oficina del Comisionado de Información (ICO), han actuado de forma permisiva por la presión que ha ejercido la pandemia sobre las empresas. No obstante, ahora que la mayoría de restricciones se están eliminando en Europa, la ICO será menos benevolente, así que es fundamental actuar ya, si su idea es trabajar de forma híbrida para siempre. Debe garantizar que se revisan y actualizan las políticas para que se integre la nueva forma de trabajar y abarcar los posibles riesgos de filtración de datos.

Una vez que se hayan actualizado las políticas, es importante disponer de un plan sólido de aplicación y comunicación. El estudio puso de relieve una clara desconexión dentro de las organizaciones. Si bien la mayoría de encuestados **(el 83 %)** en cargos de mayor responsabilidad parecían conocer bien el RGPD y seguían activamente las normas y reglamentos de protección de datos de las empresas, solamente el **57 %** de los encuestados en cargos de menor responsabilidad se habían familiarizado con el RGPD y por lo tanto, no seguían sus directrices, independientemente desde dónde trabajaran.

La comunicación y el control de lo que ocurre con los documentos y datos sensibles tienden a parecer más fáciles cuando se trabaja desde la oficina junto a todo el equipo. No obstante, la realidad es que el trabajo híbrido ha llegado para quedarse y que las empresas deben integrarlo para respaldar a su personal. Al mismo tiempo, es esencial que se adapten los procesos y los reglamentos para que reflejen estos cambios. Las consecuencias que tiene el hecho de que la documentación sensible se extravíe son graves, por lo que es fundamental concienciar sobre esta regulación a todos los compañeros de todos los niveles, porque solamente hace falta un dato mal protegido para que se produzca una filtración. En la siguiente sección, le ofrecemos sugerencias sobre formas de cómo aplicar estos cambios en la empresa.

CUMPLE CON EL **RGPD**

¿Qué pueden hacer las empresas para ayudar a que su personal cumpla la Política de privacidad y de datos?

Actualizar las políticas de seguridad

Piense en la política sobre el uso del dispositivo propio (BYOD), en que si los empleados utilizan sus propios dispositivos cuando trabajan desde casa.

Haga hincapié en el hecho de que las redes wifi públicas y domésticas suponen una amenaza y lo que debe hacer el personal para utilizarlas de forma segura.

Revise y adapte sus políticas sobre impresión, almacenamiento y eliminación de documentos en papel y añada una sección sobre el almacenamiento y eliminación de documentos en la oficina en casa.

Revise las políticas de seguridad de las contraseñas. En la actualidad, el Centro Nacional de Seguridad Informática (NCSC) recomienda utilizar tres frases de contraseña en vez de palabras. Además, debe plantearse utilizar la autenticación multifactor.

La política debe hacer constar que, antes de eliminar, vender o donar un ordenador o disco duro viejo, se deben eliminar todos los datos del disco duro.

Formación

No puede dar por hecho que todo el mundo entiende el RGPD. Eduque a todos los empleados sobre los requisitos del RGPD, el tratamiento de datos personales y los seis principios de protección de datos. Debe ofrecerse formación a todos los recién llegados y como parte de las sesiones periódicas de repaso sobre seguridad.

Facilite a sus empleados una lista para que comprueben todos los ámbitos que pueden suponer un riesgo de filtración de datos; también puede dejarles que hagan una **comprobación de la seguridad de los datos.**

Asegúrese de que la formación incluye el aspecto de los documentos sensibles en papel y la forma de gestionarlos. Qué documentos y registros deben conservarse durante plazos fijos y qué documentos deben destruirse inmediatamente después de que ya no se necesiten.

Añada un módulo de formación sobre la seguridad de los datos en teletrabajo que haga hincapié en los nuevos elementos añadidos a las políticas.

Plantéese crear un portal de formación digital para poder hacer un seguimiento del progreso educativo de todos y marcar una fecha final flexible.

Equipo

A fin de evitar problemas con la BYOD, recomendaríamos a la empresa que invierta en ordenadores portátiles en vez de en ordenadores de sobremesa; de esta forma, es fácil mover el equipo entre el domicilio y la oficina de la empresa.

Invierta en sistemas antivirus y de cortafuegos de calidad superior.

Asegúrese de que su personal tiene acceso a una destructora en la oficina de la empresa. Además, los empleados que trabajen desde casa deben disponer de una destructora pequeña o doméstica.

En el caso de datos personales o altamente confidenciales —como direcciones, facturas o balances contables—, optar por una destructora de microcorte (P-5), ya que la reducción en el tamaño de las partículas da una seguridad superior y hace que los datos sean imposibles de leer o recuperar.

Garantice que el espacio de trabajo es productivo y seguro para los empleados teniendo en cuenta la prevención de atascos y las características de seguridad cuando vaya a comprar una destructora.

Comunicación

Es fundamental la comunicación entre todos los niveles de la empresa. Evite que haya deficiencias de conocimiento en los cargos de menor responsabilidad.

La seguridad de los datos es un tema que deberá tratarse en la siguiente reunión, así como en grupos más pequeños durante las reuniones mensuales de equipo y las sesiones informativas personales.

Cuelgue carteles de recordatorio por la empresa, pero también incluya la actualización de las políticas en el boletín y publíquelo en la intranet.

Compartir las mejores prácticas y las amenazas de phishing u otros ataques informáticos con el personal de la empresa para que todo el mundo esté al corriente de los peligros.

Integre el ámbito de la seguridad de los datos en las revisiones empresariales trimestrales.

¿Qué pueden hacer los empleados para evitar las filtraciones de datos?

Saber qué datos son sensibles y qué debe protegerse

Los documentos que contengan datos personales o registros empresariales deben destruirse de forma segura conforme a los requisitos legales sobre retención de datos.

Asegúrese de que sabe que cada país tiene sus propios plazos para el archivo de contratos, acuerdos empresariales y documentos similares. Cuando se hayan cumplido los requisitos de retención, destruir los documentos es la forma más segura de ahorrar espacio y proteger la confidencialidad.

Lo normal es que los recibos, los comprobantes de depósito y los estados bancarios se suelen destruir en cuanto se han cuadrado las cuentas.

Deben revisarse periódicamente los registros de RR. HH. y en cuanto haya llegado su fecha de vencimiento legal, deben destruirse. El RGPD exige que los departamentos de RR. HH. demuestren el motivo por el que conservan datos de los empleados pasados y presentes y que justifiquen el motivo por el que los conservan más tiempo del requerido.

Almacenar y eliminar los datos en papel de forma segura

Piense antes de imprimir. Pregúntese: ¿realmente necesito una copia física? ¿quién podría coger ese documento por error?

Vaya destruyendo conforme avanza o, si eso no es posible, destruya toda la documentación sensible antes de reciclarla o eliminarla; lo ideal sería hacerlo sin correr el riesgo de transportarla de casa a la oficina o viceversa.

No debe dejar nunca desatendidos datos sensibles en papel ni en casa ni en la oficina. Despeje siempre el escritorio por la noche y guarde bajo llave la documentación con marcado de protección y todos los medios informáticos extraíbles antes de abandonar su espacio de trabajo.

Revise periódicamente los datos que conserva y cuando sea posible, anonimice los datos personales en cuanto ya no se necesiten.

Estar al día con la formación y las políticas

Asegúrese de estar al tanto de los módulos de formación existentes y de que puede acceder a ellos. Asimismo, plantéese configurar recordatorios trimestrales en el calendario para asistir a las sesiones de repaso.

Anime a sus compañeros y a los miembros de su equipo para que asistan a la formación, y recuérdense entre ustedes las normas y directrices en caso de ver a alguien que no actúa conforme a la política (p. ej., dejando desatendidos documentos sensibles, usando dispositivos personales, etc.)

Familiarícese con los seis principios de protección de datos.

Hable con su superior o con el responsable de la protección de datos si tiene alguna pregunta.

Principales conclusiones de nuestro estudio

El 70% de todos los encuestados
se ha llevado a casa documentos de trabajo impresos, ha imprimido documentos en casa o ambas cosas.

El 47%
de los encuestados **no destruye los documentos de trabajo** después de terminar de trabajar con ellos **>>> ¡Esto conduce a riesgos de seguridad durante sus desplazamientos!**

El 46%
ha visto a personas dejar documentos documentos relacionados con el trabajo sin vigilancia

Hay un gran desconocimiento sobre el RGPD entre trabajadores de categorías inferiores o no directivos

Solo el 57%
Dicen estar familiarizados con el reglamento

Después de 4 años

Solo el 60%
de todos los encuestados dice conocer el RGPD.

4 de cada 10 (41%)
Dicen no haber visto todavía una actualización formal de la **política del RGPD para el trabajo en casa.**

Pautas para mejorar las prácticas de destrucción de documentos:

Una destrucción segura es fundamental para mantener los documentos confidenciales alejados de delincuentes y reducir la exposición de la organización a las filtraciones de datos. En una época en la que más personas que nunca trabajan de forma híbrida, entre el hogar y la oficina, y en la que cumplir con el RGPD es más importante que nunca, los riesgos de seguridad de los datos que esto supone son evidentes.

Utilizar una destructora para eliminar de forma segura los documentos confidenciales debería formar parte de nuestra rutina diaria, trabajemos donde trabajemos.

- No dé por sentado que todo el mundo entiende el RGPD. Eduque a todos los empleados sobre los requisitos del RGPD, el tratamiento de datos personales y los seis principios de protección de datos. Esta formación debe impartirse a todos los nuevos empleados, siempre que se actualice la legislación y como parte de las sesiones periódicas de actualización de la seguridad de los datos.
- Guarde bajo llave los documentos confidenciales cuando no se utilicen y no los deje nunca sin supervisión, ni en su casa ni en la oficina.
- Destruya toda la documentación sensible antes de reciclarla o eliminarla. Lo ideal sería hacerlo sin correr el riesgo de transportarla de casa a la oficina o viceversa.
- Facilite a todos los empleados el acceso a una destructora segura en casa y en el trabajo.

Encuentre la destructora adecuada para su entorno de trabajo.
Visite www.Fellowes.com o haga clic **aquí**

Estudio de Fellowes “Protege tus datos Confidenciales” 2022
Metodología

Este estudio lo llevó a cabo B2B International en abril de 2022. Se ha encuestado a un total de 605 usuarios de destructoras, repartidos equitativamente entre Reino Unido, Francia y Alemania. La demografía principal han sido usuarios de destructoras en cargos con diferente responsabilidad en pequeñas y medianas empresas de los siguientes sectores: servicios financieros (206), sector público (206) y sanidad/ medicina (193).
A fin de poder comparar costumbres laborales relativas a la seguridad de los datos en un mundo laboral híbrido, era importante que la división entre personas que trabajan desde casa y en la oficina, personas que trabajan principalmente desde la oficina y personas que trabajan principalmente desde casa fuera equitativa.

Si precisa más información sobre la metodología del estudio, póngase en contacto con marketingiberica@fellowes.com

Fellowes

www.fellowes.com