Resumen ejecutivo de IDC

Patrocinado por: **Brother**

Autor:

Jacqui Hendriks

Marzo de 2018

Asegurar la privacidad de los datos: el desafío de una gestión de documentos físicos y electrónicos en constante evolución

Muchas empresas no cumplen con la nueva legislación en materia de seguridad y privacidad de datos porque no tienen en cuenta las vulnerabilidades relacionadas con los documentos físicos. Un entorno inseguro de impresión es un entorno inseguro de TI.

Este resumen ejecutivo de IDC ofrece una introducción a la nueva legislación en materia de privacidad de datos, las iniciativas necesarias para cumplir esta legislación y las acciones específicas requeridas para que los procesos de gestión de documentos físicos y electrónicos la cumplan.

Proteger los datos del cliente

La innovación tecnológica ha cambiado drásticamente la manera en que las empresas de todos los tamaños reciben, procesan, utilizan y entregan información. Las empresas reciben incrementos exponenciales de volumen de información en formatos físico y electrónico. Según datos de IDC, la cantidad de datos creados, capturados y replicados crecerá hasta 163 zettabytes (ZB) o 163 billones de gigabytes (GB) en 2025, diez veces la cantidad de 16,12 ZB de datos generados en 2016[1]. La legislación en materia de protección de datos avanza aún con retraso debido a los cambios en los comportamientos en los lugares de trabajo.

La capacidad de mantener a salvo esta información ayuda a atraer y retener clientes al mejorar la experiencia de usuario[2]. Sin embargo, por culpa de una gestión ineficaz de la información, las empresas a menudo encuentran dificultades incluso para encontrar esta información[3]. Lo que es más importante, si la información no se gestiona adecuadamente, el riesgo de que los datos vulnerables caigan en manos equivocadas aumenta. Esto puede provocar infracciones importantes, poniendo en riesgo los datos personales de los clientes.

Los puntos de vulnerabilidad son, entre otros:

- Uso incorrecto de los dispositivos de impresión y los documentos físicos.
- Datos guardados en el almacenamiento de los dispositivos y también en su memoria interna.
- Posibles infracciones originadas en los puertos de red de los dispositivos.
- Documentos no recogidos.

La legislación en materia de protección de datos está siendo actualizada para recoger los valores y los comportamientos actuales, incluido el uso de las redes sociales y otros servicios en línea. La Directiva de protección de datos de la UE de 1995 (95/46/CE) es anterior a la existencia de los modelos actuales de negocio en línea y mucho menos contempla la llegada de las redes sociales y los servicios en la nube. La nueva legislación impondrá sanciones significativas a aquellas empresas que no hagan un esfuerzo para reducir el riesgo.

Actualmente está en vigor el Reglamento General de Protección de Datos de la Unión Europea (UE) (GDPR) 2016/679, pero pronto se aplicarán más leyes europeas relacionadas con la privacidad de la propia UE.

Actualmente está en vigor el Reglamento General de Protección de Datos de la Unión Europea (UE) (GDPR) 2016/679, pero pronto se aplicarán más leyes europeas relacionadas, por ejemplo, con la privacidad de la propia UE[4]:

- **Directiva 2016/680**: similar al Reglamento GDPR y centrada en el tratamiento de datos personales para prevenir, investigar, detectar y juzgar delitos penales o imponer sanciones penales. Es una antigua directiva que a partir del 6 de mayo de 2018 se trasladará a las leyes locales de los 28 estados miembros de la UE.
- **Directiva de Seguridad de la Información en las Redes (NIS)**: fue aprobada por la UE para establecer un enfoque coherente contra ataques cibernéticos en servicios fundamentales como energía, transporte, banca, infraestructuras del mercado financiero, sanidad, abastecimiento de agua potable e infraestructura y servicios digitales.
- **Reglamento de Privacidad Digital (ePD)**: junto al Reglamento GDPR, esta directiva constituye el marco jurídico de privacidad digital para los ciudadanos de la UE y abarca las comunicaciones a través de redes públicas. El Reglamento ePD se remonta a 2002, pero actualmente está siendo revisdo y actualizado para adaptarlo a los avances tecnológicos.
- **Directiva de registro de nombres de pasajeros (PNR)**: abarca la práctica común de recopilación de datos de pasajeros antes de embarcar en un vuelo. Los Estados miembros de la UE deben incorporar esta directiva a sus legislaciones nacionales antes del 24 de mayo de 2018. Los datos personales recogidos en la Directiva PNR deben almacenarse durante seis meses, tras lo cual deben ser anonimizados y posteriormente almacenados durante un periodo de cuatro años y medio.

Aunque parte de la nueva legislación es o demasiado genérica o muy específica para un sector, tendrá un impacto importante en la forma en que las empresas gestionarán el flujo de trabajo de documentos electrónicos y físicos en el futuro.

Privacidad y seguridad de los datos

El Reglamento GDPR 2016/679 define una infracción de datos como "destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos". Representa un cambio fundamental en las leyes de la UE que regulan los datos personales y la privacidad de los

ciudadanos de la propia UE. Las empresas internacionales situadas fuera de la UE, incluidas las empresas de Reino Unido tras el Brexit, también se verán afectadas a la hora de gestionar los datos de los ciudadanos de la UE.

El Reglamento GDPR tiene dos objetivos principales. El primero es actualizar la ley de protección de datos y el segundo unificar las normas comunitarias de protección de datos en una única ley. Parte de la siguiente premisa:

- Las empresas no son propietarias de los datos personales. La última legislación vigente respalda el derecho de las personas a saber si sus datos se gestionan correctamente y a ser informados de si estos se han perdido, robado o no han sido tratados adecuadamente cuando la infracción es de alto riesgo (notificaciones de infracción obligatorias).
- Las empresas tienen que cumplir el "derecho al olvido" del público. Para ello, deben saber dónde se encuentran los datos de cualquier persona, en qué aplicación o equipo. También es necesario que toda la información se deposite de manera estandarizada en los repositorios de datos de todos los sistemas, plataformas o equipos.

Muchos de los requisitos, así como los de otras leyes de entrada en vigor inminente, posiblemente son mucho más estrictos que los que imponían las leyes que vienen a sustituir. Las multas por incumplimiento son deliberadamente severas: "efectivas, proporcionadas y disuasorias" de acuerdo al texto del Reglamento GDPR, si bien el objetivo es que todos cumplan el reglamento de una manera clara y sencilla. La prueba de que una empresa se esfuerza en cumplir la ley es muy importante cuando la autoridad competente tiene que investigar una infracción de seguridad.

Incumplir la ley puede tener un fuerte impacto negativo en la reputación de la empresa. De hecho, el riesgo que supone el incumplimiento para la reputación es una de las principales preocupaciones relacionadas con el Reglamento GDPR[5].

Al abordar los requisitos para el cumplimiento de la ley, las empresas tienen cuatro prioridades clave de inversión[6]:

- Identificar las aplicaciones que utilizan los datos a los que se refiere una legislación específica
- Rastrear y detectar datos: evaluarlos y clasificarlos
- Establecer procesos de documentación
- Revisar y mejorar la gestión de la identidad y el acceso

El Reglamento GDPR pone encima de la mesa el problema de la seguridad y la privacidad de los datos de documentos electrónicos y físicos. Requiere que todo el flujo de trabajo electrónico o impreso cumpla unas determinadas condiciones. Debe autorizarse el acceso, procesamiento y registrarse las auditorías, y la información debe permanecer segura, incluidos los datos en los dispositivos de impresión. Los procesos debidamente documentados y los registros y las auditorías adecuadas no solo ayudan a mitigar las infracciones de seguridad, sino que si finalmente se produce una infracción, se dispone de

El Reglamento GDPR pone encima de la mesa el problema de la seguridad y la privacidad de los datos de documentos electrónicos y físicos. Requiere que todo el flujo de trabajo electrónico o impreso cumpla unas determinadas condiciones. Los procesos debidamente documentados y los registros y las auditorías adecuadas no solo ayudan a mitigar las infracciones de seguridad, sino que, si finalmente se produce una infracción, se dispone de pruebas suficientes para demostrar que se tomaron las medidas necesarias para evitarla.

pruebas suficientes para demostrar que se tomaron todas las medidas necesarias para evitarla.

Los proveedores de gestión de documentos electrónicos y físicos se han visto obligados a cumplir con la legislación en materia de privacidad de datos y están bien posicionados para dar apoyo a sus clientes. Sin embargo, la responsabilidad de cumplir la legislación es en última instancia de las empresas.

Hasta la fecha, parece que las empresas no están cumpliendo los requisitos relacionados con documentos físicos o desconocen la legislación, su impacto y los plazos[7]:

- Sorprendentemente, a pesar de las multas que entran en vigor en 2018, a comienzos de 2017, el 40 % de los compradores de documentos físicos no conocían el Reglamento GDPR y el 19 % lo conocían, pero no tenían información de los plazos. Las empresas que sí conocían el reglamento avanzaban lentamente, pero tenían la seguridad de que lo cumplirían finalmente.
- Aún más sorprendente fue que de entre los compradores de documentos físicos que conocían el Reglamento GDPR, el 51% no comprendían el motivo de que existiera una atención especial a estos.

Asegurar que los procesos de gestión de documentos físicos y electrónicos cumplen la legislación

Entre los compradores de documentos físicos que conocían el Reglamento GDPR, el 51% no comprendían el motivo de que existiera una atención especial a estos documentos.

La seguridad en la organización es una prioridad para todas las empresas, desde los vendedores independientes hasta las grandes empresas multinacionales. Los puntos más débiles relacionados con la seguridad que deben solucionarse son[7]:

1. La planificación del mantenimiento del negocio y la recuperación ante cualquier desastre
2. Adelantarse a ataques cada vez más sofisticados
3. El cumplimiento de la normativa

A pesar del aumento de los incidentes de filtración de datos personales y empresariales, en lo que se refiere a la seguridad de los documentos físicos no se presta suficiente atención a lo que se debe hacer para cumplir la ley[7]:

- La inversión en la seguridad de documentos físicos es baja: más de la mitad de las empresas gastan menos del 3 % de su presupuesto de TI en la seguridad de estos documentos.
- En cuanto a los planes futuros, dos tercios no tienen intención de aumentar este gasto en los próximos 12 meses y solo un tercio de las empresas incluyen la seguridad de documentos físicos en tecnologías de TI.

Ya se han desarrollado propuestas de soluciones para abordar la mejora de la eficiencia de la gestión de documentos electrónicos y físicos y el cumplimiento de la legislación en materia de privacidad de datos:

- Las empresas afirmaron que estaban interesadas en disponer de funciones de seguridad para los documentos físicos integradas en sus impresoras multifunción (MFP), como por ejemplo la tecnología *pull printing* y las soluciones de usuario final autentificado y autorizado[3]. El resultado es que las empresas pueden restringir el acceso de los empleados a información específica, en función de su puesto y responsabilidad. Esto representa una medida fiable para cumplir la ley y está dirigida a reducir riesgos.
- La creciente demanda de digitalización de la información para integrarla en el flujo de trabajo de documentos electrónicos se ha traducido en un mayor uso de escáneres. Según un estudio europeo de IDC de 2017 sobre documentos físicos, el escaneado a correo electrónico, carpetas de red y sistemas (por ejemplo, ERP, CRM) resulta en la actualidad de gran interés para las empresas. Además, hay una mayor demanda de impresoras multifunción (MFP) inteligentes que dispongan de escáner y acceso directo al almacenamiento de datos[3].

Los proveedores de documentos físicos e imágenes no han pasado por alto la gestión segura y eficaz de estos documentos. Ofrecen una gran variedad de soluciones y ayudan a las empresas a optimizar la manera en que gestionan el cumplimiento de la legislación sin tener que desviar demasiados recursos de las actividades que generan ingresos:

Los proveedores de documentos físicos e imágenes no han pasado por alto la gestión segura y eficaz de estos documentos. Ofrecen una gran variedad de soluciones y ayudan a las empresas a optimizar la manera en que gestionan el cumplimiento de la legislación.

- **Soluciones de supervisión y gestión de documentos físicos**: son instrumentos eficaces para realizar un seguimiento e informar del uso de dispositivos para la evaluación del entorno de impresión en negociaciones comerciales o contractuales. Por esta razón, más de la mitad de las empresas (53 %) han implementado estas soluciones[8]. Estas soluciones también valoran la creación de un registro de auditoría para identificar lo que se imprime o se procesa, dónde y quién lo hace. La capacidad de mantener un registro de auditoría es un componente fundamental para reducir las principales infracciones de la seguridad.
- **Autenticación y acceso seguro**: el 46 % de las empresas exigen a los empleados que se identifiquen en los dispositivos de impresión[8] antes de utilizarlos, mediante un código PIN o a través de la tecnología NFC (Comunicación de Campo Cercano) con tarjeta de acceso. Esta funcionalidad suele ser obligatoria únicamente en aquellos departamentos que procesan principalmente material confidencial, como los departamentos de recursos humanos, jurídicos o financieros.
- **Acceso seguro a documentos físicos con *Active Directory***: ofrece una mayor seguridad gracias al bloqueo de funciones en el dispositivo físico y una mayor flexibilidad, por ejemplo, con un tiempo límite para recoger trabajos de impresión. Los documentos del dispositivo que no reclame nadie presentan el riesgo de que alguien ajeno los recoja.
- **Seguridad de los dispositivos de impresión**: las empresas están cada vez más preocupadas por que la información confidencial almacenada

en dispositivos de red periférica pueda pasar inadvertidamente a dominio público[8]. Algunos fabricantes de impresoras se aseguran de que los usuarios no puedan almacenar información en el dispositivo, aunque pueden aprovechar la capacidad de recuperar documentos desde un servidor central seguro o un servicio seguro de almacenamiento en la nube. Por tanto, las empresas tienen la garantía de que los documentos no se pueden recuperar desde el dispositivo, por lo que el dispositivo no se ve comprometido.

- **Escaneado seguro**: las medidas de seguridad no se limitan solo a la impresión de documentos. También se puede mejorar la seguridad de los documentos escaneados gracias a archivos PDF con acceso limitado por código PIN o mediante el uso de un servidor de transferencia de archivos (SFTP) seguro para crear un flujo de datos seguro. El 20 % de las empresas afirmaron que su principal preocupación de seguridad es el acceso de los empleados a los documentos escaneados[9].
- **Comunicaciones de datos seguras**: los dispositivos que se utilizan para imprimir, escanear u otras tareas de gestión de documentos deberían ser seguros mediante la configuración de funciones reconocidas en el sector como *Internet Protocol Security* (IPsec) y *Transport Layer Security* (TLS). Estas funciones garantizan que las comunicaciones hacia el dispositivo y desde él sean fiables, confidenciales y autentificadas.
- **Amenazas de red**: las empresas deben asegurarse de que el dispositivo de impresión no es vulnerable, aplicando el mismo nivel de seguridad que se da a otros equipos como portátiles y tablets.

En lugar de tomarse la legislación como una pesada carga, las empresas deberían verla como una oportunidad para implementar mejores procesos.

Los flujos de trabajo optimizados no solo ayudan a cumplir la ley, sino que generalmente ayudarán a procesar información de manera más eficiente en el día a día. Además, una de las consecuencias colaterales de utilizar mejores procesos para cumplir con la legislación suele ser un ahorro en costes.

Una de las consecuencias colaterales de utilizar mejores procesos para cumplir con la legislación suele ser un ahorro en costes.

Orientación: asegurar que se cumple la ley con la gestión de documentos físicos y electrónicos

Como parte de las iniciativas de una empresa para asegurar que el negocio es seguro y cumplir con la legislación en materia de privacidad de datos, le presentamos una lista con 10 puntos para ayudar a su empresa a cumplirla:

- ☑ Realice una auditoría de la seguridad actual de su empresa y las políticas de privacidad, coordínelas con los principales requisitos de seguridad y privacidad de datos e incluya la infraestructura de impresión en esta auditoría.
- ☑ Identifique al personal interno con habilidades relevantes, así como las potenciales carencias de habilidades.
- ☑ Considere la posibilidad de preguntar a su proveedor de dispositivos de impresión acerca de los recursos que puede aprovechar el departamento de TI para apoyar iniciativas de cumplimiento.
- ☑ Proteja la red a la que están conectadas las impresoras.
- ☑ Proteja todos los tipos de información confidencial que se envía o se procesa en impresoras y escáneres.
- ☑ Asegúrese de que las impresoras no son vulnerables al malware y otros ataques cibernéticos.
- ☑ Asegúrese de que la información potencialmente confidencial no se almacena en dispositivos periféricos como impresoras.
- ☑ Implemente una herramienta de gestión de flotas para centralizar la gestión y supervisar los dispositivos de impresión y escaneado.
- ☑ Introduzca sistemas de autenticación y autorización del usuario (incluida la tecnología *pull printing*) en el dispositivo para garantizar la recuperación segura de documentos confidenciales.
- ☑ Desarrolle un plan para supervisar, escalar, aplicar y cumplir las actuales y futuras políticas de privacidad y seguridad.

Fuentes:

1. *Data Age 2025: The Evolution of Data to Life-Critical, Don't Focus on Big Data; Focus on the Data That's Big*, White Paper de IDC, Abril de 2017.
2. *What are the Top Priorities of LOBs and Industries in Western Europe?* IDC #EMEA43168117, Octubre de 2017.
3. *Content Management Opportunity: Integrated Solutions vs Outsourcing*, IDC #EMEA43165417, Octubre de 2017.
4. *An Overview of Incoming EU Privacy and Data Security Legislation*, IDC #EMEA42911917, Agosto de 2017.
5. Estudio de IDC EMEA sobre el Reglamento GDPR, marzo de 2017
6. *IDC PlanScape: EU General Data Protection Regulation Compliance*, IDC #US42574817, Junio de 2017.
7. *Low Investment in Print Security and Increasing Compliance Challenges Leave European Companies at Risk*, IDC #EMEA42819617, Junio de 2017.
8. *Still Significant Opportunity to Address Print Infrastructure /Management Challenges*, IDC #EMEA43059617, Septiembre de 2017.
9. *Workplace Dynamics Drive Print and Document Management,* IDC #EMEA41529116, Junio de 2016.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
Londres
W5 5TH, Reino Unido
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Acerca de IDC

International Data Corporation (IDC) es el proveedor global principal de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología de consumidor. IDC ayuda a profesionales de TI, ejecutivos de empresas y a la comunidad de inversores a tomar decisiones sobre compra de tecnología y estrategia empresarial. Más de 1100 analistas de IDC proporcionan sus conocimientos especializados a nivel global, regional y local sobre tecnología u oportunidades del sector, así como sobre tendencias en más de 110 países de todo el mundo. Durante 50 años, IDC ha proporcionado conocimientos estratégicos para ayudar a nuestros clientes a alcanzar sus objetivos de negocio clave. IDC es una subsidiaria de IDG, la empresa líder mundial en medios de tecnología, investigación y eventos.