Mantener un entorno de impresión seguro

Tercer informe de la serie Transformación Digital realizado por Brother

Informe

Extraído de una investigación de mercado

brother.es

Barreras para invertir en seguridad de la impresión

Debido a la amenaza creciente de ataques informáticos y brechas de seguridad que ponen en riesgo la confidencialidad, muchas empresas son cada vez más conscientes de la necesidad de proteger sus sistemas de TI.

Gestionar la seguridad del parque tecnológico es un reto que necesita ser abordado de forma global. Y las impresoras y escáneres necesitan ser tan seguros como el resto de los equipos de TI ya que, si no se les presta la debida atención, se corre el riesgo de que estén ofreciendo a los hackers una puerta trasera fácil de atravesar para entrar en nuestra organización. Las empresas son cada vez más conscientes de la importancia de este hecho: el **72%** aseguran que es fundamental que sus impresoras y escáneres sean seguros, y esto es incluso más importante para los que manejan datos sensibles en sectores como Servicios Profesionales (**82%**) y Sanidad (**81%**).

Sin embargo, aún son cerca de un tercio las compañías que no reconocen su importancia. Y se suma el hecho de que casi la mitad de los entrevistados no piensa que su empresa haya invertido lo suficiente en seguridad del hardware de impresión.

Si las empresas entienden la necesidad de invertir en la seguridad de sus equipos de impresión, ¿por qué no lo están haciendo?

Nuestra investigación muestra dos razones principales:

Responsabilidades poco definidas sobre quién se encarga de la seguridad de las impresoras

Falta de conocimientos sobre los estándares y amenazas de seguridad

Este informe está pensado para ayudar a los directivos y decisores empresariales a conocer la importancia de la seguridad en el entorno de impresión y la forma de implementar soluciones de impresión seguras. Forma parte de una serie de informes más amplia que pretende ayudarles a entender cuál es la mejor forma de utilizar las tecnologías digitales. Hemos basado las conclusiones en investigaciones de mercado realizadas entre directivos y decisores de un amplio rango de pymes y grandes empresas de la región de EMEA. Este documento forma parte de una serie de cuatro informes, cada uno centrado en uno de los siguientes temas:

- Flujos de trabajo digitales
- Implementar la solución adecuada para el negocio
- Seguridad
- Sostenibilidad

¿Quién es el responsable de la seguridad de las impresoras?

Frecuentemente hay dudas sobre quién es la persona responsable de la seguridad de los equipos de impresión. Casi la mitad de las empresas de Europa Occidental (44%) aseguran que no está claro quién es el responsable de seguridad en la impresión dentro de su organización. Y puesto que no se sabe quién debe rendir cuentas en esta área, es muy probable que la toma de decisiones y la implementación de medidas de seguridad para la impresión sufran, dejando a la empresa en una situación vulnerable.

Normalmente no se asigna un responsable para la seguridad de la impresión porque el equipo de impresión no se reconoce tradicionalmente como un 'punto débil', al contrario que otros dispositivos como los portátiles. Aunque nuestra investigación demuestra que los decisores están empezando a darse cuenta de que la seguridad en este entorno es vital, los roles en las empresas no parecen reflejarlo aún.

Las pymes son especialmente vulnerables a esta falta de responsabilidad, ya que muchas veces es un pequeño número de empleados el que cuida de todo el hardware y software de la empresa. Si los profesionales de TI no son conscientes de los riesgos de seguridad en la impresión, para ellos será una prioridad baja.

Sin embargo, todos los trabajadores de una empresa tienen una parte de responsabilidad a la hora de garantizar que la información sensible se mantiene segura.

Mientras que los expertos en tecnología se encargan de la seguridad de los dispositivos en sí mismos, los empleados tienen la responsabilidad de mantener la seguridad de los propios datos.

La seguridad de los datos incluye un amplio abanico de amenazas, entre las que se encuentran:

- Acceso no autorizado a los documentos impresos
- Olvidar cerrar sesión después de imprimir documentos confidenciales
- Falta de trazabilidad sobre quién ha accedido a qué documentos en la impresora

Casi 9 de cada 10 empresas han experimentado algún incidente de seguridad relacionado con la impresión...

… y siete de cada diez (72%) aseguran que la seguridad de los datos es una amenaza mayor que la seguridad del dispositivo. Sin embargo, actualmente menos de un tercio de las empresas dicen estar 'muy seguras' de que su infraestructura de impresión incluye medidas de seguridad suficientes, mientras que el 53% piensan que tienen la seguridad adecuada en sus equipos de hardware.

La mayoría de las empresas (64%) también afirman que garantizar la seguridad de sus datos es una prioridad. Esto se ve como un reto importante, y puede suponer una traba para un rendimiento eficiente.

Actualmente, casi la mitad de las empresas **(48%**) dicen tener pocos o ningún proceso que les permita saber con certeza quién imprime o recoge tareas de impresión. Por tanto, no resulta sorprendente que casi nueve de cada diez (**86%**) aseguren haber tenido un incidente de seguridad relacionado con la impresión: documentos confidenciales que se dejan sin supervisión en la impresora, impresiones que no se recogen o empleados que recogen documentos confidenciales que no son suyos.

Como resultado, la mayoría de las empresas (**64%)** están empezando a poner medidas para abordar este tipo de problemas de seguridad, restringiendo el acceso a ciertos equipos o introduciendo códigos PIN o tarjetas de identificación para que los trabajos de impresión sean liberados por la persona adecuada.

Son pasos en la buena dirección. En los próximos años será importante que, las empresas que no los tienen, introduzcan procesos más seguros; y las que ya lo hacen, mantengan y mejoren su responsabilidad y sus auditorías internas

Hay 3 objetivos principales para lograr una seguridad real de la información, resumidos en el acrónimo CIA, que cubren tanto la seguridad del equipo como la de los datos:

Confidencialidad

Proteger los datos confidenciales de la empresa para garantizar que solo se comparte con su destinatario. Para esto es fundamental tener medidas de autentificación y autorización que requieran que los usuarios verifiquen su identidad y se compruebe que tienen permiso para hacer lo que están intentando hacer, antes de que se libere cualquier documento impreso.

Integridad

Asegurar que el *firmware* del equipo es seguro y resistente a cualquier posible ataque o amenaza externa.

Accesibilidad

Asegurar que el equipo está funcionando y es accesible a los usuarios autorizados para realizar sus tareas.

La falta de conocimiento lleva a prácticas de seguridad poco apropiadas

Menos de un tercio (**32%**) de los decisores de TI de las empresas dicen tener un conocimiento avanzado en seguridad tecnológica y sus riesgos potenciales. Si ellos no tienen suficiente información sobre las amenazas, entonces las empresas continuarán teniendo problemas para poner en marcha las medidas adecuadas para protegerse. En las pymes, el papel del decisor cubre normalmente varias y diversas áreas tecnológicas, por lo que es entendible que no sean expertos en seguridad específica del entorno de impresión.

La responsabilidad, muchas veces, es de la jerga. Más de la mitad (**51%**) de las empresas se quejan de que hay demasiado vocabulario nuevo relacionado con la seguridad de la impresión.

En cuanto a los estándares de seguridad, casi el 60% de las empresas dice conocerlos bien.

Con todo esto, es poco probable que los decisores conozcan bien o sepan qué proveedores de tecnología de impresión pueden cubrir mejor sus necesidades de seguridad. Por tanto, no sorprende que las empresas busquen marcas que 'conocen' para sus equipos de impresión, sin preocuparse de saber realmente qué medidas de seguridad incorporan o no.

Es responsabilidad de los proveedores de impresión ayudar a las empresas a entender las normativas sobre seguridad que atañen a la impresión, y asegurar que cada una elige la mejor solución para sus necesidades.

La visión de Brother

Dada la compleja naturaleza del panorama de la seguridad de la impresión, desde Brother ofrecemos 7 recomendaciones clave que pueden ayudar a las empresas a protegerse de las enormes implicaciones financieras, legales y reputacionales de una pérdida de datos.

Implicar al comité de dirección

La escalada de ciberataques y brechas de seguridad, combinada con los requerimientos del Reglamento General de Protección de Datos (RGPD) implica que la seguridad de la impresión necesita ir más allá del dominio del departamento de tecnología. Debe ser considerada de manera estratégica en el comité de dirección, con la participación del CIO y el responsable de seguridad (CISO).

Llevar a cabo una auditoría exhaustiva

Para las empresas es fundamental descubrir cualquier vulnerabilidad potencial relacionada con la seguridad de la impresión, y asegurarse de que este entorno está incluido en las auditorías regulares de seguridad. Esto es especialmente importante si la empresa tiene una mezcla de dispositivos nuevos y antiguos.

En cuanto a los Servicios Gestionados de Impresión (MPS), la mayoría de los proveedores ofrecen no solo una evaluación completa, sino además una monitorización constante de los dispositivos, una vez que el parque de impresión ha sido optimizado y asegurado.

Cambiar las contraseñas preconfiguradas

Las contraseñas preconfiguradas o por defecto son un punto débil para los dispositivos de impresión. La buena noticia es que esto se puede arreglar fácilmente. Una vez el equipo ha sido instalado, solo hay que cambiarla eligiendo una que sea fiable y segura.

Actualizar y parchear el firmware

Es posible reducir significativamente las vulnerabilidades potenciales de seguridad de los equipos de impresión actualizando el firmware y configurándolo para que realice actualizaciones automáticas. En caso de dudas, lo mejor es contactar con el fabricante y dejarse asesorar.

Proteger las impresiones

No solo los equipos de impresión son los que necesitan protección, sino también los documentos que enviamos a imprimir. Un cifrado extremo a extremo del tráfico de red asegura una transferencia segura de los trabajos al equipo de impresión. Y puesto que la mayoría de las impresoras guarda temporalmente los trabajos en su memoria, hay que asegurarse de que los datos estén encriptados.

Monitorizar los equipos

Conocer el estado actual de nuestro parque de impresión nos ofrece una visión global de todo el entorno de impresión. Las empresas deberían considerar el uso de herramientas de software para monitorizar los equipos. Normalmente, estos pueden generar una gran cantidad de datos que pueden ser usados para identificar problemas potenciales de seguridad y permitir una respuesta rápida a los ataques. Los usuarios de Servicios Gestionados de Impresión también pueden obtener informes de conformidad regularmente, que deberían incluir monitorización y reportes de posibles brechas de datos.

Formar a los empleados

Hay muchas pérdidas de datos desintencionadas, por lo que es vital que las empresas formen a sus trabajadores sobre la importancia de proteger la información sensible, y difundan información sobre amenazas maliciosas. Muchas veces, los proveedores de Servicios Gestionados de Impresión ofrecen ayuda con estas necesidades de formación.

Conclusiones

En el pasado, los sistemas de impresión pueden haber sido obviados en los planes de seguridad organizacionales, pero las empresas ya se están dando cuenta de su importancia. Sin embargo, aún hay retos significativos en la implementación de medidas de seguridad en la impresión.

Las empresas tienen que definir claramente responsabilidades sobre la seguridad de la impresión para garantizar que los dispositivos están bien protegidos y pueden resistir amenazas. Así como la seguridad del equipo, las brechas de seguridad de los datos son también de vital importancia. También la cooperación de todos los empleados es necesaria para minimizar riesgos.

Incluso teniendo una definición clara de las responsabilidades dentro de las empresas, contar con los suficientes conocimientos para manejar la seguridad de la impresión de forma eficiente es aún un reto importante. La tecnología de impresión es cada vez más compleja y está llena de jerga. Las empresas deberían tratar de confiar en sus proveedores para tomar decisiones acertadas.

Un equipo de impresión eficiente tiene que ser más que seguro.

El resto de los informes de esta serie de Transformación Digital contienen más información sobre cómo implementar flujos de trabajo digitales, maximizar la productividad y asegurar que son sostenibles.

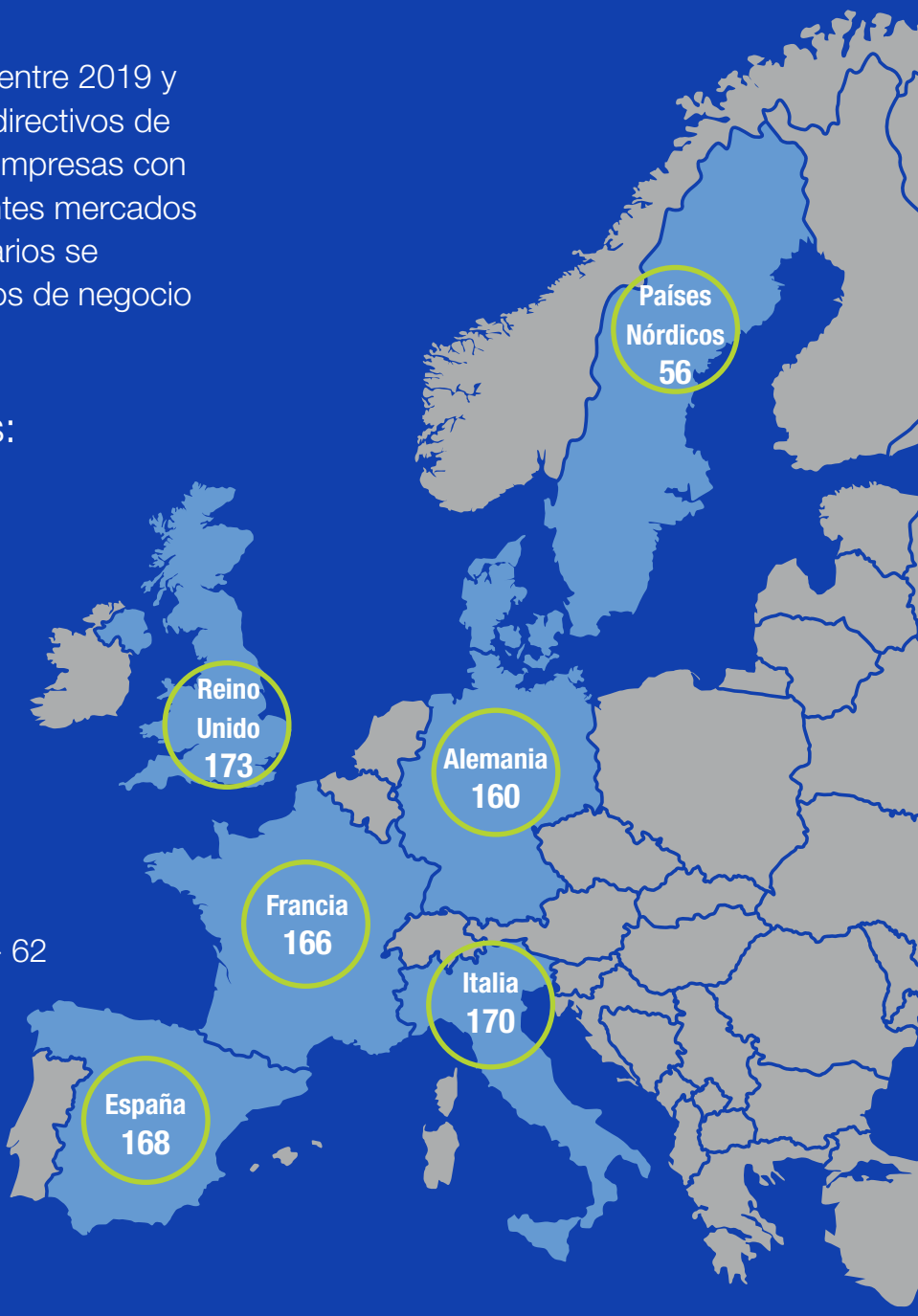
Nuestra metodología

Este informe se basa en 893 encuestas online a responsables de empresas y de TI.

El trabajo de campo se llevó a cabo entre 2019 y principios de 2020, entrevistando a directivos de TI y decisores de pymes y grandes empresas con entre 10 y 499 empleados en diferentes mercados de Europa Occidental. Los cuestionarios se dividieron entre decisores estratégicos de negocio (448) y directivos de TI (445).

Sectores clave entrevistados:

- Sanidad - 152
- Retail - 117
- Logística - 113
- Hostelería - 81
- Transporte y almacenamiento - 62
- Servicios profesionales - 65
- Fabricantes - 54
- Servicios financieros - 53
- Educación - 51
- Construcción - 39



También se realizaron entrevistas en otros sectores incluyendo energía, farmacia, agricultura, defensa, inmobiliaria, deportes y entretenimiento.

El informe ha sido llevado a cabo por la empresa de investigación de mercados Savanta.

Consigue la serie completa

Próximos informes de la serie Transformación Digital realizados por Brother.

brother
at your side

brother.es

Brother Iberia, S.L.U.
Edificio Brother
C/Julián Camarillo, nº 57
Tel: + 34 91 655 75 70