



Encargado por: HP:

Autores:

Angèle Boyd

Keith Kmetz
Matthew Marden

Noviembre de 2015

El valor para la empresa de la seguridad de las impresoras

OPINION DE IDC

Según investigaciones de IDC, el 80 % de las empresas encuestadas indicó que la seguridad de la IT es importante para su proceso empresarial, pero solo el 59 % de dichas empresas afirmó que la seguridad de la impresión es importante para sus procesos empresariales. Además, es casi un 40 % más probable que los altos directivos participen de la toma de decisiones referentes a la seguridad de la IT en general que de la seguridad de impresión. Creemos que estos datos muestran la falta de atención hacia la seguridad de la impresión que puede traducirse en la vulnerabilidad de las empresas. Las investigaciones de IDC han rebelado que hay razones de peso para que las empresas presten más atención a la seguridad de la impresión ya que de un entorno de impresión seguro derivan ventajas sustanciales para la IT y las empresas, como:

- » La encuesta de IDC concluyó que más de la mitad de las empresas encuestadas han tenido fallos de seguridad en la IT que incluyen la seguridad de impresión durante los últimos 12 meses.
- » Todos los entornos de impresión/documentos de una organización están llenos de vulnerabilidades. Estas vulnerabilidades pueden proceder de ataques malintencionados o de fuera de la organización además del uso negligente de los dispositivos de impresión y de las impresiones. Los fallos de seguridad potenciales relacionados con la impresión se podrían producir desde los puertos de red del dispositivo, la interceptación de los trabajos de impresión/copia/escaneo, los discos duros y la memoria (RAM) de las impresoras/equipos multifunción, los documentos impresos o copiados que quedan en las bandejas de salida o el uso ilegal de soportes de medios seguros (cheques, recetas), entre otros.
- » Entrevistas en profundidad a empresas realizadas por IDC con organizaciones que tienen algún nivel de seguridad con el flujo de trabajo de la impresión y los documentos relacionados revelaron dos tipos de empresas que adoptan la seguridad de impresión/documentos:

- Empresas con preocupaciones por la seguridad y el cumplimiento que adoptan una infraestructura de seguridad de la IT
- Empresas motivadas por los beneficios en los costes y la eficiencia de la IT que aportan las iniciativas de seguridad
- » Entrevistas realizadas por IDC con organizaciones que han iniciado un programa de seguridad de impresión revelaron que han alcanzado las ventajas más significativas y el valor para la empresa en tres áreas: Mejora en la seguridad de las impresoras, eficiencias en el personal de IT y reducciones de costes. Las organizaciones entrevistadas informaron de un conjunto destacable de ventajas para sus entornos de seguridad e impresión, que incluye:
 - Hasta seis veces menos de fallos de seguridad relacionados con la impresora tras la implementación de soluciones de seguridad de la impresora
 - Reducción media a la mitad del tiempo que dedica el personal a dar asistencia a los entornos de impresión tras la implementación de soluciones de seguridad de la impresora
 - Ahorro medio de un 15 % en los costes del papel, tóner y tinta
- » La forma en que se implementan las soluciones de seguridad de impresión determina su efectividad y el impacto que tiene en la productividad de los trabajadores. Se trata de personal tecnológico importante y requisitos de procesos a tener en cuenta para garantizar las máximas ventajas.

TABLA 1

Demografías de empresa de las organizaciones entrevistadas — Entrevistas en profundidad			
	Regular	Media	Rango
Número de empleados	60.300	20.500	De 200 a 290.000
Número de empleados de IT	4.500	610	De 40 a 25.000
Número de usuarios de IT	57.200	19.500	De 180 a 290.000
Total de impresoras	8.800	1.200	De 4 a 100.000
Número de usuarios que imprimen	50.800	9.000	De 200 a 280.000
Número de páginas impresas al año	51 millones	10 millones	De 10.000 a 300 millones

n = 15 organizaciones

Fuente: Entrevistas de seguridad de las impresoras de IDC, 2015

Telecomunicaciones, fabricación, servicios financieros, editorial, aeroespacial, biotecnología, educación y sanitario



En este informe técnico

Este informe técnico se basa en la investigación principal y secundaria que IDC ha realizado referente a la TI y a la seguridad relacionada con la impresión. IDC realizó entrevistas en profundidad de julio a septiembre de 2015 a personas responsables de la implementación y la gestión de soluciones de seguridad de las impresoras en 16 organizaciones. Las entrevistas se pensaron para permitir a IDC comprender el impacto cuantitativo y cualitativo del uso de soluciones de seguridad para impresoras para empresas por parte de las organizaciones. Las entrevistas reflejaron la experiencia de un conjunto diverso de organizaciones. La tabla 1 ofrece una introducción al entorno de impresión de las 16 organizaciones entrevistadas.

IDC complementó las entrevistas en profundidad con el análisis de las encuestas. Los entrevistados cualificados procedían de más de 440 organizaciones de todos los tamaños y eran empleados a tiempo completo. Los entrevistados debían tener conocimientos del equipo de impresión que utilizaba la empresa y de las políticas de seguridad informática de la misma.

Introducción de la situación

Por qué las empresas deberían preocuparse por la seguridad de la infraestructura de impresión/documentos

La mayoría de organizaciones han convertido la seguridad de la IT en una prioridad y tiene razón de hacerlo. La proliferación de la informática, los móviles, la nube y otras tecnologías facilita un entorno de IT donde los trabajadores cualificados necesitan y piden un acceso “en cualquier momento y en cualquier lugar” a la información de la empresa. Sin embargo, IDC a menudo ve que los activos de impresión y las tecnologías relacionadas con la impresión son un elemento que se ignora en la estrategia de seguridad de la IT de las organizaciones.

Así que, ¿por qué deberían las empresas cambiar su aproximación existente ante la seguridad de impresión y asegurar sus dispositivos de impresión como lo hacen con otras tecnologías (PC, servidores, dispositivos móviles, etc.)? La respuesta es que una infraestructura de impresión no segura se traduce en un entorno de IT no seguro. El riesgo de fallos de seguridad relacionados con la impresora es más alto de lo esperado e implican responsabilidades costosas.

La encuesta de IDC concluyó que más de la mitad de las empresas han tenido fallos de seguridad en la IT que incluyen la seguridad de impresión durante los últimos 12 meses.

Las preocupaciones de seguridad por la propiedad intelectual, información confidencial o restringida, cumplimiento de las regulaciones y la necesidad de una infraestructura de seguridad de IT coherente en toda la empresa son factores clave para un programa de seguridad de impresión.

La encuesta de IDC concluyó que más de la mitad de las empresas han tenido fallos de seguridad en la IT que incluyen la seguridad de impresión durante los últimos 12 meses. Esta vulnerabilidad puede proceder de ataques malintencionados o de fuera de la organización además del uso negligente de los dispositivos de impresión y de las impresiones. Los fallos de seguridad potenciales relacionados con la impresión se podrían producir desde los puertos de red, la interceptación de los trabajos de impresión/copia/escaneo, los discos duros y la memoria (RAM) de las impresoras/equipos multifunción, los documentos impresos o copiados que quedan en las bandejas de salida o el uso ilegal de soporte medios seguros (cheques, recetas), entre otros. En profundidad:

- » Los puertos de red no seguros son un punto de entrada a la red de la empresa y a sus activos de información.
- » La impresión de documentos confidenciales (es decir, documentos con información de pacientes o transacciones financieras de clientes) en impresoras compartidas donde los documentos permanecen en las bandejas de salida durante períodos de tiempo es una oportunidad para robar información confidencial y fallos en el cumplimiento de la normativa.
- » La transmisión de impresiones/escáneres no cifrados es prácticamente una invitación a los piratas informáticos.

Los fallos de seguridad resultan costosos. Hay tres tipos de responsabilidades financieras potenciales:

- » **Recursos de la empresa utilizados para solventar el fallo.** Las empresas que sufran un fallo de seguridad utilizarán un tiempo significativo de los trabajadores y unos costes para “limpiar” el incidente. Las oportunidades potenciales que generan ingresos se retrasan o cancelan para hacer frente al fallo.
- » **Multas/penalizaciones.** Las empresas pueden enfrentarse una penalización financiera por incumplimiento (por ejemplo, HIPAA) o demandas de un cliente por el incumplimiento de la confidencialidad.
- » **Reputación de la empresa.** Como consecuencia del incidente, la organización todavía podría sufrir financieramente debido a una pérdida de reputación o mala prensa.

Activadores de la infraestructura de seguridad de impresión

En base a las entrevistas en profundidad con las organizaciones que han implementado

El ahorro en costes es una de las ventajas adicionales, aunque importantes, de adquirir un plan de seguridad de impresión segura y de sus documentos relacionados.

varios niveles de seguridad de impresión, hemos detectado los siguientes activadores para su implementación:

- » Preocupaciones por la seguridad y el cumplimiento (que incluye la reacción a un fallo)
- » Estandarización de la seguridad proactiva a través de la infraestructura de IT
- » Ahorros en costes y eficiencia de la IT

Preocupaciones de seguridad y cumplimiento

Las preocupaciones de seguridad por la propiedad intelectual, información confidencial o restringida, cumplimiento de las regulaciones y la necesidad de una infraestructura de seguridad de IT coherente en toda la empresa son factores clave para un programa de seguridad de impresión. Algunas organizaciones implementan de forma reactiva programas de seguridad de impresión más sólidos en respuesta a los incidentes y a los fallos pasados.

En palabras de un director de sistemas senior de una empresa de servicios financieros: “Las preocupaciones por la seguridad están en todas partes, y la impresora es un dispositivo de acceso público que se utiliza para usos confidenciales, restringidos y no confidenciales. Todos los dispositivos de red que tratan con datos confidenciales/restringidos están sujetos a la seguridad, al cumplimiento y a los requisitos de auditorías; por eso tenemos que hacerlo.”

Estandarización a través de la infraestructura de IT

La estandarización de la seguridad a través de una infraestructura de IT general de la organización también promueve la adopción de la seguridad de la impresión y de los documentos relacionados además de una política completa para resolver cualquier incidencia relacionada con el uso del equipo. Un vicepresidente de tecnología de la información de una editorial explicó: “Queríamos seguridad basada en la política, autorresolutiva y fundacional de certificados de identidad [para impresoras] coherentes con nuestra aproximación a otros servicios de la infraestructura.”

Ahorros en costes y eficiencias de la IT

De media, estas organizaciones informaron de la reducción de la frecuencia de fallos de seguridad relacionados con la impresora en hasta seis veces desde la implementación de las soluciones de seguridad de la impresora empresarial.

Cualquier iniciativa de IT que ayude a recortar los costes operativos de una organización resultará atractiva para los altos directivos. El ahorro en costes es una de las ventajas adicionales, aunque importantes, de adquirir un plan de seguridad de impresión segura y de sus documentos relacionados. Aunque esta ventaja puede que no haya sido el motivo principal para adoptar un programa de seguridad de impresión y de documentos, su impacto fue la ventaja principal destacada por un tercio de los participantes en la encuesta.

Un director de IT senior de una empresa de servicios financieros explicó: “La necesidad de proteger la propiedad intelectual y los impactos financieros potenciales relacionados con los fallos en la seguridad de los datos ha formado la base del porqué de la implementación de estas soluciones... estamos convencidos de que los controles que limitan la impresión irreflexiva e innecesaria han ahorrado dinero en papel y en costes materiales.”

Evidentemente existen ventajas de ahorro de costes “menos directas” también disponibles a través de una iniciativa de seguridad de impresión. Varias organizaciones destacaron que las eficiencias de la IT obtenidas de la centralización y estandarización de la impresión y la seguridad tiene ventajas de costes. Al gestionar la gestión y la seguridad de impresión, el departamento de IT se libera y puede atender a otras necesidades tecnológicas prioritarias para la organización. Por ejemplo, un director de IT en una universidad explicó: “Estábamos buscando consolidar el control de costes y el control de la gestión central de nuestro entorno de impresión.”

Valor para la empresa de la seguridad de las impresoras

Las entrevistas en profundidad de IDC con 16 organizaciones que utilizan soluciones de seguridad para impresoras empresariales reveló que consiguen un valor para la empresa significativo mediante la implementación de estas soluciones. Estas entrevistas, donde IDC preguntó a las organizaciones que describieran sus entornos de impresión antes y después de la implementación de las soluciones de seguridad para las impresoras, mostraron que las organizaciones alcanzan sus objetivos de crear entornos de impresión más seguros mientras que continúan capturando eficiencias en términos de los costes relacionados con la impresión y el tiempo del personal.

» **Seguridad.** Los entornos de impresoras se han convertido en más seguros y los costes

relacionados con la corrección de los fallos de seguridad y garantizar el cumplimiento de las normativas y auditorías se han reducido.

- » **Eficiencia del personal de IT.** La cantidad de tiempo que el personal necesitaba para gestionar y mantener los entornos de la impresora y crear, modificar y aplicar la política relacionada con la impresora se ha reducido, permitiendo que trabaje en otras iniciativas.
- » **Ahorro de costes.** Los costes asociados con la impresión se han reducido mediante la visibilidad mejorada y ha cambiado el comportamiento referente a la impresión, incluyendo ahorros en las impresoras y en sus consumibles.

TABLA 2

Impacto de las soluciones de seguridad de las impresoras para empresas en los

fallos de seguridad — Entrevistas en profundidad

Fallos de seguridad generales

Número medio de fallos al año — antes de la implementación de la seguridad de la impresora 9,9

Número medio de fallos al año — con seguridad de las impresoras 1,5

Cambio en el número de fallos de seguridad Hasta 6 veces menos

Fallos de seguridad significativos

Número de organizaciones entrevistadas que padecen 5

Número medio de empleados afectados 54

Tiempo medio que necesitan los empleados para resolverlo (horas) 277

n = 16 organizaciones

Coste medio total para remediar por fallo (incluyendo penalizaciones) 521.400 dólares

Fuente: Entrevistas de seguridad de las impresoras de IDC, 2015

Como resultado, las organizaciones entrevistadas declararon a IDC que, de media, su personal ha reducido a la mitad el tiempo necesario para dar asistencia a los entornos de impresión tras implementar las soluciones de seguridad de las impresoras.

Reducción del riesgo: Mejor seguridad de la impresora y el cumplimiento de normas

Las organizaciones entrevistadas informaron de que han aprovechado el uso de las soluciones de seguridad de la impresora de la empresa para reducir el impacto de los fallos de seguridad relacionados con la impresora y hacer esfuerzos de cumplimientos de forma más efectiva y rentable.

IDC preguntó a los participantes en la entrevista en profundidad sobre la frecuencia en la que se producían los fallos de datos y de seguridad relacionados con la impresora en sus organizaciones y sobre si sus organizaciones han experimentado lo que definirían como fallos de seguridad sustanciales relacionados con las impresoras. De media, estas organizaciones informaron de la reducción de la frecuencia de fallos de seguridad relacionados con la impresora en hasta seis veces desde la implementación de las soluciones de seguridad de la impresora empresarial. La implementación del cifrado de los trabajos de impresión, la autenticación de los usuarios y la impresión pull han permitido un nivel de seguimiento y recuento que garantiza y ayuda a prevenir los fallos. Además, la seguridad de la impresora ha ayudado a completar algunas iniciativas de seguridad de TI en toda la infraestructura, cerrando así los posibles fallos que quedaban. Las organizaciones entrevistadas dieron ejemplos de fallos de seguridad relacionados con la impresora que habían experimentado, que incluyen:

- » **Impresión de información confidencial con intención de hacer un mal uso de la misma.** Un director de IT en una empresa de fabricación explicó que su organización perdió propiedad intelectual como resultado de que, entre otras cosas, los empleados imprimiendo información de propiedad intelectual de alto nivel y entregándola a la competencia.
- » **Impresión y uso indebido de datos seguros.** Un director de IT de una empresa de servicios financieros explicó que los empleados de su organización ponían diseños y otras propiedades intelectuales en riesgo al imprimir de forma indiscriminada o al dejar trabajos de impresión en la impresora

Organizaciones entrevistadas aportaron varios ejemplos de cómo el uso de soluciones de seguridad de impresión empresarial les ha ayudado a minimizar el impacto de los fallos de seguridad a través de las impresoras:

- » **Protección de la información a través del proceso de impresión.** Un vicepresidente de tecnología de la información de una editorial explicó: "La solución se ha convertido en una herramienta vital para proteger el flujo de trabajo del contenido y de los datos de las impresoras a través de la red, asegurando la confianza efectiva lo que nos permite

reducir las oportunidades de que se produzcan fallos.”

- » **Evitar la impresión innecesaria o inadecuada.** Un director de IT de una empresa de servicios financieros afirmó: “Los documentos confidenciales que distribuimos de forma interna no se deberían imprimir. Estas soluciones nos ayudan a minimizar los fallos, un número creciente de los cuales se produce de forma interna, ya sea de forma expresa o como resultado de la impresión indiscriminada.”

Como muestra la tabla 2, aunque todos los fallos de seguridad relacionados con la impresora pueden conllevar costes, es importante que las organizaciones eviten los fallos de seguridad significativos debido a los costes sustanciales que implica remediarlos. Según las cinco organizaciones entrevistadas que han experimentado lo que describen como fallos de seguridad significativos relacionados con las impresoras, el coste medio de un fallo de seguridad significativo incluye pérdidas de la productividad de 54 empleados, 277 horas de tiempo para remediarlo y un coste de más de 500.000 dólares por fallo, incluyendo las penalizaciones.

Además de reducir la frecuencia de los fallos de seguridad relacionados con la impresora, 10 de las 16 organizaciones entrevistadas reconocía sus soluciones de seguridad de las impresoras con el cumplimiento de las normativas y esfuerzos de auditorías más efectivas y eficientes. Una mejora en seguridad y seguimiento potencia estas ventajas:

- » **Seguridad mejorada:** Un director de sistemas en una empresa de servicios financieros explicó: “En el núcleo de la implementación de este modelo de seguridad están las ventajas que obtiene al crear un entorno muy sólido y seguro que protege los datos, documentos, incrementa la confidencialidad del diseño, la arquitectura y la seguridad de las impresoras que ha ayudado significativamente a alcanzar nuestros estándares de seguridad.”
- » **Trazabilidad y visibilidad:** Un vicepresidente de operaciones de IT de una empresa de ciencias biológicas explicó: “Hemos podido crear un seguimiento de auditorías, evitar la interceptación de datos y mostrar que hemos restringido el acceso de los usuarios a los datos confidenciales. Además nuestra verificación y auditoría incluye la identificación de riesgos y el análisis de amenazas, junto con las soluciones recomendadas para los problemas. Obtenemos una visión en profundidad del estado del sistema y podemos realizar una monitorización en tiempo real: todos ellos requisitos para el cumplimiento.”

Estas mejoras también han significado ahorros de tiempo y costes de los esfuerzos de cumplimiento y auditorías de las organizaciones. De media, las organizaciones entrevistadas informaron de que su uso de soluciones de seguridad les ahorra más de 200 horas de tiempo de empleados al año, casi 250.000 dólares al año de costes relacionados, que incluyen los

costes de asistencia de terceros de auditorías y cumplimientos.

Ventajas en la productividad del personal del departamento de informática

Las organizaciones entrevistadas por IDC informaron que han reducido la carga de tiempo de gestionar y dar asistencia a sus entornos de impresión desde la implementación de soluciones de seguridad de impresoras. Estas deficiencias se han visto potenciadas por factores como la introducción o ampliación del uso de capacidades de gestión centralizada y automatización, además de poder resolver más rápidamente las incidencias relacionadas con las impresoras. Un director de IT senior de una empresa de servicios financieros explicó: "Ha supuesto un gran impacto en el personal [el uso de soluciones de seguridad para impresoras], en lo que se refiere a las horas invertidas en actividades que requieren tiempo y al liberar al equipo para centrarse en actividades más estratégicas. La respuesta a las incidencias relacionadas con la impresora ya no es aislada, sino que está integrada y es repetible." Como resultado, las organizaciones entrevistadas declararon a IDC que, de media, su personal ha reducido a la mitad el tiempo necesario para dar asistencia a los entornos de impresión tras implementar las soluciones de seguridad de las impresoras.

Las organizaciones entrevistadas informaron de que las soluciones de seguridad de impresoras han permitido más eficiencia en el personal para sus entornos de impresión. Los ahorros en tiempo de personal resultan de los cambios como la automatización del soporte y mantenimiento que incluye la automatización de los certificados además de la aplicación de otros procesos repetibles. Por ejemplo, un vicepresidente en una empresa de servicios financieros que utiliza certificados únicos y políticas de autenticación de empleados explica cómo alcanzó una disminución del 60 % del tiempo que el personal dedicaba a monitorizar dispositivos: "Ahorramos tiempo de personal de IT porque se pueden crear perfiles fácilmente y aplicarlos a muchos dispositivos simultáneamente y podemos automatizar la gestión de certificados."

Mientras tanto, las organizaciones entrevistadas también se benefician de los ahorros en tiempo que permiten las soluciones de seguridad de la impresora al crear, aplicar y modificar las políticas relacionadas con las impresoras. De media, el personal de estas organizaciones dedica un 59 % menos de tiempo en políticas relacionadas con las impresoras. Más allá de los ahorros en tiempo de personal, una implementación más efectiva de la política relacionada con las impresoras tiene más ventajas como la reducción de la posibilidad de fallos y la creación de una guía más efectiva para el uso de

Las iniciativas de seguridad de impresoras ha hecho que los empleados que imprimen sean más conscientes de cómo usan las impresoras y han contribuido a los ahorros relacionados con los costes relacionados con la

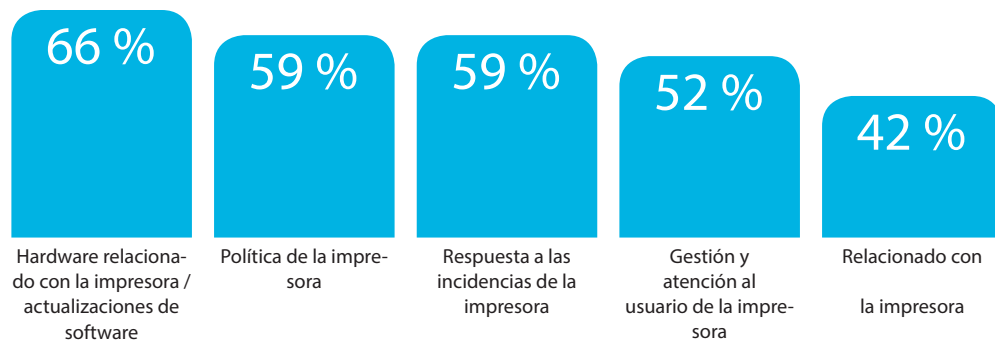
la impresora.

Cuando surgen problemas relacionados con la impresora, las organizaciones entrevistadas afirmaron que sus empleados se han beneficiado de las funciones de las soluciones de seguridad de las impresoras como tener (o mejor aprovechar) las consolas centrales y el acceso remoto a las impresoras. Estos factores, además de la política relacionada con las impresoras mejorada, han ayudado a las organizaciones entrevistadas a reducir en una media del 59 % y del 42 %, respectivamente, el tiempo necesario para responder a las incidencias relacionadas con las impresoras y a responder a las llamadas relacionadas con las impresoras de los usuarios de impresoras (consulte la figura 1). Un vicepresidente de IT en una empresa pública que utilizaba soluciones de seguridad que incluyan la reparación automática y gestionaba certificados únicos explicó el impacto en su equipo de la capacidad de dar asistencia a las impresoras: "Ahora tenemos menos incidencias, y las que se producen se solucionan en menos tiempo. El impacto, que es favorable, es que libera tiempo para otras actividades de asistencia y de planificación." Un director de IT en una empresa de servicios financieros que utiliza un producto de gestión de seguridad de impresoras afirmó: "Nuestra atención al usuario ahora tiene una visión clara de la configuración de la impresora, los permisos y las incidencias y puede actuar independientemente o contactar un equipo de impresión de pequeñas empresas para obtener asistencia de nivel 2."

FIGURA 1

Ahorro medio en tiempo de personal relacionado con las impresoras —

Entrevistas en profundidad



n = 16 organizaciones

Fuente: Entrevistas de seguridad de las impresoras de IDC, 2015

IDC recomienda que una organización blinde su tecnología de seguridad de impresión/ documentos.

Reducciones de costes relacionados con la impresión

Cualquier iniciativa de IT que también reduzca los costes incrementa su atractivo. Como resultado, la capacidad de las organizaciones entrevistadas para alcanzar ahorros en costes mediante su implementación de soluciones de seguridad de impresión ha sido un valor añadido sustancial. Prácticas como la autenticación de los empleados y la impresión pull estaban entre las más utilizadas por los participantes en las entrevistas en profundidad (más de dos tercios de las organizaciones entrevistadas las utilizan). Estas soluciones preservan la confidencialidad de los documentos y potencian los ahorros de costes al requerir a los usuarios de impresión que realicen pasos afirmativos para imprimir documentos reduciendo el número de trabajo de impresión mal dirigidos o no reclamados. La capacidad de las soluciones de seguridad de las impresoras para servir como vehículo para reducir los costes relacionados con la impresora son suficientemente claros y varias organizaciones entrevistadas destacaron la optimización de costes como el impulso principal para su uso de soluciones de seguridad de la impresora.

Las organizaciones entrevistadas explicaron que las soluciones de seguridad de las impresoras les ayudaron a reducir los costes con:

- » **Reducción de la impresión al modificar el comportamiento de impresión:** Un tesorero corporativo en una empresa del sector alimentario afirmó: "La función de impresión pull que utilizamos nos permite enviar a imprimir pero requiere la introducción de su identificador en la impresora para poder imprimir. Creo que se han reducido al menos, por los números que he visto, entre un 21 % y un 24 % las impresiones que hacíamos antes."
- » **Proporcionar visibilidad al uso de la impresora:** Un director de IT en una universidad indicó: "Ahora podemos hacer un seguimiento del coste de las páginas impresas y cargarlos a los departamentos correspondientes." Con la capacidad de atribuir los costes de impresión basados en departamentos, la universidad puede atribuir las cargas a cada departamento y obtener fórmulas para que los usuarios de la impresora sean tan eficientes como sea posible.
- » **Decomisiones innecesarias o impresoras obsoletas:** Un vicepresidente en una organización de servicios financieros destacó: "Estamos reduciendo el número de trabajos de impresión innecesarios cuando se sabe que la actividad de impresión está supervisada y estamos retirando y sustituyendo el hardware de impresión antiguo que no admita las líneas básicas de seguridad de impresión empresarial."

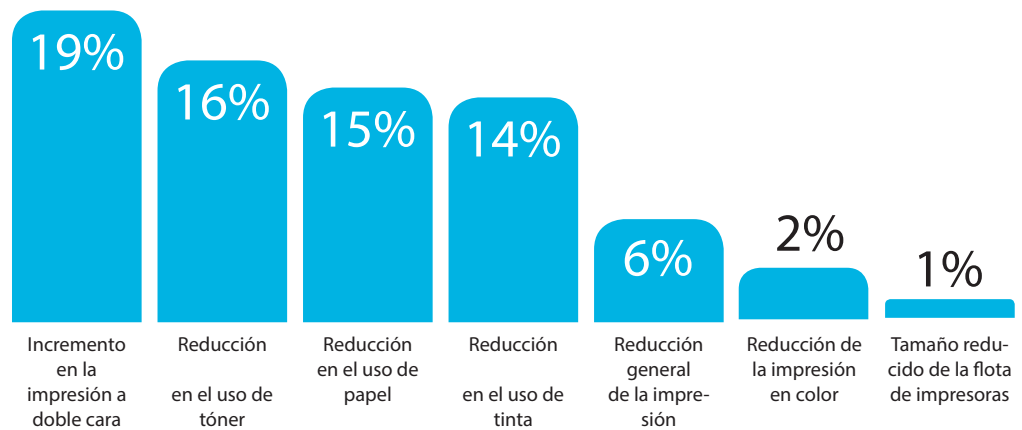
Las iniciativas de seguridad de impresoras ha hecho que los empleados que imprimen sean más conscientes de cómo usan las impresoras y han contribuido a los ahorros

relacionados con los costes relacionados con la impresora. De media, los participantes en las entrevistas en profundidad afirmaron que sus empleados envían un 43 % menos de trabajos de impresión a la impresora incorrecta. Como resultado, menos trabajos de impresión quedan abandonados o se repiten. Como se muestra en la figura 2, estos tipos de entornos han contribuido a un uso de impresoras general más eficiente, que incluye menos impresión en general (reducción de un 6 % de media), imprimir más en doble cara (un incremento del 19 %) y una pequeña disminución de la impresión en color (reducción del 2 %). Estos factores, además de una mejora en la visibilidad de los entornos de impresión, han permitido que las organizaciones entrevistadas consigan mayores ahorros de costes en sus entornos de impresión, que incluye el número de impresoras que utilizan y mantienen (reducción del 1 %, o 115 impresoras de media por organización) además de los costes asociados al papel, la tinta y el tóner (reducciones del 15 %, 14 % y 16 % respectivamente).

FIGURA 2

Media de ahorro de costes de impresión y eficiencias de las impresoras — Entrevistas en profundidad

(% de eficiencia o mejora)



n = 16 organizaciones

Fuente: Entrevistas de seguridad de las impresoras de IDC, 2015

Sede central global de IDC

5 Speen Street

Framingham, MA 01701

EE. UU.

508.872.8200

Twitter: @IDC

idc-insights-community.com

www.idc.com copyright

Publicación externa de información y datos de IDC — Toda la información de IDC que se deba utilizar en publicidad, ruedas de prensa o materiales promocionales requiere la aprobación anterior y por escrito del vicepresidente o responsable de IDC del país pertinente. Dicha solicitud debería ir acompañada de un borrador del documento propuesto. IDC se reserva el derecho de denegar la aprobación del uso externo por cualquier motivo.

Copyright 2015 IDC. La reproducción sin el permiso por escrito queda terminantemente prohibida.

Desafíos.

Con prácticamente todas las implantaciones de las organizaciones, algunos retos se pueden evitar con una planificación. Los retos del grupo del estudio abarcaban las tres fases de la implantación de la seguridad de la impresión: planificación, implementación y postimplementation.

Las empresas estudiadas informaron que sentían una restricción de tiempo para desarrollar la estrategia y el plan. Se necesita un tiempo inicial significativo para alcanzar la reducción en la carga de trabajo de IT tras la implementación. Además, la aplicación del cumplimiento de los empleados debería ser un proceso automatizado que abarque herramientas de supervisión, un proceso de escalada y las correcciones para reducir las llamadas de atención al cliente relacionadas con la impresión.

Para los usuarios de las impresoras de la organización, observamos dos precauciones que se deberían planificar:

- » **Equilibrar bien la seguridad de la impresión mientras se minimiza la productividad de los empleados:** La seguridad empresarial debe ser de la máxima importancia, pero una organización debería trabajar en un sistema que tenga el menor impacto negativo en la productividad. Por ejemplo, algunas organizaciones que implementan

Acerca de IDC

International Data Corporation (IDC) es el principal proveedor global de inteligencia de mercados, servicios de consultas y eventos para la tecnología de la información, los mercados de telecomunicaciones y tecnología de consumidores. IDC ayuda a los profesionales de IT, ejecutivos empresariales y la comunidad de inversores a tomar decisiones basadas en hechos sobre la adquisición de tecnología y la estrategia empresarial. Más de 1.100 analistas de IDC aportan conocimientos expertos globales, regionales y locales sobre oportunidades de tecnología y del sector y tendencias en más de 110 países de todo el mundo. Durante 50 años, IDC ha aportado información estratégica para ayudar a nuestros clientes a alcanzar sus objetivos empresariales clave. IDC es una filial de IDG, la empresa líder en investigación, eventos y tecnología de medios.

la impresión pull para solventar sus necesidades de seguridad de la impresión pueden topar con la resistencia de los usuarios frente a la necesidad de autenticar (es decir, introducir una contraseña) y esperar que se imprima todo el documento. La contrapartida en este caso es la protección de la información contenida en el documento (es decir, nadie puede ver los documentos impresos dejados sin supervisión a la bandeja de salida) frente a esperar que un documento se imprima (es decir, la impresión se inicia solo después de que el usuario se haya autenticado en el dispositivo).

- » **Formación de los empleados:** Relacionado con la productividad de los empleados, el plan de seguridad de impresión debe incluir el proceso y el tiempo necesarios para formar a los empleados en políticas y procedimientos nuevos. Las empresas deberían estar preparadas para proporcionar la formación de forma repetida y utilizar diferentes formatos que se adapten a las generaciones de empleados y a los diferentes estilos de aprendizaje.

Guía esencial

IDC ha identificado varias razones convincentes para incorporar la impresora y los flujos de trabajo de documentos relacionados en un marco de seguridad de IT de toda la organización. Evidentemente, una de las ventajas principales tiene que ver con la provisión de un programa de seguridad de IT integral que incluya la impresión, pero dicho plan también tiene un número de ventajas significativas más allá de la seguridad. Dos ventajas clave son los ahorros de costes notables y el incremento en la eficiencia de IT.

IDC recomienda que una organización blinde su tecnología de seguridad de impresión/documentos. La organización debe reconocer que este objetivo se puede alcanzar de forma efectiva cuando las personas y los procesos se incorporan en la ejecución del plan.

Tecnología

Referente a la seguridad, la implementación de soluciones de tecnología es básicamente un tema de blanco o negro... una organización es segura o no es segura.

IDC le recomienda que las siguientes capacidades se implementen en toda la organización tan pronto como sea posible. El personal de IT y los proveedores de la infraestructura de impresión deberían garantizar que las siguientes funciones y capacidades estén configuradas para todos los dispositivos de impresión que se utilicen en la organización:

- » Garantizar que todos los dispositivos de impresión conectados en red tengan las siguientes funciones o al menos el firmware actualizado para reflejarlas.
- » Asegurarse de que los dispositivos solo utilizan protocolos de comunicación cifrados y deshabilitar el resto.
- » Establecer un sistema que borre o destruya los datos de los discos duros del dispositivo como parte de la eliminación del dispositivo.
- » Admitir como mínimo una forma de autenticación de usuario (preferiblemente dos o tres), y considerar la implementación de la impresión pull para los entornos de impresión con un alto volumen de información de confidencialidad o requisitos de cumplimiento.
- » Garantizar que el firmware esté actualizado y que solo se cargue firmware legal.
- » Asegurar que todas las unidades de disco duro de la impresora sean seguras (cifrar y borrar los datos de forma periódica).
- » Implementar funciones que evidencien la manipulación o utilizar impresoras con bandejas de bloqueo para soportes especializados si la impresión de la organización lo garantiza. Sería una impresión segura para un objeto potencial de fraude como los cheques, recetas medicas, etcétera.
- » Utilizar una herramienta de gestión de flotas para gestionar, supervisar y remediar el dispositivo de forma centralizada para garantizar el cumplimiento con las políticas de seguridad. De esta forma, la organización puede evitar tener que configurar manualmente y mantener cada dispositivo de forma individual. La herramienta debería permitir la creación y administración simple y fácil de la política de seguridad, detectar cuando se añaden dispositivos a la red, proporcionar la gestión de certificados de dispositivos única y registrar las incidencias de incumplimientos mediante un proceso de escalado y corrección. La herramienta debería trabajar con herramientas de gestión de seguridad de IT que supervisen los extremos acerca de incidentes y anomalías de incumplimiento para que cualquier fallo de seguridad potencial se identifique rápidamente.
- » Asegurar que las impresiones y los escaneos de los equipos de sobremesa y dispositivos móviles (mientras se desplazan o en una posición estática) estén cifrados para garantizar que los datos relacionados con la impresión estén totalmente protegidos. Esto significa que incluso los adjuntos que se deben imprimir se deberían abrir y exponer para un nivel de protección adicional. Una herramienta que supervisa

el contenido impreso y escaneado es un elemento clave para garantizar el nivel más alto de seguridad y para que cumpla con las políticas establecidas de la empresa y los estándares del sector.

Personas

Una organización que se toma en serio sus necesidades de seguridad de IT debe garantizar que el equipo de seguridad incluya personal cualificado en garantizar la seguridad de los dispositivos de impresión y con los documentos de flujos de trabajo relacionados. Este equipo de seguridad puede consistir en el personal interno propio de la organización y/o recursos de seguridad externos cualificados. El equipo se reunirá para aconsejar sobre incidencias futuras de impresión y seguridad de flujo de trabajo además de ayuda con la integración de un plan de seguridad de IT en toda la empresa.

Para garantizar que la seguridad de los dispositivos de impresión y los flujos de trabajo de documentos relacionados no tienen un impacto negativo en la productividad de los empleados, la organización debería recibir información de ciertos empleados de toda la organización como parte del proceso de planificación. También se recomienda la implicación de un experto en gestión de cambios, especialmente si el importe o la naturaleza de los cambios requeridos es significativo. Dicho experto también puede aconsejar sobre la aproximación de formación y la implantación que se debe utilizar.

La mayoría de organizaciones no tienen los conocimientos ni las capacidades necesarias para establecer adecuadamente la seguridad de su infraestructura de impresión y documentos por sí mismas. Por eso, una organización debería plantearse preguntar al proveedor de dispositivos de impresión sobre los recursos que el departamento de IT puede aprovechar. Los recursos abarcan las funciones de seguridad disponibles en el hardware de la impresora/equipo multifunción, las herramientas de software de seguridad y los servicios de seguridad (es decir, servicios profesionales de seguridad, activos de seguridad, gestión de cambios y expertos en el cumplimiento de las regulaciones de sectores concretos) de una organización.

Proceso

Es importante que una organización empiece su iniciativa de seguridad asesorando el estado actual de su entorno de impresión y desarrolle un plan que alcance un nivel de seguridad coherente con el del resto del entorno de IT. Esta iniciativa debería incluir un acuerdo de los requisitos de seguridad básicos específicos para las organizaciones del sector de la organización además de un plan para supervisar, escalar e implementar estas políticas en una base constante.

El plan se debería reevaluar periódicamente utilizando los datos recopilados durante el período para determinar si los ajustes son necesarios y para aprender de los fallos de impresión/documentos fuera de la empresa. Todos los ajustes estarán influenciados por los datos recopilados además de por el nivel de aceptación de la organización sobre el nivel aceptable de riesgos y gastos en seguridad.