SEGURIDAD DE LA INFORMACIÓN EN ACCIÓN

EN UN MUNDO EN EL QUE LAS CIBERAMENAZAS SON CADA VEZ MÁS SOFISTICADAS Y EL CUMPLIMIENTO NORMATIVO ES CADA VEZ MÁS ESTRICTO, ¿CÓMO MANTENDRÁ TU EMPRESA LA SEGURIDAD DE LA INFORMACIÓN?

Canon

ÍNDICE

En la actualidad, los datos son el bien más preciado de toda organización. Aumenta la capacidad del departamento financiero, proporciona a los equipos ejecutivos poderes de predicción y dota a los empleados de una mayor inteligencia empresarial.

Este valioso recurso debe protegerse, cueste lo que cueste.

A medida que el valor de los datos aumenta, también lo hace el número de enemigos que intentan hacerse con ellos: los atacantes están al acecho para robar la información cuando menos te lo esperas. Al mismo tiempo, los agentes dobles pueden llevarse los datos para sí mismos.

Pero no hacen falta enemigos para acabar con una organización.

Estamos sometidos a un control normativo que garantiza que todo el mundo siga las normas de cumplimiento de los datos. Pero aunque las leyes son estrictas y las sanciones son severas, nunca ha sido tan fácil cometer un error.

Las empresas de hoy en día no funcionan como una ciudad amurallada, y con frecuencia vemos que se sitúan en distintos puntos geográficos. El trabajo híbrido significa que los empleados almacenan y comparten información, y colaboran entre ellos desde diversas ubicaciones.

En un entorno de trabajo tan complejo, mantener la información segura y los procesos de conformidad con las normativas puede parecer un desafío imposible.

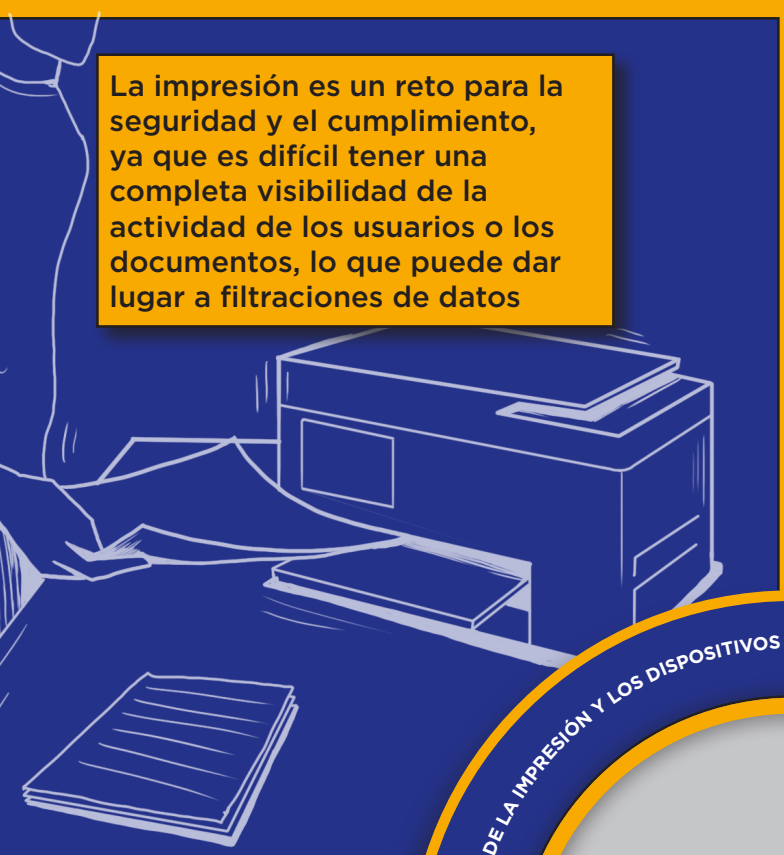
Necesitas un socio de confianza que pueda proteger tus datos, protegerte de los ciberdelincuentes y ayudar a tus empleados a cumplir las normas en todo momento.

Veamos cómo Canon y nuestras armas secretas pueden ayudarte a superar el desafío.

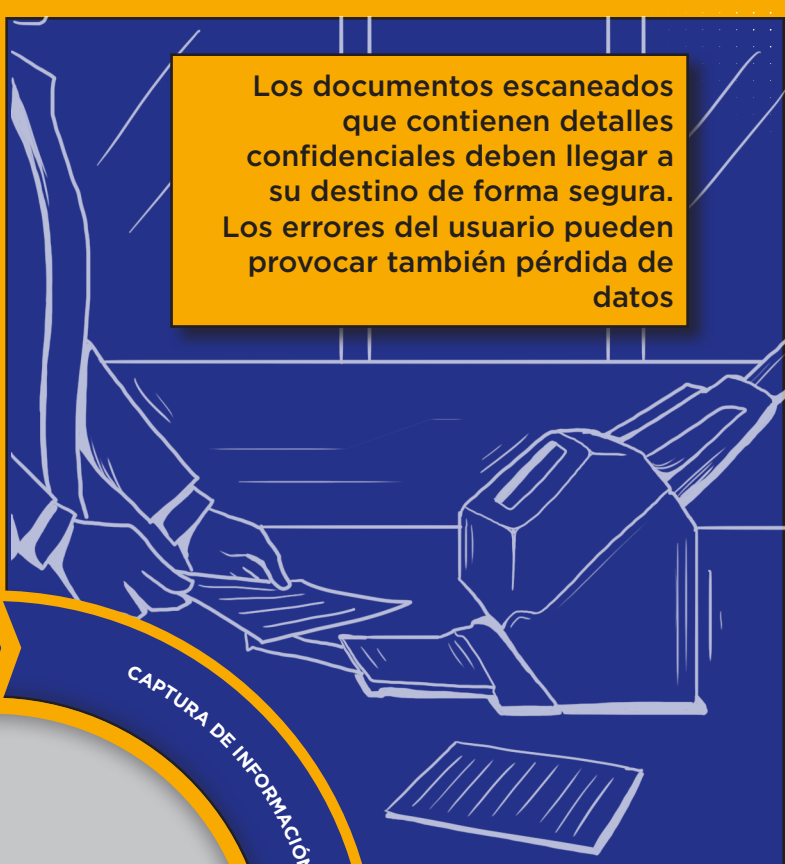
DESAFÍOS EN EL CICLO DE VIDA DE LOS DOCUMENTOS

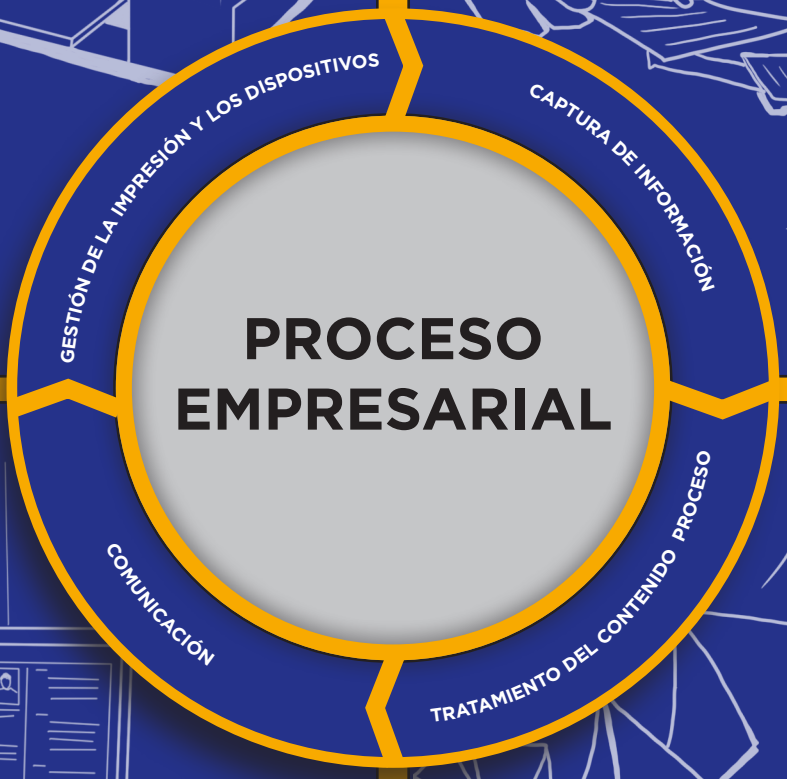
Los documentos se crean, copian, almacenan y comparten durante su ciclo de vida dentro de tu organización; todas estas etapas plantean retos para mantener la seguridad de los datos que contienen, así como el cumplimiento.

La impresión es un reto para la seguridad y el cumplimiento, ya que es difícil tener una completa visibilidad de la actividad de los usuarios o los documentos, lo que puede dar lugar a filtraciones de datos

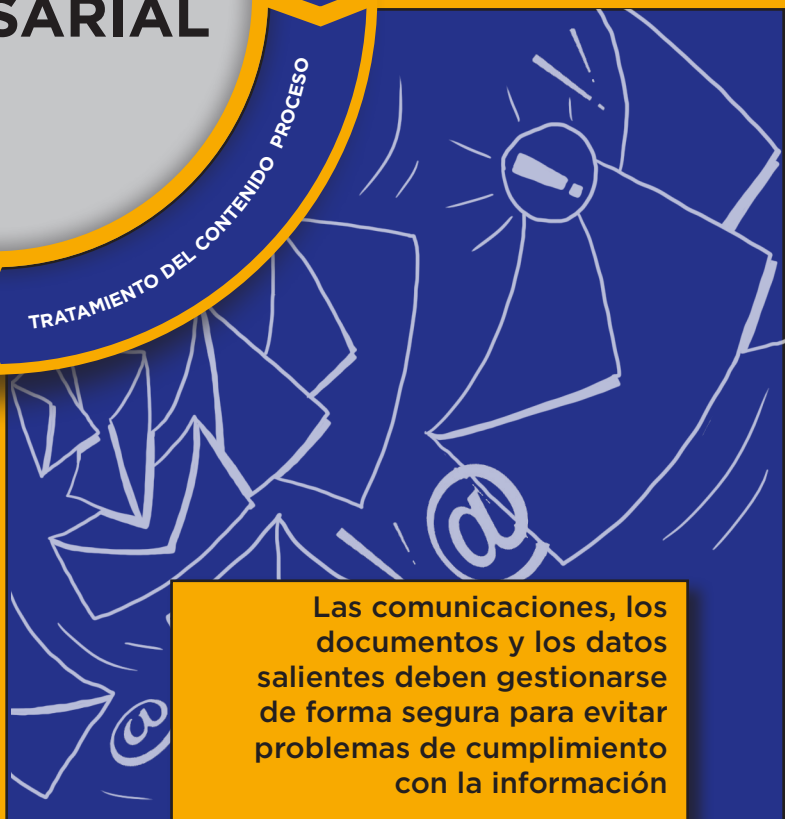


Los documentos escaneados que contienen detalles confidenciales deben llegar a su destino de forma segura. Los errores del usuario pueden provocar también pérdida de datos





Los datos personales y la información confidencial de los clientes y empleados deben almacenarse, tratarse y destruirse de forma segura, en cumplimiento de las normas de privacidad de los datos



Las comunicaciones, los documentos y los datos salientes deben gestionarse de forma segura para evitar problemas de cumplimiento con la información

DESAFÍO 1

LA ESTRATEGIA SECRETA

La organización X tiene un gran secreto: está preparada para embarcarse en una nueva aventura. El equipo directivo ha decidido invertir en una nueva área de negocio con la esperanza de obtener nuevas oportunidades y descubrir riquezas incalculables.

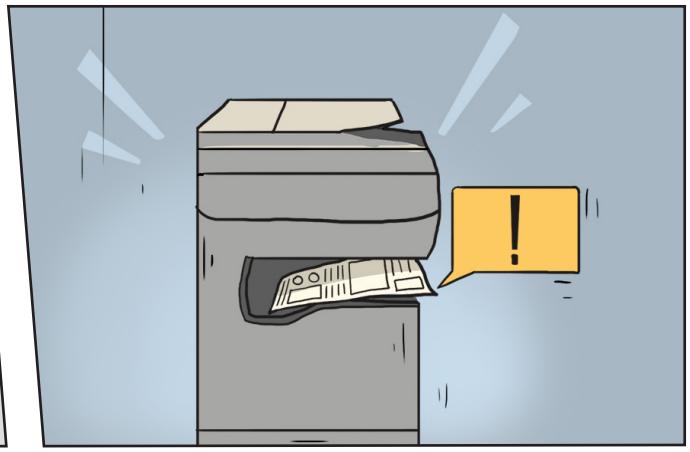
Es esencial que estos planes permanezcan en secreto hasta que se hagan públicos. La noticia revelaría el plan de la organización X a sus rivales, lo que les advertiría de que hay un nuevo competidor en el mercado. Por su parte, los empleados de la organización X se están jugando mucho: ¿podría haber nuevas oportunidades en su departamento? ¿Nuevas áreas de negocio que descubrir? ¿Es posible que sus empleos estén en peligro?

El equipo directivo debe proceder con cuidado si quiere asegurarse de que sus planes no caen en manos de empleados conspiradores ni de enemigos externos. A lo largo del proceso de elaboración del presupuesto y de los anuncios, debe salvarse toda una serie de obstáculos, desde las amenazas internas hasta el malware y los ataques a la red. ¿Es posible guardar el secreto?

El equipo de comunicaciones ha redactado un comunicado de prensa que refleja la nueva dirección estratégica de la organización. La información sigue siendo confidencial y un grupo reducido de altos ejecutivos está redactando y aprobando el comunicado. Selma, la directora financiera, ha solicitado revisar una copia física del documento. Polina, su ayudante, lo tiene todo preparado para imprimir la copia.

La impresión del documento representa una amenaza de seguridad más importante de lo que las organizaciones creen. Entre los riesgos habituales de seguridad y cumplimiento de normativas se incluyen que los documentos en papel se retiren de la impresora antes de que el usuario los recoja o que se le olviden por completo, exponiendo información sensible o confidencial a personas no autorizadas.

La innovación también ha abierto las puertas a una serie de nuevas amenazas para la seguridad. Las impresoras multifunción modernas son tan potentes como un ordenador, están equipadas con un disco duro, una memoria y una unidad de procesamiento central (CPU), y a menudo están conectadas a Internet. Como resultado, es posible que el firmware de las impresoras sea objetivo de los hackers que intentan acceder a la red y a los datos corporativos.



ARMAS SECRETAS

imageRUNNER ADVANCE DX C5800

La impresora imageRUNNER ADVANCE DX C5800 se ha diseñado con seguridad integrada de serie. Polina solo puede imprimir el documento al iniciar sesión en el dispositivo con su tarjeta de identidad, lo que significa que nadie más puede acceder al documento en la cola de impresión y que este no quede olvidado en la bandeja del dispositivo.

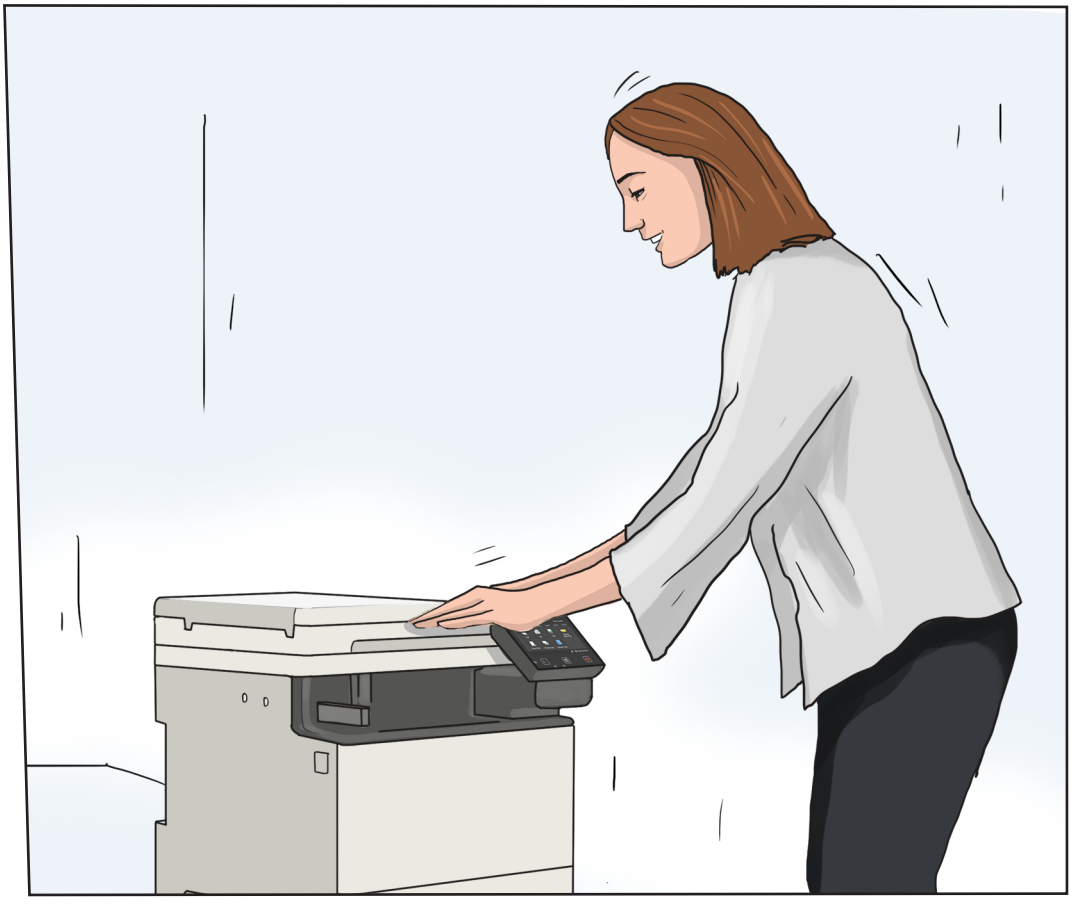
El dispositivo también ofrece Trellix McAfee Embedded Control, que protege contra amenazas persistentes avanzadas (APT) y de día cero al bloquear la ejecución de aplicaciones no autorizadas mediante listas blancas inteligentes. Para evitar que un atacante acceda al comunicado de prensa a través de un acceso no autorizado a la red, McAfee Embedded Control protege contra la manipulación de programas.

Por último, el modelo imageRUNNER ADVANCE DX C5800 admite la integración de la gestión de eventos de información de seguridad (SIEM), lo que facilita a las organizaciones la inclusión de las impresoras en sus sistemas de control de seguridad existentes (por ejemplo, Syslog). Estos sistemas pueden reconocer y marcar los eventos de seguridad en una flota de dispositivos en tiempo real, alertando a la empresa de cualquier problema o amenaza a medida que se producen.

Device Hardening Service
Con Canon, la seguridad comienza incluso antes de comprar un dispositivo. Configuramos los equipos multifunción imageRUNNER ADVANCE para reforzar su seguridad, incluyendo el refuerzo de los controles de seguridad integrados y el bloqueo de las funciones no esenciales y los puertos no protegidos. El dispositivo configurado se comprueba y verifica antes de enviarse.

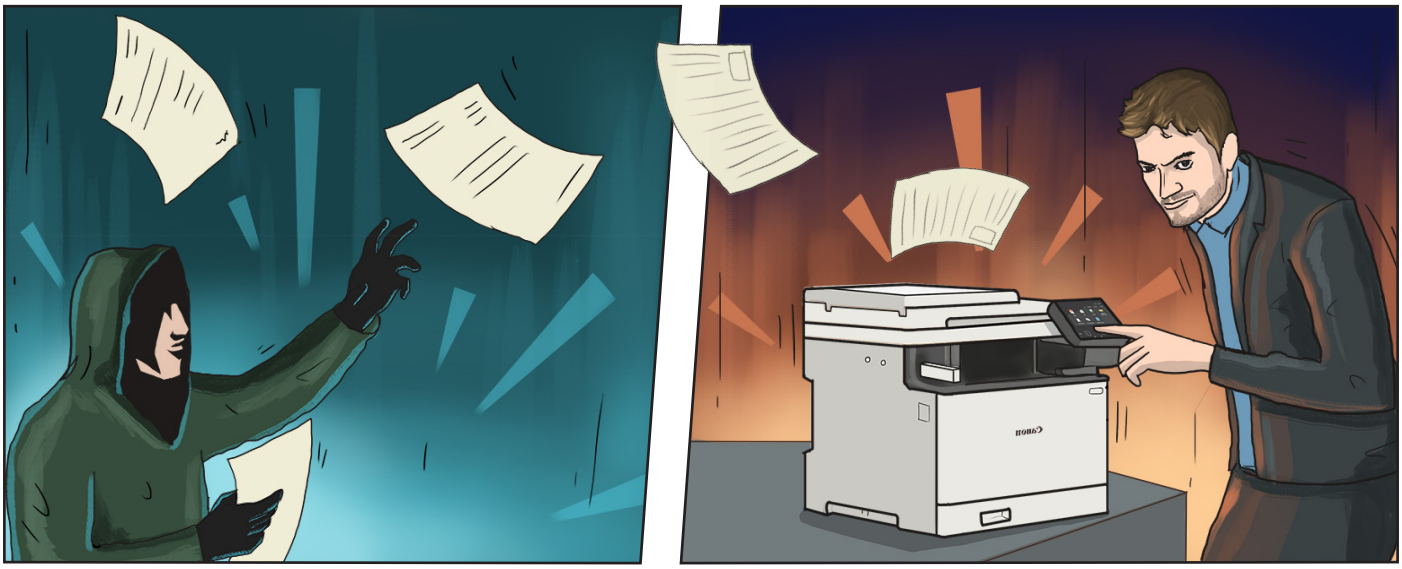
imageWARE Secure Audit Manager Express
Esta solución de seguridad para dispositivos en red permite a la empresa X controlar las actividades relacionadas con los documentos. Puede capturar, archivar y supervisar las actividades que se producen en los dispositivos Canon. Cuando Polina imprime el comunicado de prensa, imageWARE Secure Audit Manager Express envía una alerta por correo electrónico al departamento de TI indicando que se está imprimiendo un documento de alto riesgo. De este modo, la organización X puede detectar a cualquier empleado o persona no autorizada que intente copiar o imprimir información sensible.

Selma ha revisado el comunicado de prensa y ha aportado algunos comentarios por escrito. Polina debe compartir los comentarios con Pierre, el director de Relaciones Públicas responsable del anuncio. Como Pierre trabaja desde casa, Polina tendrá que crear una copia digital para enviársela. Escanear documentos y enviarlos por correo electrónico directamente desde el dispositivo crea una oportunidad para que el atacante intercepte el documento.



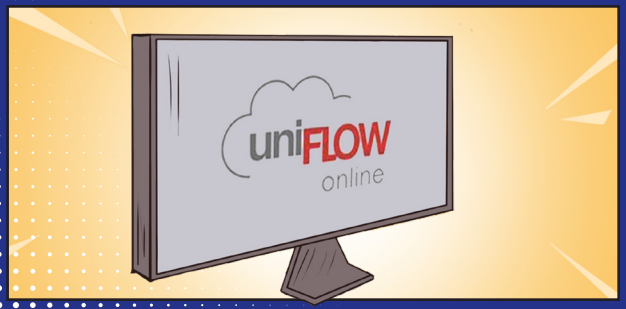
Los dispositivos de escaneo actuales suelen estar conectados a Internet, lo que permite a los usuarios enviar documentos por correo electrónico directamente a un destinatario o guardarlos en destinos en la nube. Como resultado, hay más oportunidades para que la información digital esté en riesgo, por lo que es crucial que los dispositivos de escaneo tengan funciones de seguridad eficaces. Sin funciones seguras, un escáner es vulnerable a la manipulación; por ejemplo, un usuario interno podría cambiar las colas de enrutamiento del correo electrónico para dirigir un mensaje de correo electrónico a un usuario no autorizado. Además, sin una función de cifrado, un documento podría abrirse, editarse o imprimirse libremente.

Desde un punto de vista externo, un atacante también podría acceder a través de la red y realizar cambios en los directorios de correo electrónico, lo que permitiría enviar un documento a destinatarios ajenos a la organización. O podría interceptar un documento transmitido a través de HTTPS si este y sus datos no están cifrados.



ARMAS SECRETAS

i-SENSYS X C1333iF
Selma va a escanear el documento con la impresora i-SENSYS X C1333iF. Este dispositivo multifunción (que combina las funciones de impresión y escaneo) ofrece opciones de escaneo seguras que ayudan a mantener la información a salvo. Al encender el dispositivo, su función de verificación inicial del sistema comprueba si ha habido intentos de comprometer la integridad del dispositivo, y puede alertar a Selma si este se ha manipulado. A continuación, Selma debe iniciar sesión con una tarjeta de identificación, lo que garantiza que haya un registro de quién está copiando o compartiendo información. Por último, la compatibilidad de la i-SENSYS X C1333iF con la norma IEEE802.1X proporciona un mecanismo de autenticación, de modo que cuando se conecta a la LAN o WLAN de la empresa, se confirma su autenticidad.



uniFLOW Online
Cuando Selma escanea el contrato, uniFLOW Online crea un PDF cifrado y ofrece una protección con contraseña opcional. De este modo, se evita que los usuarios no autorizados vean, editen o impriman el documento, y se protege la información de cualquiera que intente interceptarla.

Tobias se ha enterado de que la empresa podría estar tomando una nueva dirección. Como jefe de uno de los equipos que tiene dificultades con la estrategia actual, sabe que esto podría implicar graves recortes en su presupuesto este año, o incluso una amenaza para los puestos de trabajo.

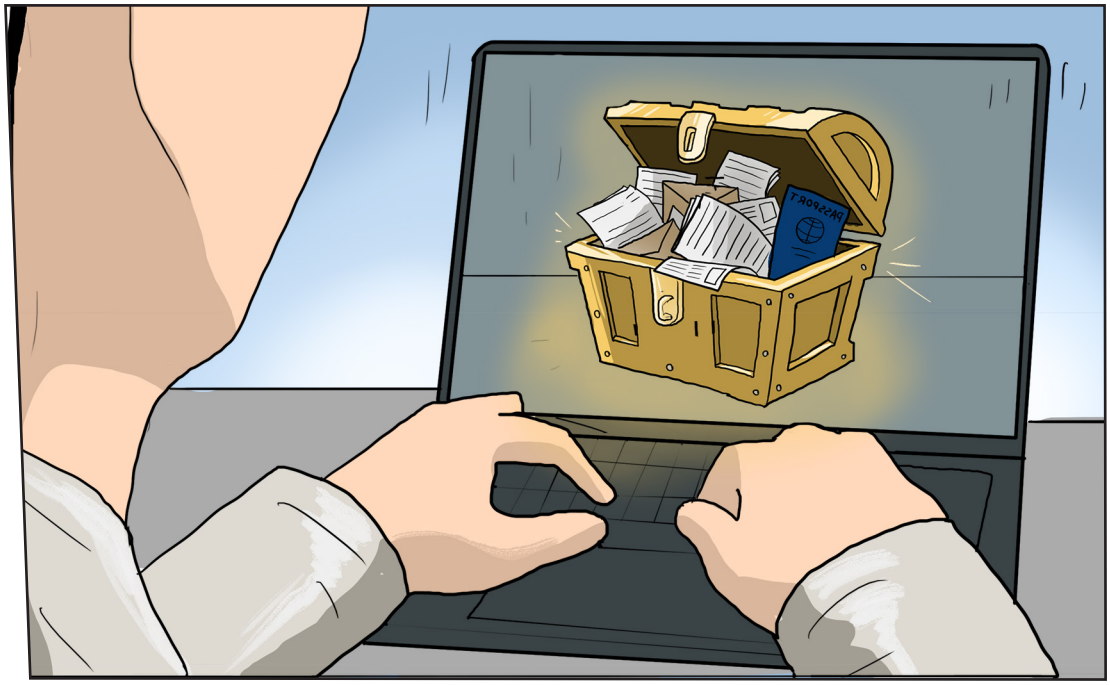
Tobias se siente confuso por la noticia, por lo que intenta confirmar la veracidad de los rumores y, en su caso, advertir a sus compañeros. Como cree saber dónde guardan los documentos financieros los altos cargos, comienza a buscar en secreto cualquier indicio que pueda estar relacionado con los nuevos planes.

Cada año, las organizaciones crean y almacenan más información. Dado que muchas de ellas también operan con modelos híbridos, esta información está repartida en un número cada vez mayor de ubicaciones, tanto físicas como virtuales. Como consecuencia, es habitual que las organizaciones se enfrenten a los problemas con estrategias de almacenamiento poco sistemáticas, en las que los empleados utilizan archivadores o servicios personales de almacenamiento en la nube, como Dropbox, para guardar los datos de la empresa. Además, los empleados suelen tratar información confidencial, como contratos, datos bancarios del personal y resultados financieros de la empresa. Incluso con datos tan importantes como estos, es casi imposible que los equipos de TI garanticen una gestión de la información acorde con las prácticas recomendadas si los documentos se almacenan de esta manera.

ARMAS SECRETAS

Therefore Online
Gracias a su sólida seguridad integrada, Therefore Online permite a las organizaciones establecer políticas automatizadas sobre quién puede acceder a los documentos y cómo se almacena, comparte o edita la información. Los controles de acceso impiden que empleados no autorizados, como Tobias, abran documentos privados o confidenciales como el comunicado de prensa.

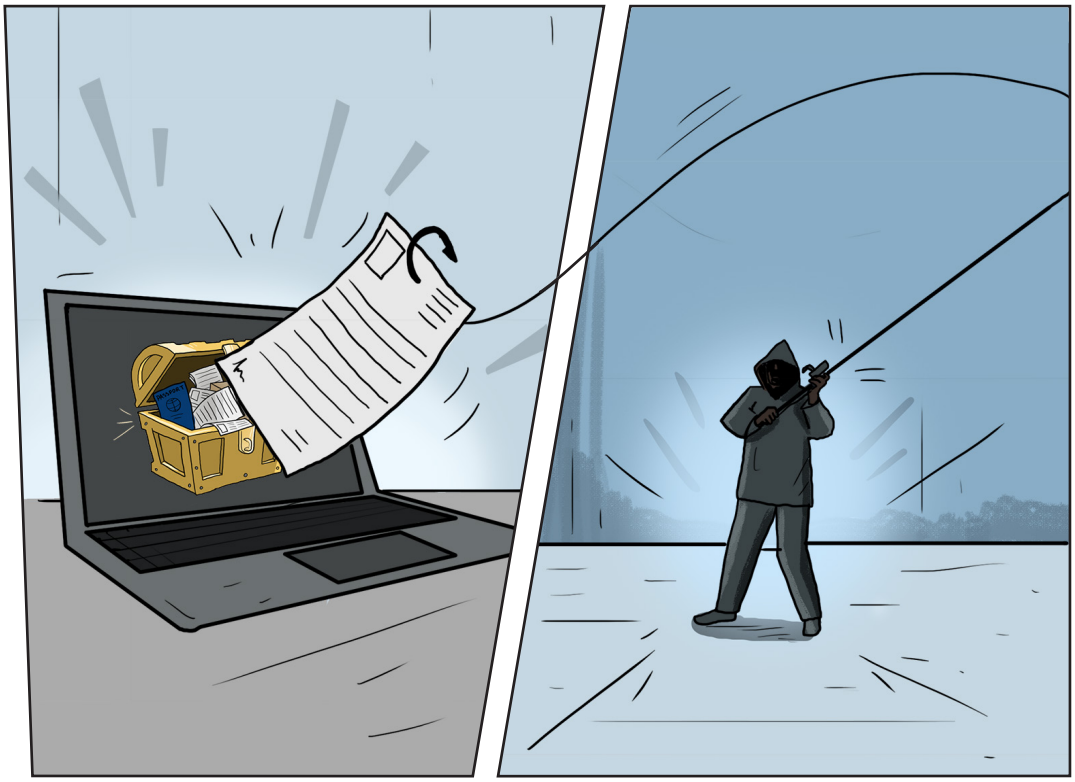
Therefore Online está basado en la nube, lo que garantiza que la ubicación de un usuario no afecte a la accesibilidad, es decir, los usuarios autorizados que trabajan desde casa o se encuentran de viaje pueden seguir accediendo a los documentos esenciales. Se realiza un seguimiento de cualquier interacción con un documento, lo que garantiza que la información se gestiona de forma precisa y es visible de manera integral, y proporciona un registro de auditoría digital.



Pierre se está preparando para enviar el anuncio secreto a los destinatarios, incluidos los principales interesados y los periodistas seleccionados. Es esencial que el documento solo se envíe a estos contactos; Pierre no puede arriesgarse a que la información acabe en las manos equivocadas.

Además, debe tener cuidado con otra información que la organización X mantiene en secreto. La base de datos de la empresa contiene innumerables detalles que no deben revelarse, por ejemplo, datos sensibles sobre los destinatarios, como sus direcciones de correo electrónico, números de teléfono y, en el caso de los periodistas, los datos de sus documentos de identidad de anteriores viajes de prensa.

Esta información es un potencial punto de acceso para los ladrones de datos, que podrían utilizar estas credenciales para filtrar el anuncio antes de tiempo, o utilizar los datos de las personas en la base de datos para realizar robos de identidad u organizar ataques de phishing.

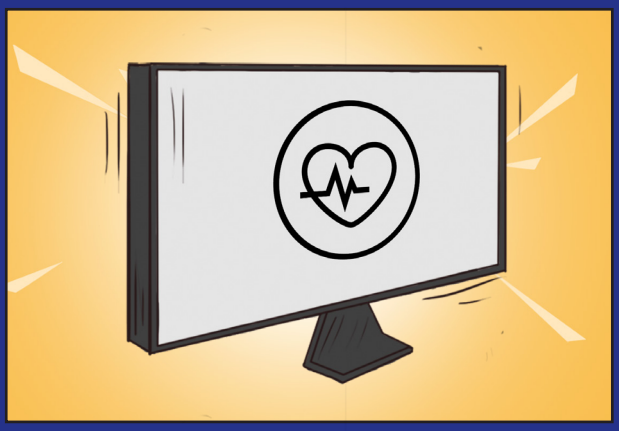


Las empresas suelen guardar información personal altamente confidencial de sus clientes, socios y otros interesados con los que trabajan. Esta información no solo se encuentra en los servidores de la empresa, sino que se incluye en las comunicaciones salientes, como los extractos bancarios, las facturas y la correspondencia con terceros.

La posesión de esta información representa un riesgo para la empresa, ya que si los atacantes la borraran o la robaran, la empresa se enfrentaría a significativas multas y daños a su reputación. Por otra parte, si una organización mantiene conversaciones con estos contactos, es fundamental que la información personal contenida en esas comunicaciones solo llegue al destinatario.

ARMAS SECRETAS

Comprobación del estado de la oficina
Con Office Health Check, las organizaciones pueden revisar su entorno informático para garantizar su seguridad desde el primer momento. El experto en ciberseguridad global NCC Group llevará a cabo un análisis remoto de la infraestructura informática interna y externa de la organización, incluidos los canales y los puertos de comunicación, para revelar cualquier vulnerabilidad. Al identificar los posibles problemas, la organización puede evitar que un atacante potencial se aproveche de ellos, impidiendo la interceptación de las comunicaciones de Pierre o el robo de los datos de los periodistas u otros contactos de sus bases de datos.



uniFLOW sysHUB
uniFLOW sysHUB ofrece a los usuarios un control y una supervisión estrictos de las comunicaciones con los clientes. Con este software, Pierre puede garantizar que la comunicación llega al destino correcto. Esta solución consolida los procesos y aplicaciones de comunicaciones internas en un solo flujo de trabajo, gestionado desde un único punto operativo. A continuación, uniFLOW sysHUB automatiza este flujo de trabajo para hacerlo más eficiente y reducir el riesgo de error. Cada paso del flujo de trabajo se registra y se almacena en una biblioteca de sysHUB para su posterior revisión y para mantener los registros de auditoría, lo que dificulta que un empleado filtre deliberadamente un documento sin que quede registrado. A su vez, Pierre puede revisar el comprobante de entrega para asegurarse de que la comunicación ha llegado a la persona correcta.

DESAFÍO 2

LA CONTRATACIÓN CONFIDENCIAL

La organización Y quiere atraer a nuevos trabajadores para seguir creciendo. La plantilla solía estar en una única ubicación, pero gracias al modelo de trabajo híbrido, sus empleados trabajan desde diversos puntos geográficos. El equipo de RR. HH. ha tenido que adaptarse rápidamente. Ahora, los nuevos empleados se incorporan a través de procesos de contratación e iniciación virtuales. El equipo de RR. HH. debe tenerlo todo bajo control y comunicarse a distancia para compartir documentos confidenciales relacionados con las nuevas incorporaciones.

Un gran poder conlleva una gran responsabilidad: el equipo de RR. HH. posee una gran cantidad de información valiosa y confidencial, como los datos de la nómina de los empleados, información sobre su estado de salud o los registros de rendimiento. Saben que son responsables de mantener tal información segura y en consonancia con la legislación de cumplimiento. En última instancia, el equipo de RR. HH. está sujeto al control de los auditores y sabe que se espera que justifique cómo se almacena y se comparte la información. Esta labor no es nada fácil. Por mucho que el equipo de RR. HH. trabaje duro, no puede hacer magia. Es fácil que los accidentes y los errores lleven al equipo a tener problemas.

Sin las soluciones tecnológicas adecuadas para salvar la situación, esto podría suponer un problema para la organización Y.

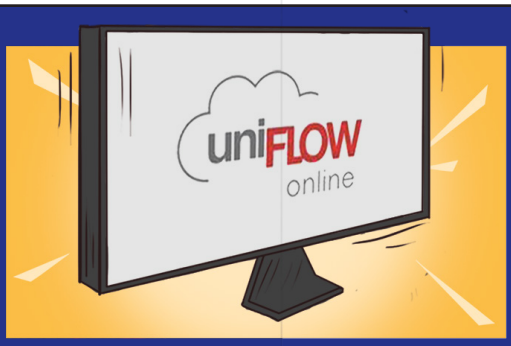
Tras un proceso de entrevistas satisfactorio, la organización Y va a contratar a un nuevo empleado. El candidato ha visitado la oficina central para entregar su documento de identidad y firmar el contrato con Fátima, la responsable de contrataciones. Fátima quiere hacer copias de los documentos para sus propios registros y compartirlos con el responsable de RR. HH., quien trabaja desde casa. En este caso, es fácil que Fátima se equivoque de destinatario o que guarde los documentos en un lugar al que pueda acceder cualquier persona. Si la persona equivocada recibiera estos documentos, podría tener acceso a la información con solo abrirlos.

Las organizaciones tienen la responsabilidad de garantizar que los documentos escaneados solo los vean las personas autorizadas a ello. Un simple error podría dar lugar a una posible pérdida o filtración de datos, lo que podría afectar negativamente al cumplimiento de la normativa.

Si la organización no se da cuenta de que ha sufrido una filtración grave y no lo comunica, el organismo regulador de la protección de datos puede imponer una multa de hasta el 4 % de la facturación global de la organización.

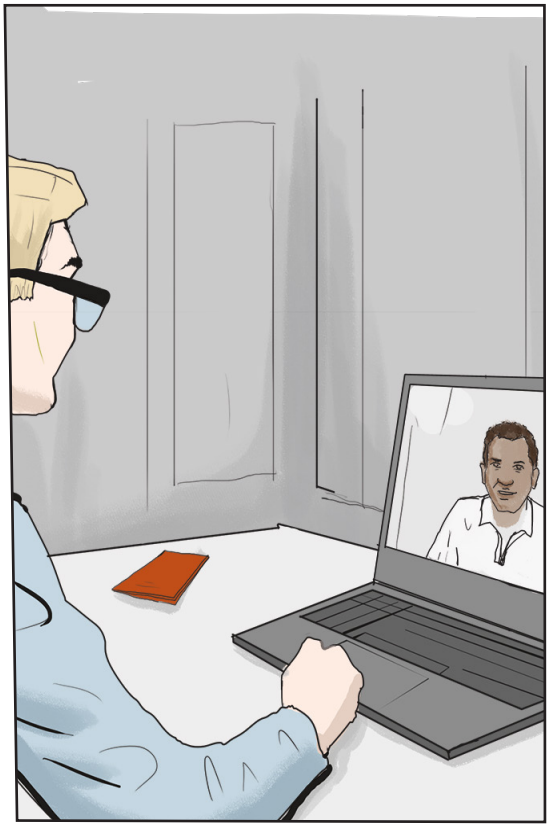
ARMAS SECRETAS

uniFLOW Online
uniFLOW Online ofrece flujos de escaneado seguros que permiten a la organización Y preconfigurar flujos de trabajo de escaneado específicos para cada usuario. Los flujos de trabajo de documentos, como la incorporación de RR. HH., ya están predefinidos, lo que impide que Fátima guarde los documentos escaneados de un nuevo empleado en un destino incorrecto.



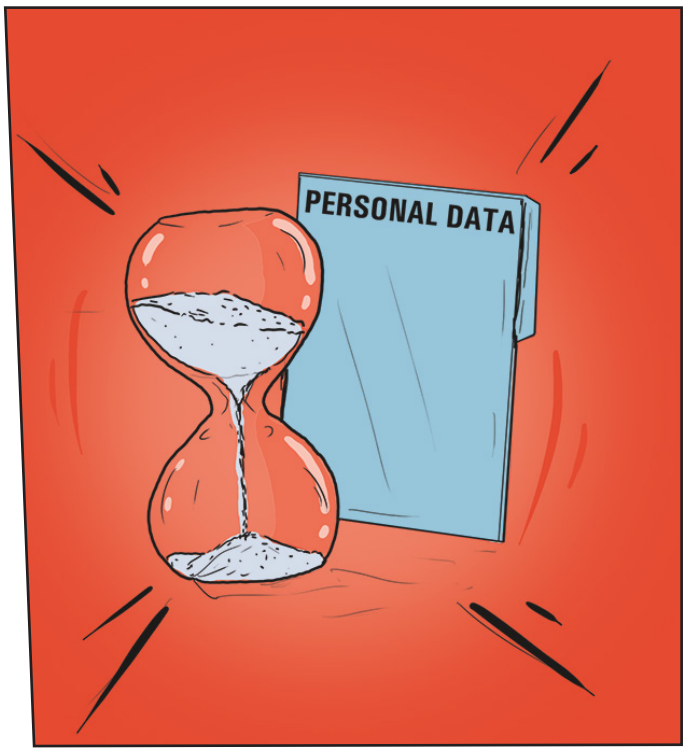
imageFORMULA DR-S150
Fátima va a escanear el documento con el escáner imageFORMULA DR-S150. Este escáner ofrece funciones seguras que ayudan a proteger la información: es necesario que los usuarios inicien sesión con una tarjeta de identificación, lo que garantiza que solo Fátima pueda acceder al documento que se ha escaneado. También aplica automáticamente el cifrado a la versión digitalizada, lo que significa que solo un destinatario con una contraseña puede abrirla, editarla e imprimirla. Los dispositivos imageFORMULA DR-S150 también ofrecen opciones para enviar documentos a través de protocolos seguros como FTPS, SFTP y SMTPS.

IRISPowerscan
La empresa también cuenta con IRISPowerscan, lo que significa que, una vez digitalizados los documentos, se identifican automáticamente como documento de identidad y contrato. El software corrige cualquier fallo de escaneado, como las inclinaciones, y utiliza el reconocimiento óptico de caracteres para identificar datos clave como el nombre del empleado y el número de documento de identidad. Esta información se añade a la indexación, lo que facilita a la organización su búsqueda en el futuro. Además, IRISPowerscan dirige automáticamente los escaneos de contratos y documentos de identidad a la ubicación de almacenamiento segura adecuada en el sistema de la empresa.



Durante el proceso de contratación, varios empleados, incluidos Fátima y su compañero Nick, participaron en la entrevista de los candidatos y la revisión de los CV. Los dos empleados trabajan de forma virtual desde diferentes lugares de Europa. Tanto Fátima como Nick tienen copias de los CV de los candidatos y notas sobre las entrevistas guardadas en sus ordenadores portátiles personales y en ubicaciones compartidas de Dropbox. Una vez que el nuevo candidato ha recibido la oferta de trabajo, es fácil que Fátima y Nick se olviden de eliminar cualquiera de estos documentos.

El reciente endurecimiento de la legislación ha supuesto que el cumplimiento tenga una importancia máxima. Leyes como el RGPD han introducido reglas específicas sobre cómo se debe almacenar la información; por ejemplo, las organizaciones no deben conservar la información de identificación personal durante más tiempo del estrictamente necesario. Sin embargo, muchas organizaciones siguen teniendo dificultades con las estrategias de almacenamiento poco sistemáticas, ya que no cuentan con ubicaciones oficiales para guardar los documentos ni pueden localizar los documentos guardados en sus propios servidores.
Si un antiguo empleado, o incluso un antiguo candidato, presenta una solicitud de acceso a la organización, sería muy difícil para la empresa señalar qué información posee. Además, a efectos de auditoría, la organización tendría dificultades para demostrar que tiene control sobre el lugar en el que se almacena la información de identificación personal.

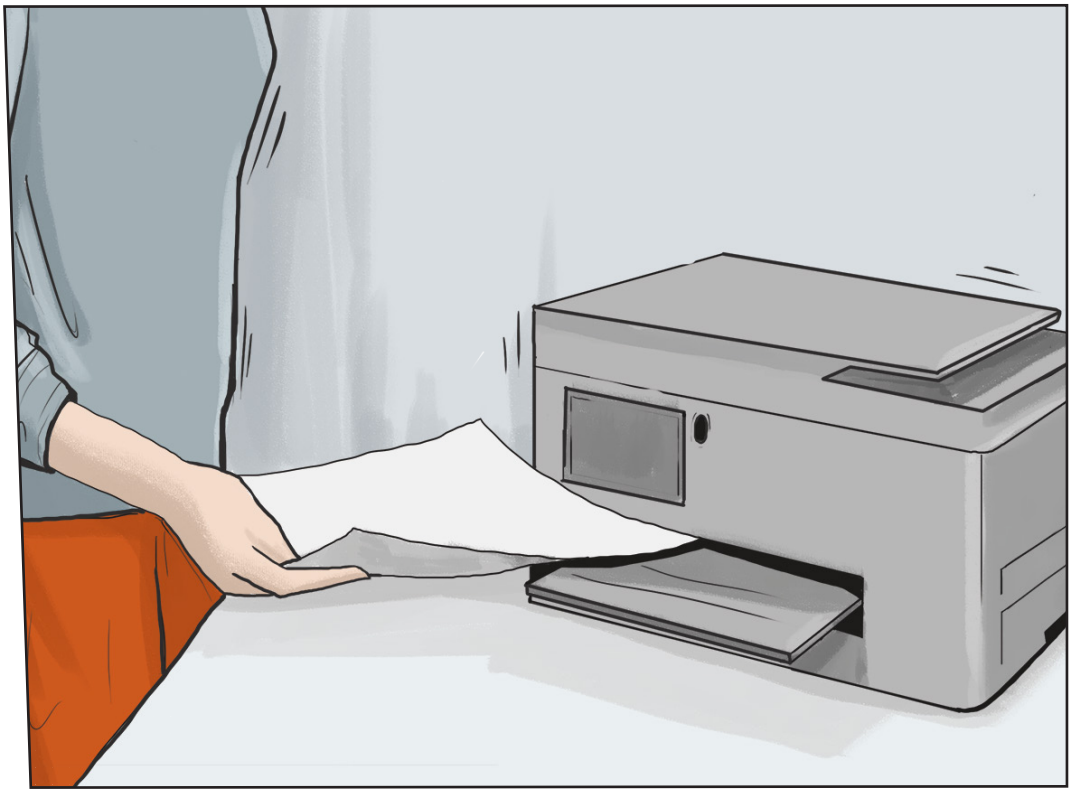


ARMAS SECRETAS

Therefore Online
Gracias a la sólida seguridad integrada, Therefore Online permite a las organizaciones establecer políticas automatizadas sobre quién puede acceder a los documentos y cómo se almacena, comparte o edita la información. Hace un seguimiento de todas las interacciones que se producen con un documento, manteniendo la información bien gestionada y visible de manera integral, lo que hace que el proceso de auditoría sea mucho más sencillo.

La organización Y también puede establecer políticas de retención automáticas para garantizar que los documentos antiguos que contienen información confidencial se eliminan después de un periodo de retención adecuado, cumpliendo así con la normativa. Como Therefore Online está basado en la nube, los equipos pueden seguir cargando documentos cuando se encuentran fuera de las instalaciones y tener la seguridad de que están protegidos.

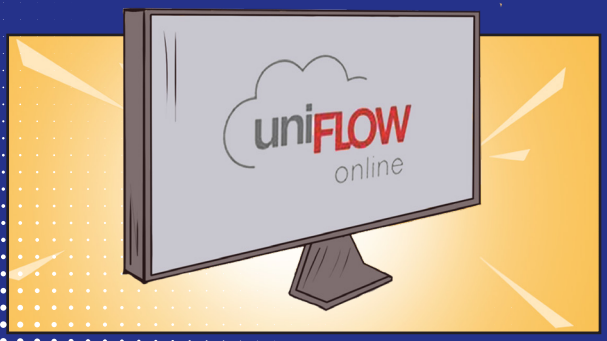
Ingrid, la nueva responsable directa del empleado, trabaja desde casa y se prepara para realizar una entrevista inicial en la oficina al día siguiente. Quiere imprimir una copia de la carta de confirmación del salario del nuevo empleado, junto con otros formularios, para compartirla con él durante ese proceso. Ingrid acaba de empezar a trabajar desde casa y no le han proporcionado una impresora de trabajo, así que utiliza un dispositivo personal.



Es fácil que las organizaciones olviden que las impresoras desempeñan un papel importante en la seguridad y el cumplimiento normativo de los flujos de trabajo, ya que los dispositivos contienen datos y documentos valiosos. Como parte de las obligaciones de cumplimiento legal, se espera que las organizaciones proporcionen registros de auditoría que informen sobre el uso de la información confidencial. Esto requiere que tengan una mayor visibilidad y control de cómo interactúan los documentos con los dispositivos. Sin embargo, como Ingrid utiliza su impresora personal, esta no está conectada a la red de la empresa: no se puede rastrear, no se registran los datos almacenados en el dispositivo ni hay garantías de que la impresora sea segura.

ARMAS SECRETAS

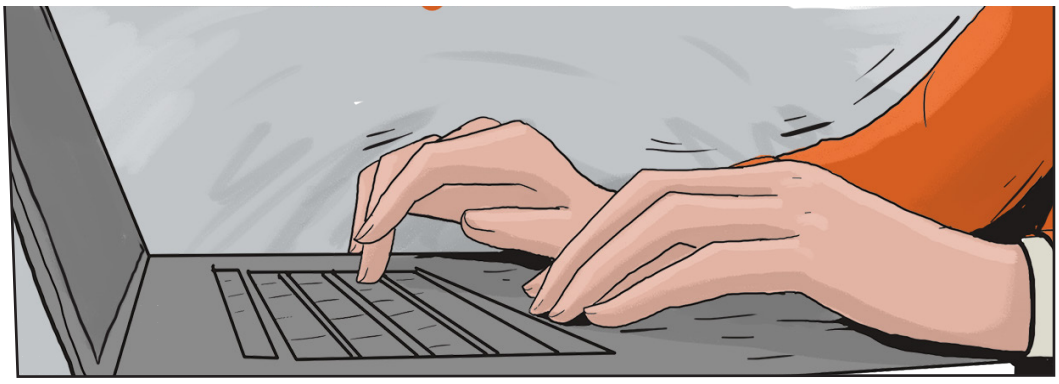
MAXIFY GX6050
Esta eficiente impresora de sobremesa imprime documentos de alta calidad para quienes trabajan desde casa, al tiempo que ayuda a mantener la seguridad y el cumplimiento de la normativa de los documentos gracias a su integración con uniFLOW Online. La función Escaneo a mí mismo impide que Ingrid envíe documentos a otras personas, ya que solo puede enviar los documentos a su correo electrónico o una carpeta personal, para evitar que envíe accidentalmente documentos de la empresa a contactos personales. La función de impresión segura permite que Ingrid solo imprima los documentos cuando esté preparada, lo que significa que los documentos empresariales confidenciales no se quedan en el dispositivo.



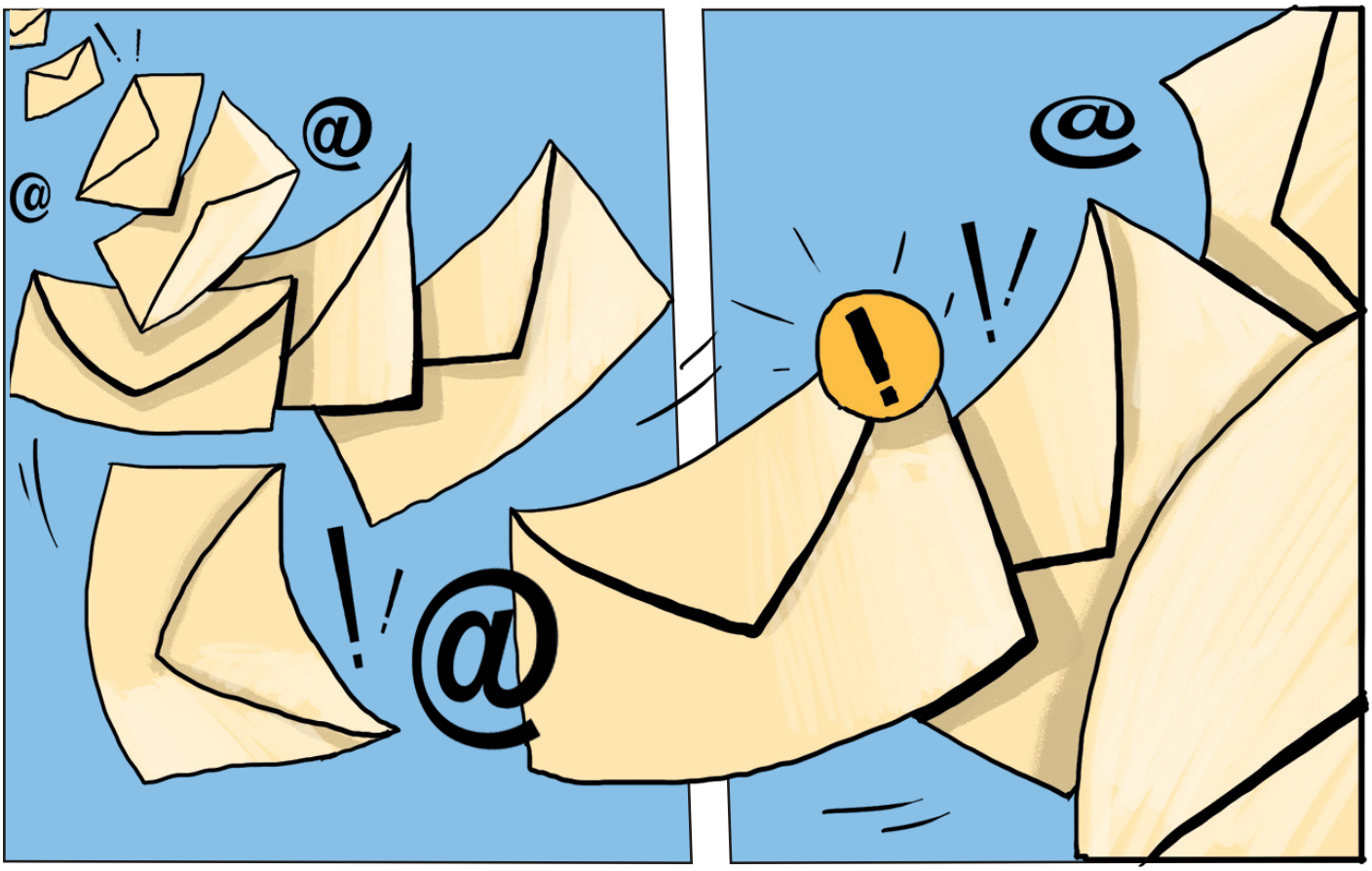
uniFLOW Online
Este software integrado en el dispositivo MAXIFY GX6050 se adapta al entorno de la organización, lo que permite al equipo de TI de la organización Y realizar un seguimiento de la actividad de impresión de Ingrid e informar con precisión sobre el uso de la información confidencial, incluso cuando trabaja desde casa.

Llega final de mes para el nuevo empleado, y Fátima de RR. HH. está preparando su nómina. Casualmente el nuevo empleado se llama igual que otro que lleva más tiempo en plantilla. Fátima envía accidentalmente la nómina al destinatario equivocado, lo que significa que ambos pueden ver cuánto se paga a la otra persona.

La organización ha violado la confidencialidad de los empleados quienes técnicamente tienen motivos para llevar a la empresa a un tribunal laboral. Además, tras haber visto la nómina de su compañero, el nuevo empleado quiere discutir su salario con Recursos humanos y puede que ya no se sienta cómodo en su puesto.



La comunicación es una etapa de alto riesgo de cualquier flujo de trabajo documental, ya que implica compartir información, ya sea de manera interna con los empleados o externa con los clientes, proveedores y otras partes interesadas. En un proceso de auditoría estándar, se espera que las organizaciones justifiquen cómo se comparte la información confidencial con otras partes. Dado el elevado volumen de comunicaciones que una organización lleva a cabo en una semana determinada, es esencial contar con soluciones que faciliten el seguimiento y la localización de estos procesos.



ARMAS SECRETAS

uniFLOW sysHUB
uniFLOW sysHUB ofrece a los usuarios un control y una supervisión estrictos de sus comunicaciones internas, lo que permite a Fátima mantener la confidencialidad de las comunicaciones de RR. HH. La solución consolida los procesos y aplicaciones de comunicaciones internas en un solo flujo de trabajo, gestionado desde un único punto operativo. uniFLOW sysHUB automatiza este flujo de trabajo para hacerlo más eficiente y reducir el riesgo de error. En este ejemplo, Fátima no habría enviado por error información confidencial a otro empleado.

Cada paso del flujo de trabajo se registra y se almacena en una biblioteca de sysHUB para su posterior revisión y para mantener los registros de auditoría, lo que significa que Fátima puede revisar el comprobante de entrega para asegurarse de que la comunicación ha llegado a la persona correcta.

¿CÓMO PODEMOS AYUDAR?

Todas las empresas desean mantener su información protegida y cumplir con la normativa. No obstante, como han demostrado las organizaciones X e Y, esta labor es muy difícil. Las organizaciones se enfrentan cada vez a más ataques, y una legislación más estricta implica que las empresas tienen mucho que perder si se cometen errores. Puede parecer una batalla perdida, pero no tiene por qué serlo. El secreto está en contar con la tecnología y el socio adecuados.

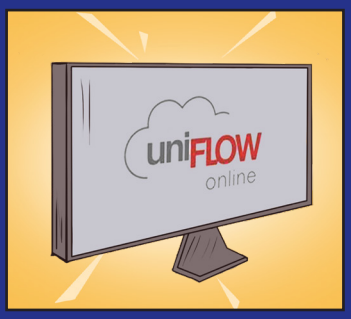
Canon es líder en IDC MarketScape en soluciones y servicios de seguridad de impresión y documentos, así como en el panorama de seguridad de impresión de Quocirca. El hardware, el software y los servicios que ofrecemos se han diseñado para ayudar a tu organización a funcionar de la forma más eficiente y eficaz en un mundo complejo. Independientemente del lugar en el que tus empleados trabajen o del punto del proceso de transformación digital en el que te encuentres, nuestra tecnología se adapta a todos los entornos de trabajo.

Nos encargamos de mantener la información protegida con nuestro enfoque de seguridad por diseño. Nuestras soluciones están diseñadas para prevenir ataques, proteger los datos y mantener y salvaguardar el cumplimiento de la normativa, para que puedas aprovechar las nuevas capacidades sin que ello suponga un mayor trabajo para tu equipo.

DISPOSITIVOS DE IMPRESIÓN Y ESCANEO

Nuestra gama de impresión y escaneo está equipada con las últimas características de seguridad para proteger los datos importantes en cada fase del flujo de trabajo de los documentos. Todos los productos de Canon se someten a comprobaciones de seguridad en las fases de diseño y desarrollo antes de su lanzamiento.

Seguimos estableciendo sólidas colaboraciones con empresas líderes del sector, como Trellix y Microsoft, para garantizar la mayor cobertura y compatibilidad posibles a la hora de proteger las flotas de dispositivos. Además, contamos con un equipo de respuesta a incidentes de seguridad de los productos.



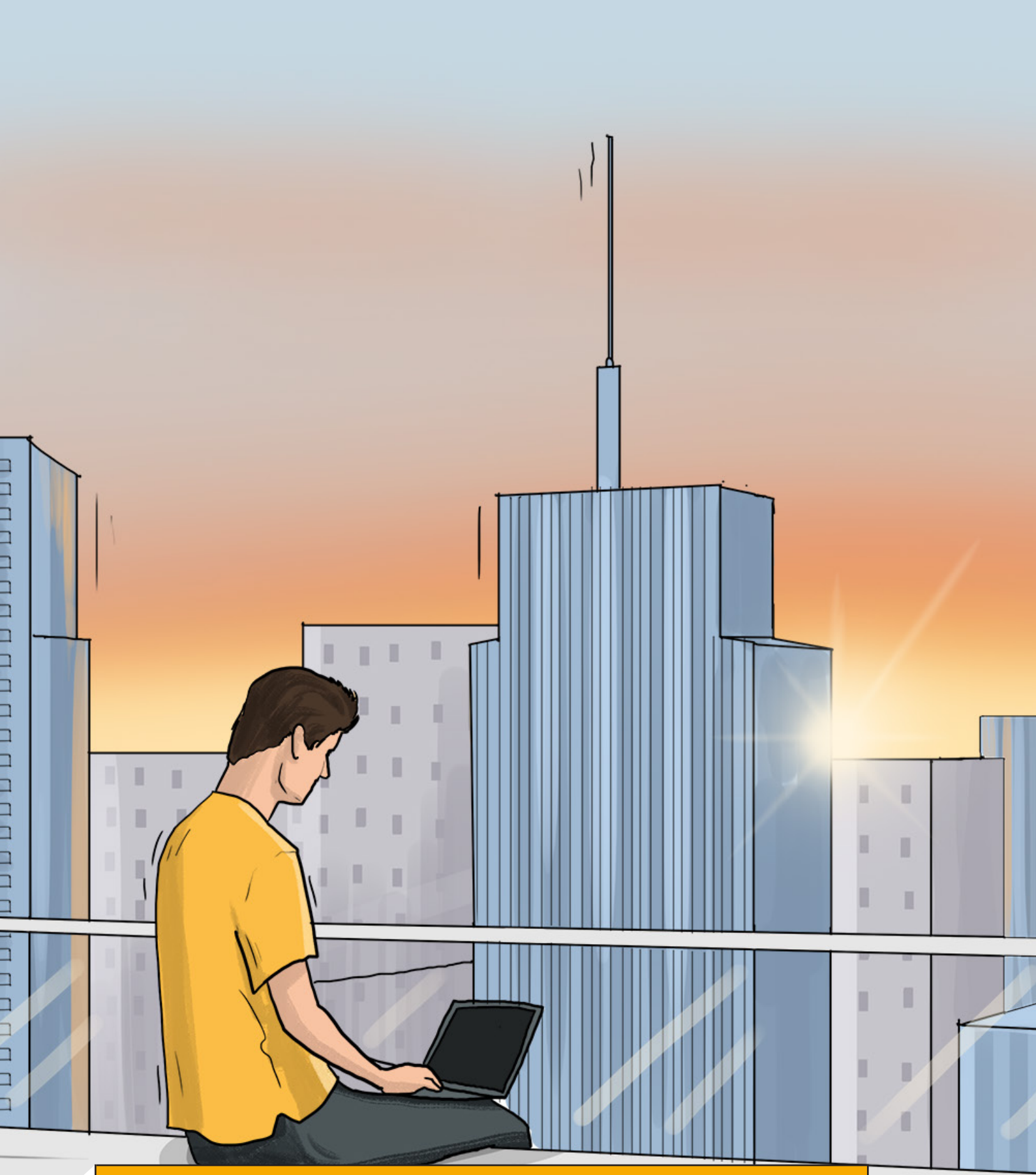
SOFTWARE

Entendemos que la información no está limitada por la ubicación, por lo que ofrecemos software que protege los datos dondequiera que se encuentren. También trabajamos con organizaciones externas como IOActive para realizar pruebas de penetración (pentest) en la fase de lanzamiento y para las principales actualizaciones de software.

SERVICIOS

Ofrecemos servicios de seguridad diseñados para ayudarte a respetar el cumplimiento de la normativa de protección de datos y a salvaguardar la información confidencial durante toda su vida útil en tu infraestructura de impresión y escaneo.


PASSPORT



¿Quieres acabar con los problemas de seguridad y cumplimiento? Ven a ver nuestras tecnologías en acción en nuestro centro de exposiciones o reserva una demostración con nuestro equipo de expertos para comprobar lo que pueden hacer nuestras soluciones por tu empresa.

¿Quieres obtener más información sobre nuestras armas secretas? Visita nuestra página web Digital Transformation Services para descubrirlas.

ACERCA DE CANON

Canon es imagen. Utilizamos esa imagen para marcar la diferencia y habilitar el cambio. Para nuestros clientes mientras emprenden la transformación digital y trabajan de nuevas formas. Para un cambio social más amplio con nuestro objetivo continuo de sostenibilidad como parte del legado y la cultura de nuestra corporación.

Por último, estamos cambiando con la inversión en nuevos mercados, productos y tecnologías, por lo que estaremos aquí mucho tiempo para beneficio de todos; nuestros clientes, nuestros empleados y la sociedad en general.

CANON SE BASA EN 4 PILARES FUNDAMENTALES:

Innovación

Un largo historial de innovación en imagen, ofreciendo tecnología de vanguardia desde hace más de 80 años. Pioneros en el sector y con un sólido compromiso con futuros desarrollos en tecnología.

Asistencia

Una amplia cartera de servicios para garantizar la máxima calidad, que redunda en la satisfacción de los clientes. Experiencia interna trabajando para mejorar la eficiencia y compromiso con liberar el potencial de nuestros clientes.

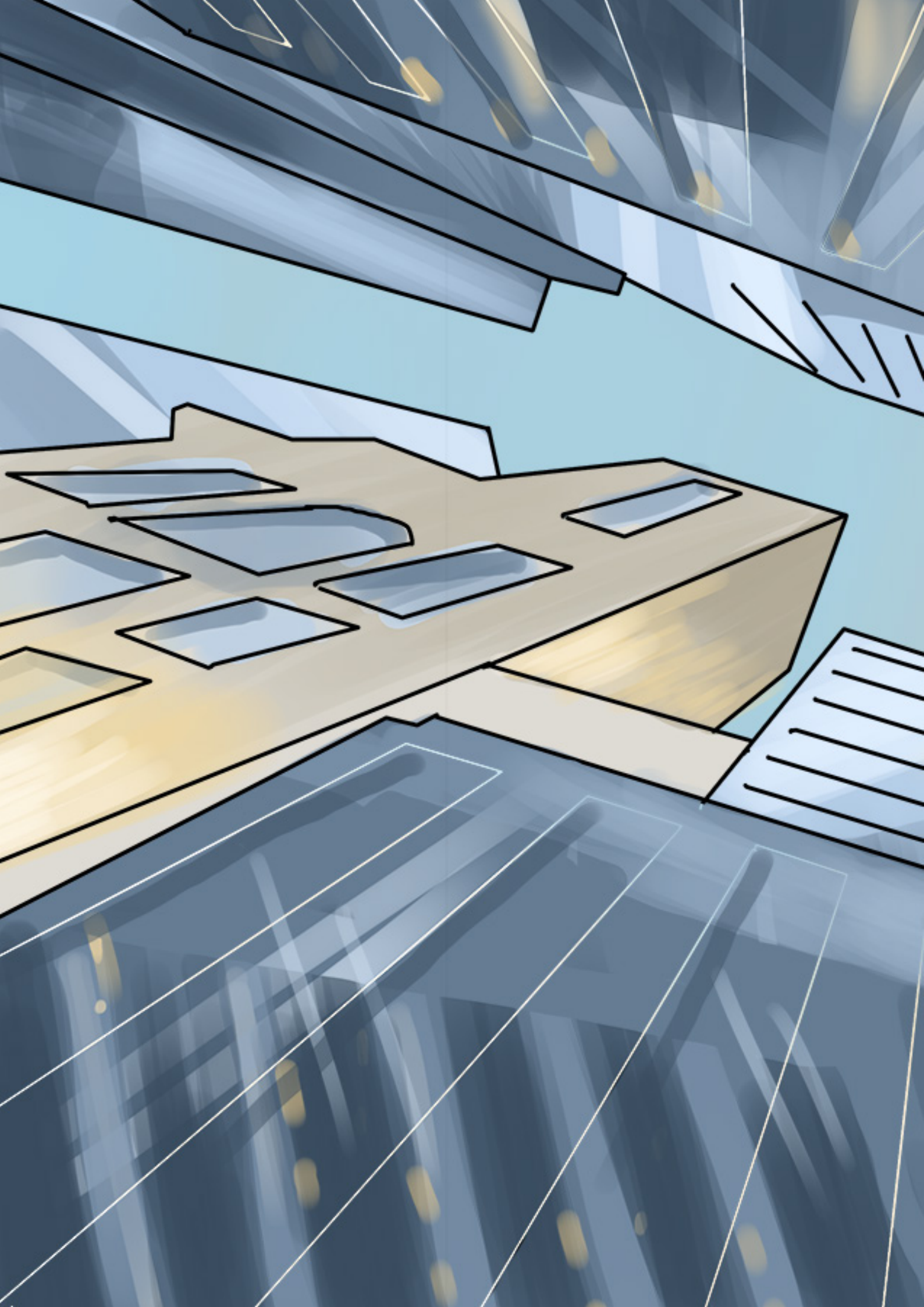
Seguridad

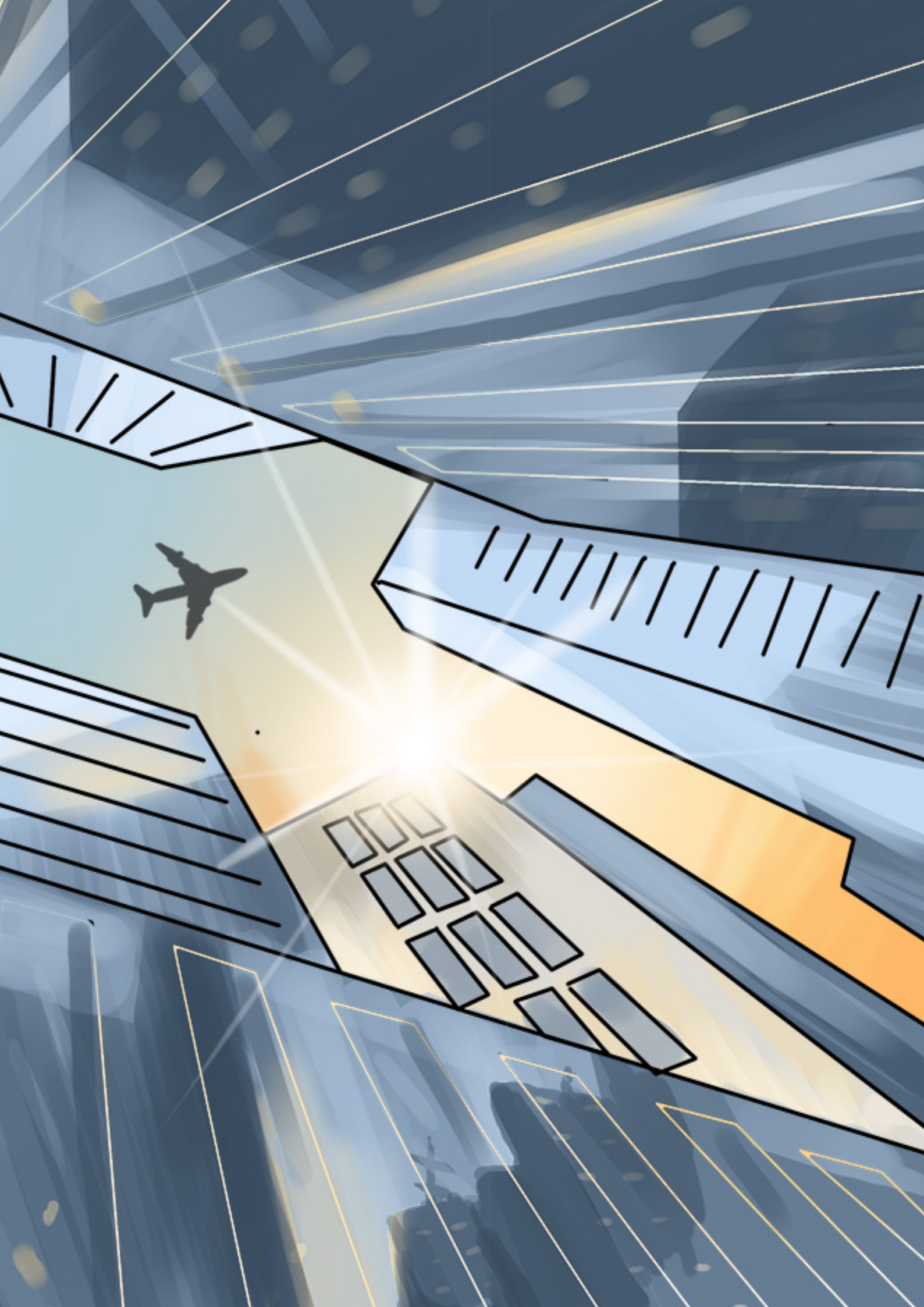
Las soluciones y los servicios de Canon ayudan a proteger todos los documentos y datos confidenciales, ya sea en papel o en formato digital, a lo largo del ciclo de vida de los documentos. Los dispositivos, las soluciones y los servicios, seguros por diseño, se crean pensando en la seguridad.

Sostenibilidad

Canon ha alineado sus prácticas de sostenibilidad con los Objetivos de Desarrollo Sostenible (ODS) de la ONU, como el compromiso con reducir las emisiones de CO_2 a lo largo del ciclo de vida de los productos mediante la reducción del tamaño de los paquetes y la consolidación de los centros de distribución.

TODOS ESTOS ELEMENTOS COMBINADOS HACEN DE CANON EL SOCIO ADECUADO PARA TI.





Canon Inc.
Canon.com

Canon Europe
canon.es
Spanish edition

Canon España, S.A.
Avda. de Europa, 6
28108 Alcobendas (Madrid)
Tel.: 91 538 45 00
Fax: 91 564 01 17
canon.es