olivetti

Preparados para el RGPD

INTRODUCCIÓN

MUCHOS ASPECTOS IMPLICADOS EN LA SEGURIDAD DE DATOS ESTÁN SOPORTADOS POR LOS EQUIPOS MULTIFUNCIONALES Y LAS SOLUCIONES DOCUMENTALES Y DE FLUJOS DE TRABAJO. EN ESTE DOCUMENTO IDENTIFICAREMOS ALGUNAS DE ESTAS ÁREAS PARA AYUDAR AL LECTOR A REALIZAR SUS PROPIAS EVALUACIONES. UNA INFORMACIÓN MÁS DETALLADA PUEDE OBTENERSE A TRAVÉS DE LOS DISTRIBUIDORES DE OLIVETTI O DEL EQUIPO DE SOPORTE TÉCNICO.

CONTENIDO

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) REEMPLAZA LA ANTERIOR DIRECTIVA DE PROTECCIÓN DE DATOS 95/46/EC Y HA SIDO DISEÑADO PARA ARMONIZAR LAS DISTINTAS REGULACIONES LOCALES DE LOS DISTINTOS PAÍSES EUROPEOS, PARA PROTEGER Y EMPODERAR LA PRIVACIDAD DE LOS DATOS DE LOS CIUDADANOS EUROPEOS

¿Qué es el RGPD?

El Reglamento General de Protección de Datos (RGPD) es una legislación vinculante que entra en vigor a partir del 25 de mayo de 2018, emitido por la Unión Europea para mejorar la protección de datos personales en toda Europa.
El nuevo reglamento unifica y amplía la protección de datos hasta la fecha regulada por reglamentos locales.

El anterior marco legal ha demostrado en los últimos años su incapacidad, y el nuevo marco legislativo persigue hacer responsables, en caso de incumplimiento del Reglamento, a todos aquellos que almacenan o gestionan datos personales, siendo su responsabilidad la salvaguarda de los mismos.

Resumen

¿CUÁNDO ARRANCA EL NUEVO REGLAMENTO?

25 de Mayo de 2018

¿QUIÉN DEBE HACER CUMPLIRLO EN CADA PAÍS?

Las autoridades nacionales de supervisión.

¿QUÉ APORTA DE NUEVO?

Hay nuevos derechos para los ciudadanos para el acceso a la información que tienen las compañías acerca de ellos, reglas para una mejor gestión en las empresas, y un nuevo regimen de multas severas. gestión

DURAS SANCIONES

Las regulaciones tendrán fuertes sanciones para aquellos que no cumplam. Se pueden aplicar multas de hasta 20 millones de € o el 4% del volumen de negocio global de una empresa (el que sea mayor), lo que no solo es financieramente devastador, sino que acarrea un estigma de daño a largo plazo a la reputación de la compañía

"Vivimos en un mundo en el que los ciberataques son actualidad." *- Business Reporter - The Telegraph*

¿Porqué es necesario el RGPD?

En el marco legal anterior, cada Estado Miembro de la UE tenía su propia política de Protección de Datos.

Las anteriores regulaciones no tenían en cuenta el grado de evolución tecnológica, haciendo que algunas de ellas quedara completamente obsoleta. Por tanto, el RGPD pretende unificar a todos los Estados miembros bajo un solo conjunto de regulaciones y ha sido diseñado para ser "a prueba de futuro" para permitir cambios rápidos adicionales en tecnología y cualquier avance empresarial por parte de empresas en la UE o que usan datos de la UE.

Con los ataques cibernéticos en crecimiento, la protección de datos es vital para las empresas y las personas. Por el momento, es muy difícil para las personas averiguar quién tiene su información y qué están haciendo con ella. El nuevo RGPD velará por esta preocupación.

Con un número de datos que se producen en todo el mundo con tasas exponenciales de crecimiento, y que son utilizados como mercancía comercial por compañías sin escrúpulos, hackers, estafadores, etc., aumenta la inseguridad de todos.

Los incumplimientos de privacidad a menudo son un elemento secundario en la etapa de diseño y de la fabricación del producto, por lo que cada vez hay más informes de vulnerabilidades y reparaciones de seguridad, junto con retiradas de productos.

"Si ha construido castillos en el aire, su trabajo no necesita perderse; ahí es donde debería estar. Ahora ponle cimientos." .

Henry David Thoreau, Escritor (1817-1862)

Mayores derechos para individuos

El Nuevo RGPD incorpora bajo la presente regulación algunos derechos nuevos para las personas y fortalece algunos de los derechos existentes

El RGPD incorpora los siguientes derechos para las personas individuales :

1. Derecho a estar informado
2. Derecho de acceso
3. Derecho a rectificación
4. Derecho al olvido
5. Derecho a restringir su procesamiento
6. Derecho a la portabilidad de los datos
7. Derecho de oposición
8. Derechos en relación con el perfil y la toma de decisiones automatizada

“Una empresa tendrá buena seguridad si su cultura corporativa es correcta. Eso depende de una cosa: la actitud de la dirección“.

William Malik, VP y Research AD para seguridad de la información– Gartner

¿Cuáles son los Principios de la nueva regulación?

¿A quién se aplica RGPD ?

El RGPD se aplica a ‘Controladores’ y ‘Procesadores’ de datos. El Controlador dice cómo y por qué se procesan los datos personales y el Procesador actúa en nombre del controlador.

El RGPD impone obligaciones legales específicas a un Procesador. Por ejemplo, los procesadores están obligados a mantener registros de datos personales y actividades de procesamiento. Tendrán una responsabilidad legal significativamente mayor si son responsables de una infracción. Estas obligaciones para los Procesadores son un nuevo requisito en virtud del RGPD.

Sin embargo, un Controlador no se libera de sus obligaciones cuando hay un Procesador involucrado: el RGPD impone obligaciones adicionales a un Controlador para garantizar que sus contratos con los Procesadores cumplan con el RGPD.

El RGPD se aplica al procesamiento llevado a cabo por organizaciones que operan dentro de la UE. También se aplica a organizaciones fuera de la UE que ofrecen bienes o servicios a personas en la UE.

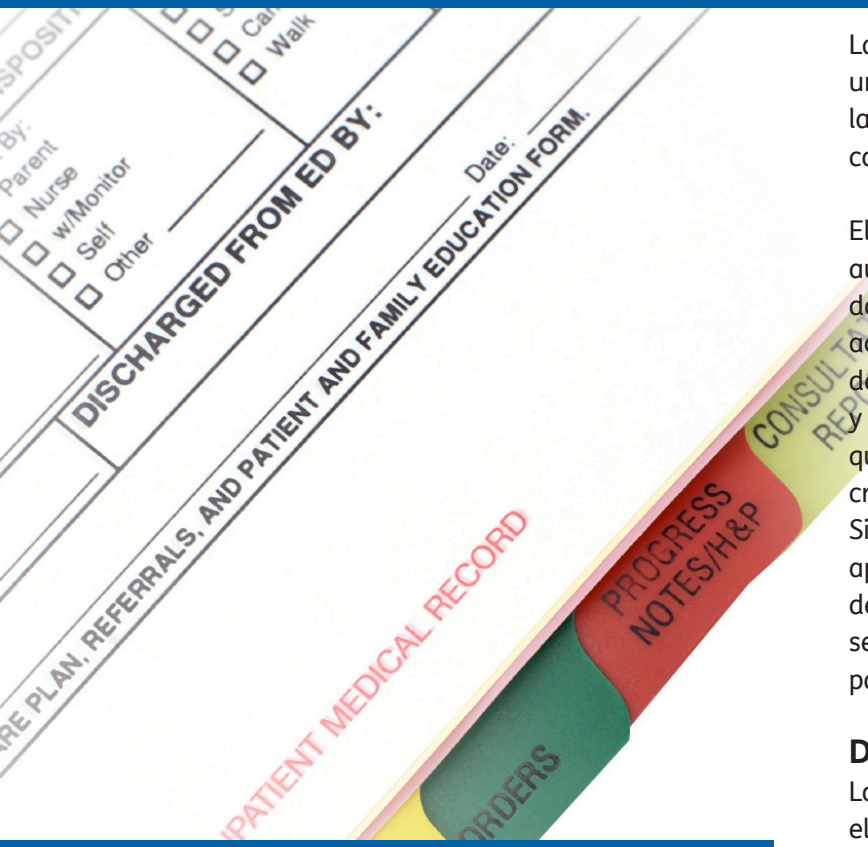
El RGPD no se aplica a ciertas actividades, incluido el procesamiento de datos cubierto por la Directiva de Aplicación de ley, el tratamiento con fines de seguridad nacional y el tratamiento llevado a cabo por personas exclusivamente vinculada a actividades personales o domésticas

¿A qué datos se aplica el RGPD?

Datos Personales

Al igual que la regulación actual, el RGPD se aplica a ‘Datos personales’. Sin embargo, la definición del RGPD es “cualquier información relacionada con una persona física identificada o identificable” y deja claro que incluso la información, como un identificador en línea, como una dirección IP o una información de ubicación puede ser información personal

Bajo la protección del RGPD existe una amplia gama de ‘identificadores personales’ que constituyen datos personales, que reflejan cambios en la tecnología y la forma en que las organizaciones recopilan información sobre las personas



"El mantra de cualquier buen ingeniero de seguridad es:« La seguridad no es un producto, sino un proceso ». Es más que diseñar una criptografía sólida en un sistema: está diseñando todo el sistema de manera que todas las medidas de seguridad, incluida la criptografía, funcionen juntas ".

Bruce Schneier: criptógrafo y especialista en privacidad

La mayoría de las organizaciones deberán hacer una diferenciación entre los datos protegidos por la regulación actual o los que entran dentro de las competencias del RGPD.

El RGPD se aplica tanto a los datos personales automatizados como a los sistemas de archivo manual donde se puede acceder a los datos personales de acuerdo con criterios específicos. Esto va más allá del alcance de la definición de la regulación actual y podría incluir conjuntos de registros manuales que contengan datos personales ordenados cronológicamente.
Si los datos personales han sido codificados con un apodo o seudónimo, entonces pueden estar dentro de los límites del RGPD dependiendo de cuán difícil sea atribuir el apodo o el seudónimo a un individuo en particular.

Datos Personales Sensibles

Los datos personales confidenciales de acuerdo con el RGPD se denominan "categorías especiales de datos personales", e incluyen: datos de origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud o datos relacionados con la vida sexual u orientación sexual de una persona individual.

Estas categorías son similares a la regulación actual pero con la adición de datos genéticos y datos biométricos que se han procesado para identificar a un individuo específico. Los datos personales relacionados con condenas y delitos penales no están incluidos, pero se aplican salvaguardas adicionales a la forma en que se recopilan, manejan y procesan.

El Articulo 5 del RGPD indica que los datos Personales y Sensibles deben ser:

(a) Procesados de manera legal, justa y transparente en relación con las personas individuales.

(b) Recopilados para fines específicos, explícitos y legítimos y no procesados de manera incompatible con esos fines; no se considerará incompatible con los fines iniciales el procesamiento ulterior con fines de archivo con fines de interés público, investigación científica o histórica o fines estadísticos.

(c) Adecuados, relevantes y limitados a lo que es necesario en relación con los fines para los que se procesan.

(d) Precisos y, cuando sea necesario, actualizados; Deben tomarse todas las medidas razonables para garantizar que los datos personales que sean inexactos, teniendo en cuenta los fines para los que se procesan, se borren o rectifiquen sin demora.

(e) Conservados en un formato que permita la identificación de los interesados por un período no superior al necesario para los fines para los que se procesan los datos personales; los datos personales pueden almacenarse durante períodos más largos en la medida en que los datos personales se procesen únicamente con fines de archivo de interés público, investigación científica o histórica o con fines estadísticos sujetos a la implementación de las medidas técnicas y organizativas apropiadas requeridas por el RGPD para salvaguardar los derechos y libertades de las personas.

(f) Procesados de manera que garantice la seguridad adecuada de los datos personales, incluida la protección contra el procesamiento no autorizado o ilegal y contra la pérdida, destrucción o daño accidental, utilizando medidas técnicas u organizativas apropiadas.

Artículo 5(2) indica que "El controlador será responsable y podrá demostrar el cumplimiento de los principios"

“El mayor error que cualquier usuario de hardware puede hacer es ignorar la copia de seguridad de sus datos”.
CyberSmart.org

Tecnología y RGPD

El RGPD consta de 8 principios principales que cubren todos los aspectos de las reglamentaciones. El Séptimo Principio es uno que puede relacionarse con la tecnología involucrada en el manejo y la administración de datos, que involucra impresoras y herramientas de administración de documentos. Establece que “se tomarán medidas técnicas y organizativas apropiadas contra el tratamiento no autorizado o ilegal de datos personales y contra la pérdida o destrucción accidental de, o el daño a, los datos personales”.

En la práctica, significa que las empresas y las personas deben tener la seguridad adecuada para evitar que los datos personales almacenados se pongan en peligro accidental o deliberadamente. En particular, las compañías deberían seguir estas sugerencias:

• **Diseñe y organice su seguridad** para adaptarse a la naturaleza de los datos personales que posee y al daño que pueda resultar de una violación de seguridad.

• **Sea claro sobre quién, en su organización, es responsable** de garantizar la seguridad de la información.

• **Asegúrese de tener la seguridad física y técnica correcta**, respaldada por políticas robustas así como procedimientos y personal de confianza y bien capacitado.

• **Prepárese para responder** a cualquier violación de la seguridad rápida y efectivamente.

Los avances en la tecnología han permitido a las organizaciones procesar cada vez más datos personales y compartir información más fácilmente. Esto tiene beneficios obvios si se recopilan y comparten datos personales de acuerdo con los Principios de Protección de Datos, pero de la misma forma también da lugar a riesgos de seguridad.

Cuantas más bases de datos estén configuradas y más información se intercambie, mayor será el riesgo de que la información se pierda, se corrompa o se use incorrectamente.

En los últimos años, una serie de pérdidas importantes de grandes cantidades de datos personales, han llamado la atención sobre el tema de la seguridad de la información.

Estos incidentes también han dejado en claro que la seguridad de la información es una cuestión de interés público así como de cumplimiento técnico. Si los datos personales no están asegurados adecuadamente, esto puede dañar seriamente la reputación y el futuro de una organización y también puede comprometer la seguridad de las personas.

"Al crear una estrategia para proteger cada nivel de datos de manera específica, las empresas pueden proteger adecuadamente los datos contra las actuales amenazas"
Chuck Davis, Profesor y Arquitecto de Seguridad Senior

Seguridad a través de dispositivos MFP y soluciones documentales

Los dispositivos multifuncionales (MFP), así como las impresoras y los escáneres a menudo no se tienen en cuenta en lo que respecta a la seguridad de los datos. Se conectan a la red de una empresa y permiten a los usuarios escanear el correo electrónico y la nube. Ellos también pueden almacenar un alto número de datos personales, como el correo electrónico y las direcciones IP, y también pueden guardar trabajos en sus memorias sofisticadas para permitir que las personas impriman de forma diferida.

Hay muchas soluciones de software documentales, que enlazan productos MFP con el fin de escanear documentos, que permiten a las empresas integrar flujos de trabajo, correos electrónicos entrantes y faxes para documentar sistemas de administración, bases de datos, servidores corporativos de archivos y aplicaciones de administración de contenido. Es una forma de captura de datos, por lo que, por su propia naturaleza, son responsabilidad de los procesadores de datos y los controladores de datos. Sin embargo, en el caso de algunos productos, como los que en realidad no almacenan datos en ellos, es decir, envían el almacenamiento a otros dispositivos, ya sea la nube u otros dispositivos de almacenamiento digital, no tienen información almacenada, aunque los datos hayan sido procesados en ellos.

¿Qué puedes hacer para comprobar que cumples?

Hay muchas cosas que evaluar. Al establecer el punto de partida para una evaluación completa hay que ser exhaustivo, no dejar piedra sin remover y evitar infracciones de seguridad. En primer lugar, el asesoramiento de fuentes oficiales consiste en utilizar una Lista de verificación y realizar una Evaluación de riesgos sobre las actividades de su empresa relacionadas con la captura, manejo, procesamiento y almacenamiento de datos, y cómo se comparte e imprime la información, qué sucede con los documentos impresos y cómo y dónde son archivados. También es aconsejable poner en marcha una estrategia segura e incluso un plan de contingencia sobre cómo tratar casos de violación - en el improbable caso de que eso suceda-. Una vez implementada la estrategia de acceso directo, es posible asegurarse de que las impresoras, MFP y soluciones de administración de documentos se hayan configurado con los últimos kits de seguridad, estructuras de autenticación e instalaciones de cifrado.

"Nuestros nombres circulan más allá de nuestro control, entre otros que sí obtienen un beneficio ". - El ojo electrónico: El aumento de la sociedad de vigilancia " - *David Lyon*

“La seguridad no solo sucede, sino que es el resultado del consenso colectivo y la inversión pública .”
Nelson Mandela

¿Cómo cumplen nuestros productos con RGPD?

Bajo el 7º Principio del RGPD, las impresoras y MFP’s actuales no deberían ser tratados de manera diferente que cualquier otro periférico de IT conectado a la red, ya que usan discos duros, procesadores y tarjetas de red como los que se encuentran en cualquier PC.

En Olivetti, nuestras impresoras, equipos multifuncionales y software de gestión de documentos se han desarrollado para proteger a los usuarios contra el acceso no autorizado y las fugas de información a través de una red, a través de dispositivos móviles, mediante copia, interferencia o eliminación de información o por fallo del equipo, pérdida o daño accidental por parte de un usuario o acceso a registros de trabajos.

Todos nuestros MFP más recientes logran la Certificación Common Criteria (ISO / IEC 15408) así como el Estándar de Seguridad IEEE 2600.1 ya sea a través de características de seguridad estándar integradas en las máquinas de serie o como resultado de agregar kits de seguridad de datos opcionales. Como se trata de un tema de gran alcance, cubriremos algunos de los aspectos básicos de cómo nuestras máquinas están preparadas para la seguridad.

Para obtener más información, póngase en contacto con nuestro equipo técnico.

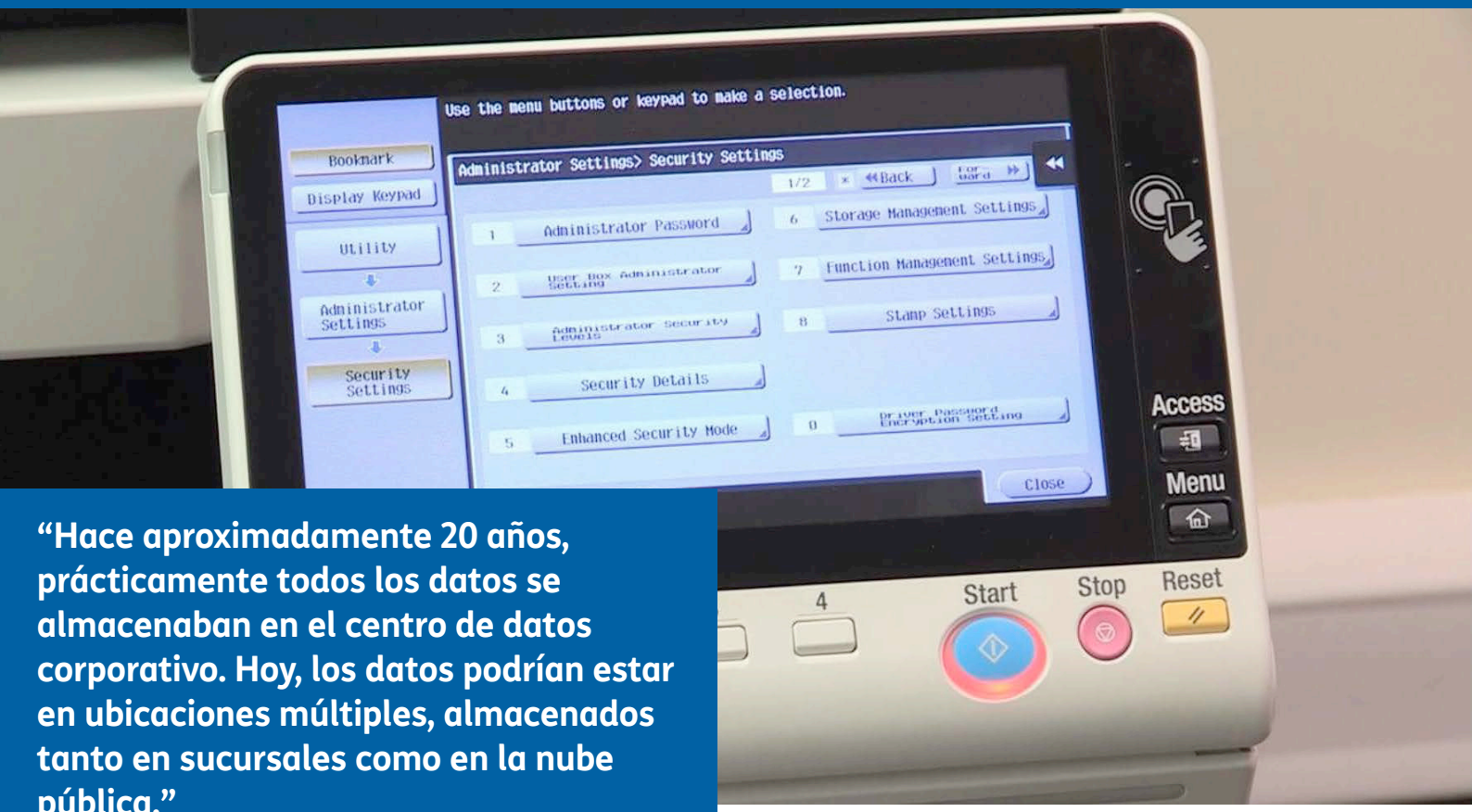
1. Seguridad para procesamiento de imagen y salida

Cuando los datos se escanean a través del escáner de la impresora multifunción, se procesan, comprimen y escriben en la memoria de la impresora multifunción. Para imprimir estos datos, se descomprime y se envía a la impresora, donde se imprime en papel. Sin embargo, una vez completada la impresión, los datos comprimidos se eliminan de la memoria y los datos de la imagen en la memoria se sobrescriben, página por página, por lo que no pueden imprimirse o transferirse nuevamente.

Es posible que los datos de trabajo se almacenen en el disco duro (HDD), en forma de datos comprimidos exclusivos, pero incluso si se pudieran leer estos datos internos, analizarlos sería prácticamente imposible. Además, en la mayoría de los modelos MFP, el disco duro se puede encriptar en su configuración estándar. También es posible bloquear la contraseña del HDD, lo que evitaría aún más el acceso no autorizado

Al usar la función de impresión segura, un trabajo de impresión puede almacenarse temporalmente en la memoria del MFP, de modo que el usuario pueda recogerlo más tarde, pero solo después de ingresar un PIN, contraseña, una tarjeta de identificación personal o un lector biométrico para acceder al archivo de impresión.

“Debemos asumir la responsabilidad de estos nuevos poderes y desarrollar una ética apropiada para ellos: ética global, ética ambiental, ética de generación futura, bioética, así como una ética de la tecnología en general”. *- Hans Jonas - Filósofo*



"Hace aproximadamente 20 años, prácticamente todos los datos se almacenaban en el centro de datos corporativo. Hoy, los datos podrían estar en ubicaciones múltiples, almacenados tanto en sucursales como en la nube pública."

Chris Evans - Computerweekly

2. Autenticación de usuarios
Para permitir la medición del uso, la restricción de uso y, lo que es más importante, la prevención del uso indebido, los dispositivos multifunción admiten la autenticación del usuario y pueden establecer reglas de permisos para que las personas, direcciones registradas o departamentos tengan acceso restringido a determinadas funciones de salida, escaneo a correos electrónicos, acceso a datos en buzón, a la configuración de un límite superior para datos de hoja de salida, o para el uso del fax. Existen diversas formas de autenticación del usuario a partir de una contraseña personal, PIN, tarjeta de identificación o lector biométrico, como reconocimiento de vena del dedo, para cada individuo en una empresa.

3. Protección de datos en el Disco Duro (HDD)
Como hemos mencionado anteriormente, los datos internos en el HDD se pueden sobrescribir para eliminar los datos. Esto se hace sobrescribiendo con números aleatorios a través de la configuración de la impresora multifunción. Además de esto, la unidad de disco duro puede estar bloqueada, y solo accesible con una contraseña, por lo que incluso si el HDD se retira de la máquina y se conecta a un PC, no se puede acceder a él. Todos los datos en la unidad de disco duro se pueden cifrar con un Estándar de cifrado avanzado (AES) y un módulo de cifrado integrado (OpenSSL / MES) y no se pueden leer o descifrar sin una clave de cifrado.
La actividad del equipo MFP se guarda como un registro de auditoría. Esto puede rastrear cualquier acceso no autorizado, pero es simplemente un registro de informes solamente y no se puede acceder para imprimir o transferir tareas o datos anteriores.

4. Encriptado de archivos PDF
Los datos escaneados con el MFP y guardados en formato PDF pueden encriptarse con una clave o código común. Para abrir un archivo PDF encriptado, usando Adobe Acrobat, se debe ingresar la clave o código común.

5. Protección de datos e-mail
Cuando un usuario envía un correo electrónico a través del MFP, puede registrarse en la libreta de direcciones del destinatario, utilizando un código para encriptar el correo electrónico, y luego el receptor puede usar su propia clave privada o código para descifrar el correo electrónico que recibe en su PC. Esto permite un envío y recepción seguros, sin que el contenido del correo electrónico sea interceptado por otros. El remitente también puede agregar una firma a un correo electrónico con la clave MFP, que el receptor debe verificar con el Certificado MFP, utilizando un chip TPM. Esto permite que el receptor confirme que el correo electrónico no fue interceptado.

6. Scan to Me, Scan to Home y Escaneo a una carpeta autorizada
Al estar habilitada la autenticación de usuario en un

"Actúe para que los efectos de su acción sean compatibles con la permanencia de la vida humana genuina."
Dr Guy Bunker, Senior Vice President - Products & Marketing

“Actúe para que los efectos de su acción sean compatibles con la permanencia de la vida humana genuina.”

Hans Jonas - filósofo

equipo multifuncional, un usuario puede enviarse facilmente datos a sí mismo. Un botón “Me” y un botón “Inicio” se muestran en la columna de la dirección registrada, habilitando la función en la configuración del Administrador.

Si se seleccionó “Me” para la dirección, se envía a la dirección de correo electrónico del usuario autenticado y, si se seleccionó “Home”, se envía a la carpeta de PC registrada previamente, lo que permite enviar archivos rápidamente con un solo click.

La autenticación SMB puede restringirse a direcciones SMB que no sean las individuales dejando las columnas [user ID] y [password] de la dirección SMB vacías. Si un usuario que ha iniciado sesión selecciona su propia dirección SMB de la libreta de direcciones y presiona ‘enviar’, el nombre de usuario y la contraseña autenticados se utilizan sin cambios.

Al restringir y prohibir la entrada directa de direcciones a través de la configuración de administrador, se puede configurar, que solo el administrador pueda administrar los destinos de envío, eliminando el potencial de uso incorrecto y el envío de datos a direcciones de correo electrónico no autorizados.

7. Tratamiento de virus

El controlador integrado en nuestras impresoras multifunción color utiliza un núcleo Linux integrado en la impresora multifunción, y la mayoría de los virus son más propensos a atacar sistemas operativos basados en Windows, debido a la naturaleza de que son más abiertos y tienden a permitir virus de una manera más fácil.
En la mayoría de los casos, los virus de memoria USB se ejecutan y causan infección simplemente insertándolos. Sin embargo, debido a que no hay ningún mecanismo en un MFP para que se abra un archivo de ejecución, debido al kernel basado en Linux, los virus contenidos en un dispositivo USB no tienen ningún efecto.

Hay funciones en un MFP que permiten la conexión y acceso a un dispositivo USB, lo que permite

(i) la impresión de datos de imagen desde un dispositivo USB
(ii) guardar los datos de imagen escaneada
(iii) los datos de imagen guardados en buzones en el dispositivo USB

Pero estas funciones deben ser activadas por el usuario, por lo que no se ejecutarán automáticamente y permite rastrear facilmente al usuario.

Además, la ruta de la interfaz USB y la ruta de la red están separadas basadas en la arquitectura del sistema. Incluso si un MFP está conectado mediante USB a un PC conectado a Internet, no se puede acceder al MFP desde el entorno de Internet a través del PC

Olivetti

“ Bueno, si se me permite decirlo, el término utopía a menudo es la forma más conveniente de disculpar que no tienes el impulso, la capacidad o el valor para hacerlo. Un sueño parece un sueño hasta que comiences a trabajar en él. Y luego puede convertirse en algo infinitamente más grande.”

Adriano Olivetti

www.olivetti.com