Seguridad Encompass
Informe técnico

Contenido

Preparado por:
Peter Davey
Director de Servicios Profesionales
Toshiba America Business Solution

15 de agosto de 2009,
Revisión A

Introducción

Durante la última década, los avances de la tecnología han incluido mejoras significativas en la infraestructura de la TI, en la colaboración de las empresas y en las aplicaciones de seguridad corporativa. Sin embargo, la vulnerabilidad de las empresas ha aumentado debido a la falta de seguridad de los dispositivos MFP y las impresoras, a controles del acceso deficientes, a documentos inseguros y al uso limitado de medidas seguras para la enajenación de activos.

Los dispositivos multifuncionales (MFP), las impresoras y los documentos son una fuente crítica de vulnerabilidad para las empresas, ya que se convierten en rampas de entrada a la red corporativa y a la web en general; por lo tanto si no se garantiza su seguridad, éstos pueden ser víctimas de ataques externos o pueden ser utilizados internamente para filtrar información corporativa a la competencia o al público en general.

En los últimos años la reglamentación en el campo de la seguridad ha aumentado y a menudo la legislación incluye normativas que responsabilizan a las empresas por la seguridad, privacidad y retención de los documentos.

Existe una variedad de contramedidas para la vulnerabilidad de los dispositivos MFP y las impresoras; sin embargo, para que éstas sean eficaces se deben emplear en forma holística como parte de una política global de seguridad.

Las Soluciones de seguridad de Encompass de Toshiba incluyen: servicios de evaluación, contramedidas incorporadas como funciones en los MFP y las impresoras, productos de Toshiba y de terceros, servicios de implementación de las medidas y programas de capacitación.

Este documento está destinado a los usuarios finales, quienes son los responsables de la toma de decisiones, y describe los problemas que enfrentan las empresas y las estrategias de Toshiba para remediarlos. La documentación técnica y otros informes técnicos sobre diversas tecnologías y contramedidas están disponibles cuando se soliciten.

Las empresas están amenazadas

Las empresas están a riesgo debido a la falta de seguridad de los dispositivos MFP y las impresoras, a controles del acceso deficientes, a documentos inseguros y al uso limitado de políticas para el fin de vida de los dispositivos. Si bien los citados riegos pueden convertirse en fuentes de fuga o hurto de propiedad intelectual, se corre además el peligro de demandas judiciales que resulten del incumplimiento de un sinnúmero de regulaciones gubernamentales y específicas de la industria. Las consecuencias también incluyen daños a la infraestructura de la TI y ataques de “denegación de servicios”.

De acuerdo con la Asociación de Examinadores de Fraude Certificados (*Association of Certified Fraud Examiners*), en Estados Unidos las empresas pierden por fuga de datos más de 600 mil millones de dólares al año, de los que dos terceras partes se pierden por falsificación o fraude de documentos.

Por lo general, la infraestructura de TI, los programas informáticos colaborativos y las aplicaciones empresariales se aseguran; mientras que los dispositivos MFP y las impresoras frecuentemente se dejan sin protección, quedando los documentos impresos y electrónicos sometidos a riesgos de seguridad durante la duración de su ciclo de vida. Otros ejemplos de vulnerabilidad incluyen los archivos que están "en reposo" dentro de los correos electrónicos corporativos y las unidades compartidas, o los archivos que están en "tránsito" de un PC hacia una impresora o de un MFP hacia un destinatario.

Los litigios están en aumento y la serie de regulaciones a las que deben adherir las empresas tienen grandes repercusiones cuyo incumplimiento puede acarrear considerables sanciones que incluyen hasta el encarcelamiento. La legislación más citada incluye: la Ley de Transferibilidad y Responsabilidad del Seguro Médico (*Health Insurance Portability and Accountability Act* o HIPAA), la Ley Sarbanes-Oxley (SOX), la Ley sobre Derechos Educativos y Privacidad de la Familia (*Family Education Rights and Privacy Act* o FERPA) y la Ley Gramm-Leach-Bliley Act (GLBA).

Además, en las redes de las empresas están aumentando las intrusiones malintencionadas, con ataques coordinados por servicios de inteligencia de distintas naciones, por organizaciones criminales y por empleados descontentos.

Las empresas están amenazadas

Las impresoras y los dispositivos MFP inseguros se pueden explotar a través de puertos abiertos que constituyen un portal de ingreso de intrusos malintencionados, quienes pueden acceder a las imágenes latentes de documentos y potencialmente explotar otros dispositivos en la red, tales como PC y servidores. Los dispositivos inseguros se pueden utilizar para atacar las infraestructuras de TI mediante la "denegación del servicio" y la puesta en funcionamiento de programas malignos tales como los virus, los robots y los registradores de digitación.

Además, el acceso a los MFP a menudo no se asegura a través de la autenticación de los usuarios, y por lo tanto, se pueden utilizar para filtrar información, o en el caso de un empleado descontento, para penetrar la red internamente.

Al igual que en otras áreas de la tecnología de la información, las medidas de seguridad se deben aplicar a todo el sistema de dispositivos MFP, impresoras y documentos; de lo contrario, las empresas corren el riesgo de perder datos, de no cumplir con las regulaciones y de ser víctimas de ataques a la infraestructura de TI.

Soluciones de seguridad de Encompass

Las Soluciones de seguridad de Encompass de Toshiba incorporan un servicio de evaluación que sirve de guía para remediar vulnerabilidades de: la seguridad en los dispositivos MFP y las impresoras, los controles para el acceso, los documentos y las políticas para el fin de vida útil. Al ofrecer una estrategia correctiva integral, las Soluciones de seguridad de Encompass también incluyen contramedidas para la vulnerabilidad de la seguridad y ofrecen cursos de capacitación que se llevan a cabo en dispositivos MFP de Toshiba y en una variedad de impresoras de otras marcas. SecureMFP es la marca que utiliza Toshiba para describir las contramedidas de seguridad y los productos y servicios afines en los MFP de Toshiba.

Las Soluciones de seguridad de Encompass agrupan las vulnerabilidades y las contramedidas respectivas en cuatro categorías:

1) Seguridad del dispositivo
2) Seguridad en el acceso
3) Seguridad de los documentos
4) Seguridad al fin del ciclo de vida

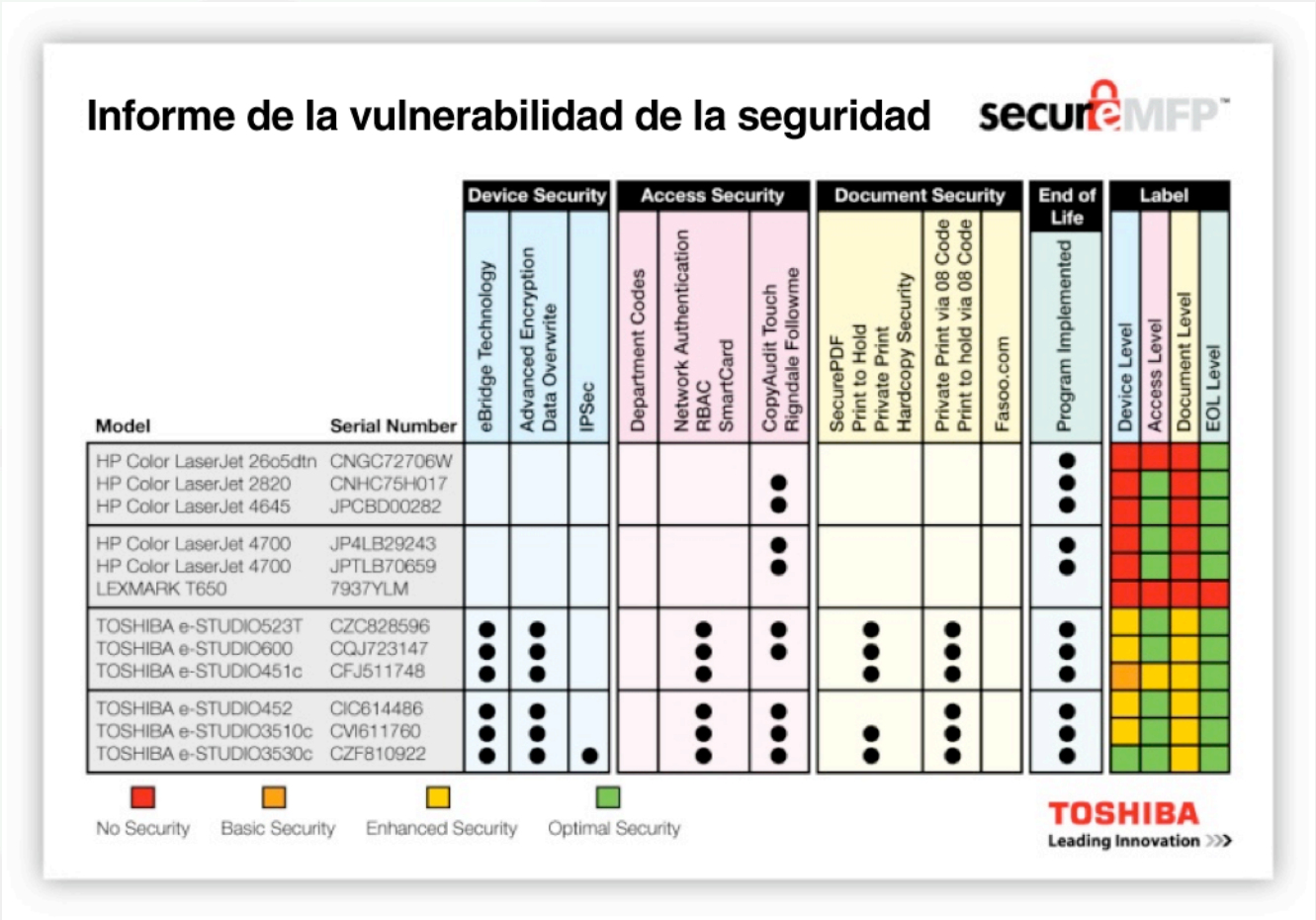
Mediante estudios de evaluación podemos calificar el nivel de seguridad de sus dispositivos, de sus controles de acceso y de sus documentos así:

1) Ninguna
2) Básica
3) Mejorada
4) Óptima

A través de consultas, el personal de los Servicios Profesionales de Toshiba evaluará la seguridad y elaborará una guía en base a la cual los ingenieros de sistemas de Toshiba pondrán en práctica las recomendaciones, instalando e implementando las contramedidas de seguridad en los dispositivos, los métodos de acceso y los documentos.

Evaluación de la seguridad Encompass

A continuación se da un ejemplo de la Evaluación de la seguridad Encompass:



Informe de la vulnerabilidad de la seguridad

securMFP™

Model	Serial Number	Device Security: eBridge Technology	Device Security: Advanced Encryption Data Overwrite	Device Security: IPSec	Access Security: Department Codes	Access Security: Network Authentication RBAC SmartCard	Access Security: CopyAudit Touch Rigndale Followme	Document Security: SecurePDF Print to Hold Private Print Hardcopy Security	Document Security: Private Print via 08 Code Print to hold via 08 Code	Document Security: Fasoo.com	End of Life: Program Implemented	Label: Device Level	Label: Access Level	Label: Document Level	Label: EOL Level
HP Color LaserJet 26o5dtn	CNGC72706W						●				●				
HP Color LaserJet 2820	CNHC75H017														
HP Color LaserJet 4645	JPCBD00282														
HP Color LaserJet 4700	JP4LB29243						●				●				
HP Color LaserJet 4700	JPTLB70659														
LEXMARK T650	7937YLM														
TOSHIBA e-STUDIO523T	CZC828596	●	●			●	●	●	●		●				
TOSHIBA e-STUDIO600	CQJ723147	●	●			●	●	●	●		●				
TOSHIBA e-STUDIO451c	CFJ511748	●	●			●	●	●	●		●				
TOSHIBA e-STUDIO452	CIC614486	●	●			●	●		●		●				
TOSHIBA e-STUDIO3510c	CVI611760	●	●			●	●		●		●				
TOSHIBA e-STUDIO3530c	CZF810922	●	●	●		●	●		●		●				

No Security Basic Security Enhanced Security Optimal Security

TOSHIBA
Leading Innovation

Contramedidas

Las vulnerabilidades y las contramedidas respectivas se agrupan en cuatro categorías y normalmente son aditivas:

Seguridad del dispositivo – *¿Están seguros los datos?*	**Seguridad de los documentos –** *¿Están protegidos los documentos?*
• SSL	• Impresión privada
• IPv6	• Imprimir y retener
• Filtrado de IP	• SecurePDF
• Firmas digitales SMB	• HardCopy Security
• IPSec	• Impresión privada (políticas)
• Cifrado avanzado	• Imprimir y retener (políticas)
• Juego de sobrescritura de datos	• Gestión de derechos digitales Fasoo
Seguridad en el acceso – *¿Está restringido el acceso?*	**Seguridad al fin del ciclo de vida –** *¿Se pueden desechar los dispositivos en forma segura?*
• Códigos de departamento	• Limpieza y eliminación de datos del disco duro
• Contraseñas fuertes	
• Limitaciones del uso	
• Registro de trabajos	
• Integración LDAP	
• Autenticación de red con acceso basado en los roles (w/RBAC)	
• Autenticación del correo electrónico	
• Autenticación con tarjetas SmartCard	
• Copy Audit Touch	
• Ringdale FollowME	

Contramedidas de seguridad del dispositivo

Seguridad del dispositivo -¿Están seguros los datos?

- **SSL**
  La capa de conectores segura (*Secure Sockets Layer o* SSL) es un protocolo criptográfico ampliamente usado en Internet para garantizar la seguridad de las comunicaciones durante la transmisión de información personal, cuando se efectúan transacciones en línea con tarjetas de crédito, se hacen pedidos, o cuando se accede a cuentas en línea. Los dispositivos MFP emplean esta tecnología de cifrado común para proteger todos los datos que viajen hacia y desde el MFP. Los trabajos de impresión que se envíen a través de la capa SSL, están cifrados por medio de criptografía simétrica, garantizando su seguridad y impidiendo que se utilicen para otras finalidades. Esto evita la intercepción de la información para propósitos fraudulentos o la alteración de datos.

- **IPv6**
  IPv6, también conocido como protocolo de Internet de nueva generación, es la versión más reciente del protocolo de Internet (IP). Con la introducción de Internet en la década del 90 y el aumento de su uso a través de los años, se presentó la necesidad de un mayor número de direcciones IP disponibles, de ahí el nacimiento de IPv6. IPv6 tiene diversas funciones para enfrentar las necesidades de seguridad de las direcciones IP, entre ellas:
  - Direcciones de mayor tamaño - el tamaño del campo para escribir la dirección pasó de 32 bits en la IPv4 a 128 bits en la IPv6. La estructura de la dirección también provee más niveles de jerarquía.
  - Compatibilidad integrada para la autenticación
  - Mayor confidencialidad

- **Filtrado de IP**
  El filtrado de IP actúa esencialmente como un cortafuegos para proteger las redes internas de los intrusos. El filtrado de IP permite controlar el tráfico IP que se autoriza hacia y desde la red, filtrando los datos de direcciones de red específicas. Los dispositivos MFP utilizan este mecanismo como un medio para controlar cuáles computadoras tienen acceso a las funciones en red.

Contramedidas de seguridad del dispositivo

Seguridad del dispositivo -¿Están seguros los datos?

- **Firma SMB**
  La firma SMB (siglas en inglés de *Server Message Block* o bloqueo de mensajes del servidor) es un método de autenticación de datos. Durante la autenticación en red, una vez que el MFP se autentica en el servidor, la firma SMB añade una firma digital a los datos transferidos entre el MFP y el servidor. La firma confirma que la identidad del servidor corresponde con las credenciales previstas por el MFP y viceversa. Al verificar que los datos recibidos provienen de una fuente autenticada, la firma garantiza la integridad de todas las comunicaciones.

- **IPSec**
  Protocolo de seguridad de IP (IPsec) protege las comunicaciones en la capa IP. Autentica y cifra los trabajos que se envían a imprimir desde el escritorio en el MFP.

- **Cifrado avanzado**
  Cifrado de la unidad de disco duro es la forma más efectiva de asegurar los datos. Las tecnologías de cifrado, tales como la tarjeta codificadora/decodificadora de Toshiba, incorporan funciones de cifrado y descifrado de todos los datos que se escriben en la unidad de disco duro del dispositivo. Esto incluye toda la información de copiado, impresión, faxeado y escaneado que se procese en el MFP. La tecnología de cifrado utiliza algoritmos criptográficos para proteger la información almacenada en la unidad de disco duro, sin retrasar los trabajos de impresión, escaneado, copiado o faxeado. El cifrado de un archivo hace que los datos no puedan ser reconocidos por otras aplicaciones e inutiliza inmediatamente los datos en caso de robo. Cuando el dispositivo de cifrado y la unidad de disco duro se desconectan del MFP los datos residuales también se pueden borrar completamente.

Contramedidas de seguridad del dispositivo

Seguridad del dispositivo -¿Están seguros los datos?

- **Juegos de sobrescritura de datos**
  La sobrescritura de datos garantiza que la unidad de disco duro quede completamente limpia de todos los datos que se puedan leer. Funciona sobrescribiendo los datos actuales con caracteres al azar y numéricos. Asimismo, al finalizar cada trabajo, el disco se limpia automáticamente después de que el dispositivo termina de usar la información, evitando que usuarios no autorizados recuperen los datos. Se recomienda que los usuarios busquen tecnologías de sobrescritura de datos que excedan la pauta del Departamento de Defensa Estadounidense de sobrescribir tres veces los datos. Esta pauta se cumple en todos los MFP de Toshiba que tengan instalado un juego de sobrescritura de datos.

Contramedidas de seguridad en el acceso

Seguridad en el acceso -¿Está restringido el acceso?

- **Códigos de usuarios/departamentos**
  Los códigos de usuarios no sólo controlan el acceso, sino que permiten rastrear los datos y obtener información sobre el uso. Los códigos de usuario exigen que el usuario ingrese su código para poder usar el dispositivo MFP. Se pueden exigir códigos para todas las funciones manuales, incluyendo copiar, escanear y faxear, al igual que para la impresión desde del escritorio de la computadora. El usuario debe ingresar un código de 5 dígitos en el panel de control para utilizar las funciones de copiado, faxeado o escaneado, o en el controlador de impresión cuando envíe trabajos para imprimir desde una computadora. Los administradores de los dispositivos pueden rastrear y constatar sin dificultad el volumen y tipo de trabajos que está generando cada usuario o cada departamento. Además, estos códigos impiden que usuarios no autorizados abusen de los recursos de la empresa o tengan acceso a información confidencial.

- **Contraseñas fuertes**
  Con la aparición de herramientas de recuperación de contraseñas que pueden descodificar una contraseña instantáneamente, se recomienda que los administradores creen contraseñas fuertes. Una contraseña fuerte es aquella que tiene al menos 8 caracteres e incluye una combinación de letras, números y símbolos que se puede recordar con facilidad pero es difícil de adivinar. Con esto se dificulta el acceso a las propiedades administrativas y de red de cada dispositivo por parte de personas no autorizadas, al igual que el acceso al panel de control del quien no conoce el nombre de usuario y la contraseña correctos. Para aumentar la protección, a veces se puede limitar a tres el número de intentos. Esta secuencia disminuye la posibilidad de que se descifre la contraseña porque bloquea la pantalla después de tres intentos fallidos. Restringir el ingreso al sistema puede evitar que personas extrañas se hagan pasar por el usuario y obtengan acceso no autorizado a datos y documentos.

Contramedidas de seguridad en el acceso

Seguridad en el acceso -¿Está restringido el acceso?

- **Limitaciones del uso**
  Las limitaciones del uso permiten que el administrador haga el seguimiento y controle la salida de documentos del dispositivo. Mediante estas limitaciones los administradores pueden restringir el número de copias o impresos disponibles para una cuenta o un departamento. Opcionalmente, también se puede restringir el uso del color en los dispositivos a color. Estas limitaciones brindan un nivel de seguridad adicional para complementar el control de acceso al dispositivo, al igual que el seguimiento y el control de costos asociados con su uso.

- **Registro de trabajos**
  La función de registro de trabajos es una herramienta valiosa que facilita el rastreo de datos y documentos a los administradores de redes, los técnicos de servicio de los distribuidores y los administradores de oficinas. Esta función mantiene un registro completo y detallado de los trabajos de impresión, copiado, faxeado y escaneado que incluye: usuario, fecha, hora, número de páginas, tipo de papel y tipo de trabajo. El registro de trabajos se puede exportar a un archivo .csv estándar para importarlo en aplicaciones de terceros. Los informes de contabilización y rastreo de datos suministran una información valiosa sobre el tipo de uso del dispositivo, el volumen y los usuarios.

- **Autenticación de red con acceso basado en los roles (w/RBAC)**
  Mediante esta autenticación se pide a los usuarios ingresar su nombre de usuario de red y su contraseña para tener acceso al panel de control. Los administradores de la red pueden controlar el acceso al dispositivo de la misma forma como controlan el acceso a la red desde el escritorio de la computadora. Si un usuario está autorizado en la red de la empresa entonces puede tener acceso al MFP. La autenticación garantiza que sólo aquellos usuarios que han sido autorizados accedan a los datos almacenados en el dispositivo. Además, permite que los destinatarios de correo electrónico conozcan la identidad del remitente, disuadiendo a los usuarios de enviar material prohibido.

Contramedidas de seguridad en el acceso

Seguridad en el acceso -¿Está restringido el acceso?

- **Autenticación del correo electrónico**
  Ofrece la capacidad de autenticación en el modo nativo de los servidores de correo electrónico de Microsoft Exchange.

- **Integración LDAP**
  La integración LDAP (siglas en inglés de *Lightweight Directory Access Protocol* o protocolo ligero de acceso a directorios) suministra una libreta de direcciones centralizada de todos los empleados y permite que el administrador establezca reglas y derechos de acceso a grupos específicos de usuarios. Por ejemplo, el administrador puede prohibir que los empleados que lleven trabajando con la empresa menos de 90 días escaneen o envíen faxes. Con la autenticación LDAP las reglas establecidas por el administrador se aplican a todos los dispositivos MFP de la empresa. Además, el nombre del usuario que escanee un documento aparece en el documento, lo que impide que los usuarios envíen material malintencionado o prohibido a través de la red de la empresa.

- **Autenticación con tarjetas SmartCard**
  La autenticación con tarjetas SmartCard ofrece funciones de seguridad ampliadas, diseñadas para eliminar las operaciones no autorizadas y reducir los costos y los tiempos de inactividad. Utilizando un punto de ingreso ágil y único, esta autenticación facilita el proceso de inicio de sesión ya que basta deslizar una tarjeta en vez de escribir el nombre de usuario y la contraseña. Como la seguridad se ha convertido en la prioridad principal en muchas empresas, Toshiba se ha comprometido con ofrecer soluciones que aseguren la integridad de los datos y que rindan cuenta de ellos durante el proceso de envío de la información hacia o desde el dispositivo MFP. Usted controla quién está autorizado, y por lo tanto mantiene la rentabilidad y la seguridad.

- **Auditoría de la impresión con Copy Audit Touch**
  Impresión segura, registro de los trabajos de impresión y contabilización de costos con Copy Audit Touch.

Contramedidas de seguridad en el acceso

Seguridad en el acceso -¿Está restringido el acceso?

- **Ringdale FollowME**
  Ofrece funciones de seguimiento de trabajos impresos, contabilización de costos y seguridad en la entrega limitando el acceso a los usuarios autorizados.

- **Pharos BluePrint Enterprise**
  Seguimiento de los trabajos impresos, contabilización de los costos, políticas de impresión y entrega segura de los trabajos de impresión tipo pull (impresión que se envía a un servidor y luego a la impresora).

Contramedidas de seguridad de los documentos

Seguridad de los documentos - ¿Están protegidos los documentos?

- **SecurePDF**
  Cuando se escanean documentos para enviar por correo electrónico o enviar a ubicaciones en la red se requiere más control y protección, como en el caso de la impresión privada. Con SecurePDF (PDF Seguro), los usuarios pueden asignar directamente, desde el panel de control del MFP, una contraseña a los documentos PDF escaneados. Esta contraseña permite varios niveles de control tales como acceso, impresión, edición y copiado del contenido. Adicionalmente, se puede aplicar un cifrado de 128 bits para garantizar el almacenamiento seguro del documento. SecurePDF es la solución perfecta para quienes deseen enviar por correo electrónico o almacenar documentos escaneados sin comprometer su contenido.

- **Impresión privada**
  Esta función ofrece control completo de la salida de impresos, exigiendo que los usuarios escriban una contraseña antes de que los documentos salgan de la máquina. Cuando el usuario va a retirar sus documentos del dispositivo, primero debe ingresar la contraseña personal confidencial. Esta contraseña libera cada documento seleccionado enviado por el usuario a quien corresponda la contraseña. Fabricantes como Toshiba, también ofrecen la función de impresión privada de lotes, que permite a los usuarios liberar todos los trabajos que estén bajo su nombre en la cola de impresión. Esto elimina la necesidad de ingresar la contraseña para cada documento individual cuando el usuario envía trabajos múltiples. La impresión privada es ideal para organizaciones que impriman información confidencial, y evita que se recoja el trabajo de impresión equivocado, accidental o intencionalmente. La función de impresión privada es esencial para el control de los datos de impresión y de salida de documentos en el MFP.

Contramedidas de seguridad de los documentos

Seguridad de los documentos - ¿Están protegidos los documentos?

- **HardCopy Security**
  La trama de seguridad incrustada es una función que restringe las copias no autorizadas y evita la fuga de información, ya que la cadena de caracteres ocultos incrustada en el documento durante el proceso de impresión aparece cuando se copia el documento. Por ejemplo: Prohibido copiar.

- **Gestión de derechos digitales Fasoo Enterprise**
  Incluye un software de gestión de derechos digitales para las empresas y para el intercambio de documentos entre varias empresas.

Seguridad al fin del ciclo de vida

Seguridad al fin del ciclo de vida -¿Se pueden desechar los dispositivos en forma segura?

- **Limpieza total del disco duro**
  Es importante que las organizaciones dispongan de políticas de seguridad para garantizar que los datos confidenciales almacenados en los MFP y las impresoras se eliminen totalmente cuando se llegue al fin del ciclo de vida o se termine el contrato de arrendamiento del equipo. Si la empresa no tiene establecidas unas políticas de seguridad para el fin de vida de los dispositivos, Toshiba las formula como parte de la evaluación de la vulnerabilidad de la seguridad de Encompass.