# GUÍA DE PROTECCIÓN PARA DISPOSITIVOS MULTIFUNCIÓN

imageRUNNER ADVANCE

Canon

# INTRODUCCIÓN

Los dispositivos multifunción modernos de Canon ofrecen funciones de impresión, copia, escaneado, envío y fax. Los dispositivos multifunción son servidores informáticos por sí solos, que ofrecen una gran cantidad de servicios en red junto con una importante capacidad de almacenamiento en disco duro.

Cuando una organización introduce estos dispositivos en su infraestructura, debe tener en cuenta varias áreas como parte de su estrategia de seguridad más amplia, con el fin de proteger la confidencialidad, integridad y disponibilidad de los sistemas en red.

Es evidente que las implantaciones serán diferentes y cada organización tendrá sus propios requisitos de seguridad. Aunque trabajamos con nuestros clientes para garantizar que los dispositivos de Canon se envíen con los parámetros de seguridad iniciales adecuados, nuestro objetivo es prestar una mayor asistencia al ofrecer distintos parámetros de configuración para permitir ajustar el dispositivo a los requisitos de cada situación específica.

El diseño de este documento tiene como fin ofrecer suficiente información para permitir hablar con Canon o con uno de nuestros partners autorizados sobre los parámetros más adecuados para tu entorno. Debe tenerse en cuenta que no todo el hardware del dispositivo tiene el mismo nivel de capacidad y que un System software diferente puede proporcionar una funcionalidad diferente. Una vez decidido, la configuración definitiva puede aplicarse al dispositivo o parque de dispositivos. Es posible contactar con Canon o con uno de nuestros partners autorizados para obtener más información y asistencia

### ¿A quién va dirigido este documento?

Este documento está dirigido a todos aquellos implicados en el diseño, implantación y protección de los dispositivos multifunción de oficina en una infraestructura de red. Esto puede incluir especialistas de IT y redes, profesionales de la seguridad de IT y personal de mantenimiento.

### Ámbito y cobertura

Esta guía explica y asesora sobre los parámetros de configuración para dos entornos de red típicos, de modo que las organizaciones puedan implantar una solución multifunción de forma segura basada en las prácticas recomendadas. También explica (a partir de la versión 3.8 de la plataforma del System software) cómo la funcionalidad Syslog puede proporcionar información en tiempo real desde el dispositivo multifunción. El equipo de seguridad de Canon ha probado y validado estos parámetros.

No hacemos ninguna suposición respecto a los requisitos normativos específicos de algunos sectores que pueden imponer otras consideraciones sobre seguridad y quedan fuera del ámbito de este documento.

Esta guía se basa en el conjunto típico de funciones de la plataforma imageRUNNER ADVANCE y, aunque la información incluida en este documento es aplicable a todos los modelos y series de la gama imageRUNNER ADVANCE, algunas funciones pueden variar de un modelo a otro.

### Implantación de la seguridad adecuada para los dispositivos multifunción dentro del entorno

Para analizar las implicaciones en materia de seguridad que tiene la implantación de un dispositivo multifunción en la red, hemos tenido en cuenta dos situaciones típicas:

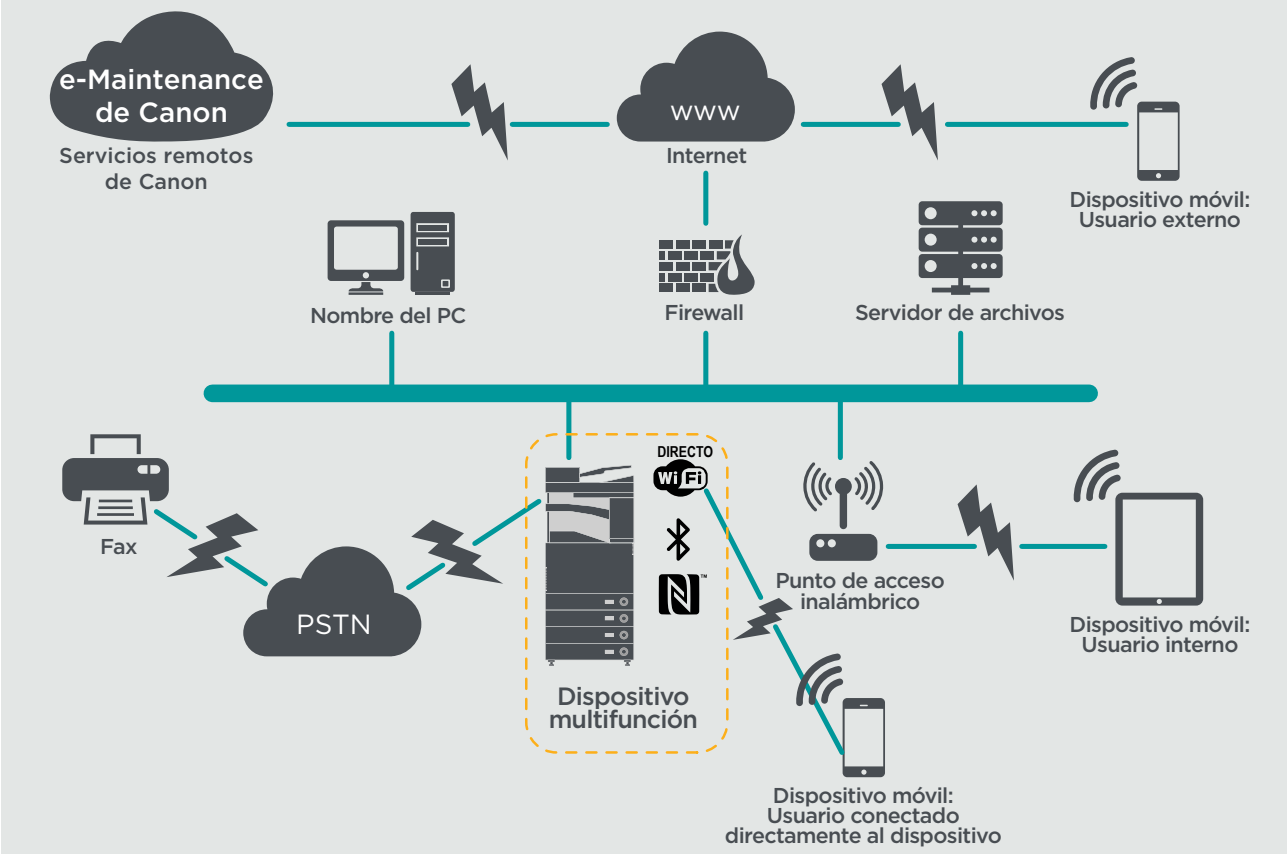
- **Un entorno de oficina de pequeña empresa**
- **Un entorno de oficina de gran empresa**

# ENTORNO DE OFICINA PEQUEÑA EMPRESA

Normalmente hablaríamos de un entorno de oficina con una topología de red donde se utilizarían uno o dos dispositivos multifunción para uso interno y estos dispositivos no están accesibles en Internet.

Aunque está disponible la impresión móvil, se necesitan componentes adicionales. Para los usuarios que necesitan servicios de impresión fuera del entorno LAN, se necesita una conexión segura. Sin embargo, debe prestarse atención a la seguridad de los datos en tránsito entre el dispositivo remoto y la infraestructura de impresión.

**Figura 1** Red de oficina pequeña empresa




La última generación de modelos de imageRUNNER ADVANCE ofrece conexión en red inalámbrica, lo que permite al dispositivo conectarse a una red WiFi. También se puede usar para establecer una conexión WiFi Direct punto a punto con un dispositivo móvil sin necesidad de usar una conexión de red.

Las opciones Bluetooth y NFC están disponibles para varios modelos y se usan para establecer la conexión WiFi Direct solo para los dispositivos iOS y Android respectivamente.

# CONSIDERACIONES PARA LA CONFIGURACIÓN

Hay que tener en cuenta que, a menos que una función de imageRUNNER ADVANCE se mencione debajo, la configuración predeterminada se considera suficiente para este entorno empresarial y de red.

**Tabla 1** Consideraciones para la configuración de un entorno de oficina pequeña empresa

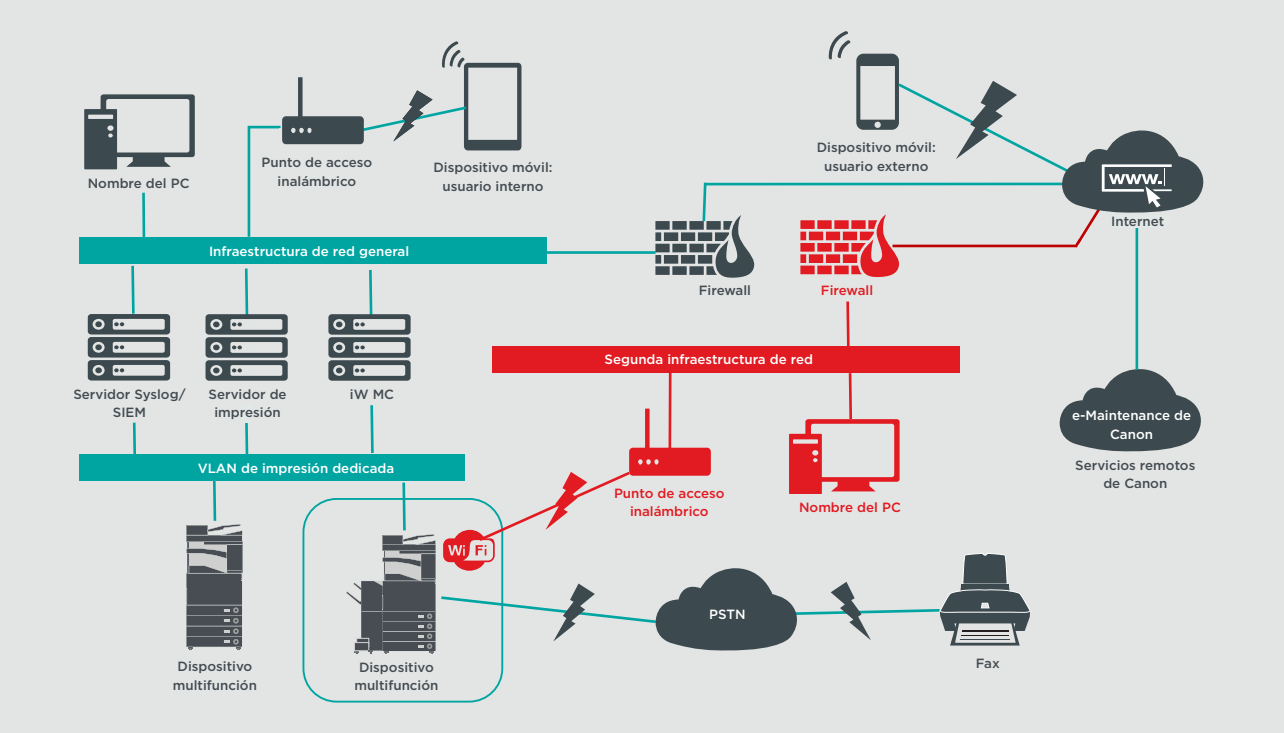
| Función de imageRUNNER ADVANCE | Descripción | Consideración |
|---|---|---|
| Modo mantenimiento | Permite el acceso a los parámetros del modo mantenimiento del dispositivo | Protección mediante contraseña no predeterminada, no trivial y de longitud máxima |
| Sistema de gestión de mantenimiento del dispositivo | Permite acceder a diversos ajustes no estándar del dispositivo | Protección mediante contraseña no predeterminada, no trivial y de longitud máxima |
| Navegación/Envío SMB | Almacenar y recuperar desde y a recursos compartidos de red SMB/Windows | Por política, los administradores del sistema no deben permitir a ningún usuario crear cuentas locales en su equipo cliente para compartir documentos con el dispositivo imageRUNNER ADVANCE a través de SMB |
| Interfaz de usuario remota | Herramienta de configuración basada en web | El administrador de imageRUNNER ADVANCE debe activar HTTPS para la IU remota y desactivar el acceso HTTP. Además, se debe activar el uso de autenticación de PIN único para cada dispositivo |
| SNMP | Integración de supervisión de red | Desactivar la versión 1 y activar solo la versión 3 |
| Enviar a correo electrónico y/o IFAX | Envía mensajes de correo electrónico desde el dispositivo con archivos adjuntos | Activar SSL<br>No usar la autenticación POP3 antes del envío SMTP<br>Usar la autenticación SMTP |
| POP3 | Recoge e imprime documentos automáticamente desde el buzón de correo | Activar SSL<br>Activar la autenticación POP3 |
| Libreta de direcciones/LDAP | Usa el servicio de directorio para buscar números o direcciones de correo electrónico a las que enviar los documentos escaneados | Activar SSL<br>No usar credenciales de dominio para autenticar en el servidor LDAP, usar credenciales específicas LDAP |
| Impresión FTP | Carga y descarga documentos de y al servidor FTP integrado | Activar la autenticación FTP. Hay que tener en cuenta que el tráfico FTP siempre se transmite por la red sin cifrar |
| Envío WebDAV | Escanea y almacena documentos en una ubicación remota | Activar la autenticación para los recursos compartidos WebDAV |
| PDF cifrado | Cifra los documentos | Por política, los documentos confidenciales solo se deben cifrar con PDF versión 1.6 (AES-128) |
| Impresión segura | El trabajo de impresión se envía al dispositivo pero queda bloqueado en la cola de impresión hasta que se introduzca el número PIN correspondiente | Permitir trabajos de impresión protegidos mediante PIN |
| Notificación de eventos Syslog | El protocolo de registro del sistema es un protocolo estándar del sector que se utiliza para enviar mensajes de eventos o registros del sistema a un servidor específico denominado servidor Syslog | Se debe considerar la posibilidad de dirigir los datos de imageRUNNER Syslog a la herramienta de análisis syslog de red o a la plataforma SIEM (Sistema de gestión de eventos de seguridad) empresarial de que se disponga |
| Verificación inicial del sistema (Arranque Seguro) | Garantiza que los componentes del software del sistema no se han visto comprometidos. Tendrá un impacto mínimo en el tiempo de arranque del sistema | Activar función |
| Navegador web integrado | Acceso a Internet a través del navegador | Aplicar mediante la administración, usar un proxy web de filtrado de contenido para impedir que se acceda a contenidos maliciosos o virales. Desactivar la creación de favoritos |
| Bluetooth y NFC<br>(Disponible como opción a partir de los modelos Generation 3) | Se usa para establecer la conexión WiFi Direct | Activar WiFi Direct para permitir la conexión directa a un dispositivo móvil. No se puede usar WiFi Direct cuando se usa WiFi para conectarse a una red |
| LAN inalámbrica | Ofrece acceso inalámbrico | Usar WPA-PSK/WPA2-PSK con contraseñas seguras |
| IPP | Conecta y envía trabajos de impresión a través de IP | Desactivar IPP |
| TPM | Función que almacena datos de seguridad, como contraseñas y claves de cifrado, en el hardware para garantizar la máxima protección | Esta función está desactivada de forma predeterminada. Cuando se active, se recomienda crear una copia de seguridad |

# ENTORNO DE OFICINA DE GRAN EMPRESA

Suele ser un entorno de varias oficinas en distintas ubicaciones con una arquitectura de red segmentada. Compuesta por varios dispositivos multifunción implantados en una red VLAN independiente accesible para el uso interno a través de servidores de impresión. No se puede acceder a estos dispositivos multifunción desde Internet.

Este entorno suele tener un equipo de soporte para gestionar sus requisitos de red y de administración junto con cuestiones informáticas generales pero se presupone que no tendrán formación específica en dispositivos multifunción.

**Figura 2** Red de oficina de gran empresa




Las conexiones resaltadas en rojo estarán disponibles a partir de los modelos Generation 3

# CONSIDERACIONES PARA LA CONFIGURACIÓN

Hay que tener en cuenta que, a menos que una función de imageRUNNER ADVANCE se mencione debajo, la configuración predeterminada se considera suficiente para este entorno empresarial y de red.

**Tabla 2** Consideraciones para la configuración de un entorno de oficina de gran empresa

| Función de imageRUNNER ADVANCE | Descripción | Consideración |
|---|---|---|
| Modo mantenimiento | Permite el acceso a los parámetros del modo mantenimiento del equipo | Protección mediante una contraseña no predeterminada, no trivial y de longitud máxima |
| Sistema de gestión de mantenimiento del dispositivo | Permite acceder a diversos ajustes no estándar del dispositivo | Protección mediante una contraseña no predeterminada, no trivial y de longitud máxima |
| Navegación/Envío SMB | Almacenar y recuperar desde y a recursos compartidos de red SMB/Windows | Por política, los administradores del sistema no deben permitir a ningún usuario crear cuentas locales en su equipo para compartir documentos con el dispositivo imageRUNNER ADVANCE a través de SMB |
| Interfaz de usuario remota | Herramienta de configuración basada en web | Tras las configuraciones del dispositivo iniciales, desactivar la IU remota completamente mediante la desactivación de HTTP y HTTPS |
| SNMP | Integración de supervisión de red | Desactivar la versión 1 y activar solo la versión 3 |
| Enviar a correo electrónico y/o IFAX | Envía mensajes de correo electrónico desde el dispositivo con archivos adjuntos | Activar SSL<br>Habilitar:<br>- Verificación del certificado en el servidor SMTP<br>O bien, si no es viable:<br>- Usar solo esta función en un entorno en el que haya un recopilador de sistema de detección de intrusos en la red No usar la autenticación POP3 antes del envío SMTP Usar autenticación SMTP |
| POP3 | Recoge e imprime documentos automáticamente desde el buzón de correo | Activar SSL<br>Habilitar:<br>- Verificación del certificado en el servidor POP3<br>O bien, si no es viable:<br>- Usar solo esta función en un entorno en el que haya un recopilador de sistema de detección de intrusos en la red Activar la autenticación POP3 |
| Libreta de direcciones/LDAP | Usa el servicio de directorio para buscar números de teléfono o direcciones de correo electrónico a las que enviar los documentos escaneados | Activar SSL<br>Habilitar:<br>- Verificación del certificado en el servidor LDAP<br>O bien, si no es viable:<br>- Usar solo esta función en un entorno en el que haya un recopilador de sistema de detección de intrusos en la red No usar credenciales de dominio para autenticar en el servidor LDAP, usar credenciales específicas LDAP |
| IPP | Conecta y envía trabajos de impresión a través de IP | Desactivar IPP |
| Envío WebDAV | Escanea y almacena documentos en una ubicación remota | Activar la autenticación para los recursos compartidos WebDAV<br>Activar SSL<br>Hacer que la impresora solo permita archivos que terminen con las «extensiones de impresión de archivo» que se carguen |
| IEEE802.1X | Mecanismo de autenticación de acceso a red | Compatible con EAPOL V1 |
| PDF cifrado | Cifra los documentos | Por política, los documentos confidenciales solo se deben cifrar con PDF versión 1.6 (AES-128) |
| Impresión segura cifrada | Mejora la protección de la impresión segura al cifrar el archivo y la contraseña durante la transmisión | Configurar el nombre de usuario en la pestaña Impresora de la configuración de la impresora cliente con otro nombre de usuario distinto al de las credenciales de dominio/LDAP de dicho usuario. Comprobar que está desactivada la opción «Restringir trabajos de impresora» |
| Inscripción automática de certificados | El proceso de inscripción automática mejora la eficacia de la recuperación e implementación de la certificación digital | Requiere una solución de certificado de red para su uso |
| Notificación de eventos Syslog | El protocolo de registro del sistema es un protocolo estándar del sector que se utiliza para enviar mensajes de eventos o registros del sistema a un servidor específico denominado servidor Syslog | Se debe considerar la posibilidad de dirigir los datos de imageRUNNER ADVANCE Syslog a la herramienta de análisis syslog de red o a la plataforma SIEM (Sistema de gestión de eventos de seguridad) empresarial de que se disponga |
| Verificación inicial del sistema (Arranque Seguro) | Garantiza que los componentes del software del sistema no se han visto comprometidos. Tendrá un impacto mínimo en el tiempo de arranque del sistema | Activar función |
| LAN inalámbrica | Ofrece acceso inalámbrico | Usar WPA-PSK/WPA2-PSK con contraseñas seguras |
| WiFi Direct | Se usa para establecer la conexión WiFi Direct | Desactivar WiFi Direct |
| Navegador web integrado (disponible a partir de los modelos Generation 3 II) | Acceso a Internet a través del navegador | Aplicar las restricciones correspondientes o desactivar la posibilidad de descargar archivos adquiridos a través del navegador |

La última generación de modelos de imageRUNNER ADVANCE ofrece conexión en red inalámbrica, lo que permite al dispositivo conectarse a una red WiFi al mismo tiempo que se conecta a una red cableada. Esta situación puede resultar útil si el cliente tiene que compartir un dispositivo con dos redes. Un ejemplo típico sería un colegio, donde hay dos redes independientes: una para los alumnos y otra para el personal.

La plataforma imageRUNNER ADVANCE proporciona un entorno de funciones para un uso flexible. Con los protocolos y servicios disponibles para lograrlo, es importante asegurarse de que solo las funciones, los servicios y los protocolos necesarios estén habilitados a fin de satisfacer las necesidades del usuario. Esta es una buena práctica de seguridad que reducirá la posible área de ataque y evitará el abuso. Dado que aparecen nuevas vulnerabilidades constantemente, debemos mantener la guardia para no comprometer el dispositivo, ni de forma intrínseca ni extrínseca. Tener la capacidad de supervisar la actividad de los usuarios es útil para ayudar a identificar y tomar medidas correctivas cuando sea necesario.

La versión 3.8 de la plataforma de software imageRUNNER ADVANCE proporciona algunas funciones adicionales a las que ya llevan varios años disponibles. Estas incluyen la capacidad de supervisar el dispositivo en tiempo real mediante Syslog y la verificación inicial del sistema. El uso de estas funciones en colaboración con sus soluciones de seguridad de red existentes, como una plataforma de gestión de eventos de información de seguridad o una solución de inicio de sesión, permite una mayor visibilidad y la identificación de incidentes, además de poder utilizarse con fines forenses.

## Módulo de plataforma segura (TPM)

Todos los dispositivos imageRUNNER ADVANCE incluyen un módulo de plataforma segura (TPM), un chip de seguridad (los modelos imageRUNNER ADVANCE DX están equipados con TPM 2.0). Se encarga del almacenamiento de contraseñas, certificados digitales y claves criptográficas.

Todos los modelos imageRUNNER ADVANCE actuales con unidades de disco duro o de estado sólido proporcionan cifrado de unidad completa. La clave de cifrado se almacena en el chip de seguridad MFP de Canon, que es conforme con la norma de seguridad FIPS 140-2 Nivel 2 (establecida por el gobierno de Estados Unidos).

De forma predeterminada, la función TPM está desactivada, pero se puede activar a través del menú Funciones adicionales de imageRUNNER ADVANCE. Se recomienda realizar una copia de seguridad del TPM en caso de que se produzca un error inmediatamente después de habilitarlo.

Para obtener más información relacionada con el TPM, introduce el siguiente enlace en tu navegador web y escribe Utilizar TPM en el cuadro de búsqueda. Accederá a información relacionada con:

- La activación del TPM
- La copia de seguridad y restauración del TPM

https://oip.manual.canon/USRMA-4790-zz-CS-5700-enGB/

## Verificación inicial del sistema (Arranque Seguro)

Esta función es un mecanismo diseñado para garantizar que todas las partes del software del sistema de imageRUNNER ADVANCE Generation 3 Edition III se verifican respecto a un Inicio Seguro para garantizar que el sistema operativo se carga según lo previsto por Canon. Si un usuario malintencionado manipula o intenta modificar el sistema, o si se produce un error al cargar el sistema, el proceso se detendrá y se mostrará un código de error.


**Figura 3** Proceso de verificación inicial del sistema

Este proceso es transparente para el usuario, aparte de la indicación en pantalla informando de que se está cargando una versión no intencionada del sistema. imageRUNNER ADVANCE DX tiene la opción de activar la verificación inicial del sistema.

## Borrado seguro de datos

El dispositivo multifunción gestiona los datos para realizar trabajos de copia, escaneado, impresión y fax, así como libretas de direcciones, registros del sistema e historial de trabajos, lo que podría contener información confidencial. La plataforma imageRUNNER ADVANCE proporciona una función de borrado de datos segura para garantizar que no solo se elimina la tabla de asignación de archivos de los datos eliminados, sino que los sectores que almacenan los datos se sobrescriben con datos ficticios que impiden la recuperación.

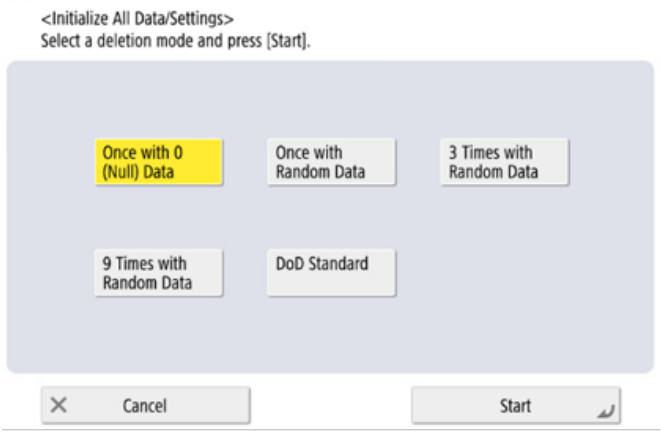



**Figura A**: Opciones de sobrescritura de datos para dispositivos imageRUNNER ADVANCE equipados con disco duro

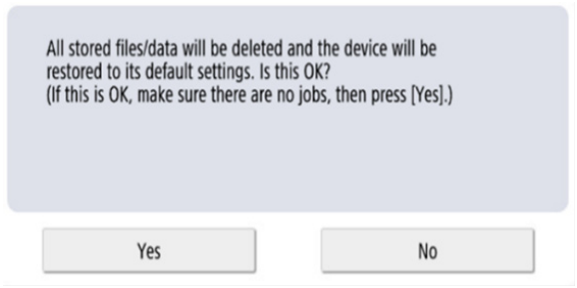



**Figura B**: Inicializar todos los datos de SSD para imageRUNNER ADVANCE

En función del modelo específico de dispositivo, se utiliza una unidad de disco duro (HDD) o una unidad de estado sólido (SSD). Puesto que una HDD utiliza un plato giratorio físico en la que se graban los datos, se necesitan varias sobrescrituras, normalmente tres, para garantizar una sobrescritura correcta. Sin embargo, la tecnología SSD gestiona el almacenamiento de forma diferente al distribuir la asignación de memoria de forma uniforme en todo el espacio disponible, lo que anula la necesidad de sobrescribir de forma continuada.

## Tecnología SSD

A diferencia de un disco duro, con un SSD no debería haber necesidad de realizar un mantenimiento, ya que se han incorporado funciones de autosuficiencia en el diseño, mediante algoritmos y mecanismos de seguridad a prueba de errores, para garantizar que los datos se eliminen de forma eficaz al tiempo que se aumenta la vida útil. Los datos se almacenan de forma eléctrica en celdas de memoria de estado sólido, lo que aumenta la velocidad de acceso.

### Nivelación de desgaste

Para garantizar que el número de escrituras se mantenga lo más uniforme posible en todos los bloques de celdas se emplea un proceso denominado nivelación de desgaste. Se utilizan dos principios: nivelación dinámica de desgaste y nivelación estática de desgaste.

La nivelación dinámica de desgaste asigna bloques de almacenamiento para que las reescrituras se vuelvan a colocar en nuevos bloques vacíos. A continuación, se incrementa un contador de desgaste para permitir que el controlador SSD realice un seguimiento del desgaste. La nivelación de desgaste estática permite trasladar los datos no modificados existentes a un nuevo bloque de memoria, lo que distribuye el desgaste de forma más uniforme en el almacenamiento disponible. Este principio trata de distribuir la cantidad de reescrituras de manera uniforme en todos los bloques de memoria, independientemente de que los datos cambien de forma ocasional o constante. El proceso de «TRIM» contribuye a prolongar la vida útil y garantizar la asignación de datos a gran velocidad.

Según el modelo de imageRUNNER ADVANCE, se ofrecen varias opciones de ajustes diferentes que se pueden configurar para establecer el punto en el que se realiza una sobrescritura y el método de sobrescritura. Los modelos que utilizaban almacenamiento en disco duro incluían una función de eliminación de datos integral para borrar los datos por completo.

- La clave de cifrado SSD se almacena en el dispositivo concreto; si se elimina del dispositivo, los datos se cifran con **AES de 256 bits** y no se pueden leer/escribir
- El chip de seguridad MFP 2.10 de Canon es conforme con la norma de seguridad **FIPS 140-2 Nivel 2** (gobierno de EE. UU.)

#### Inicializar todos los datos/ajustes

- **Limitado a [Una vez con datos 0 (nulos)]**
- La unidad SSD es de estado sólido y la unidad de disco duro utiliza discos magnéticos giratorios.
- Además, después de escribir una vez con datos 0, es prácticamente imposible leer los datos escritos porque la tabla de acceso se reescribe y la ubicación de los datos es desconocida.
- Puesto que los datos almacenados están cifrados, no se puede leer/escribir datos en un PC o tras la instalación en un MFP diferente.

## Inscripción automática de certificados

En las versiones anteriores a la 3.8 de la plataforma de software del sistema imageRUNNER ADVANCE, el administrador tenía que instalar manualmente los certificados de seguridad actualizados en cada dispositivo. Se trata de una tarea laboriosa, ya que es necesario conectarse a cada dispositivo, uno por uno, para realizar una actualización manual. Los certificados se deben instalar manualmente mediante la interfaz de usuario remota (RUI) del dispositivo específico, lo que hace que el proceso sea mucho más lento. Con el servicio de inscripción automática de certificados introducido a partir de la versión 3.8 y posteriores de la plataforma, se ha eliminado esta sobrecarga.

El proceso de inscripción automática mejora la eficiencia de la recuperación de la certificación. Permite recuperar certificados automáticamente mediante el servicio de inscripción de dispositivos de red (NDES) para Microsoft Windows y el protocolo de inscripción de certificados simple (SCEP).

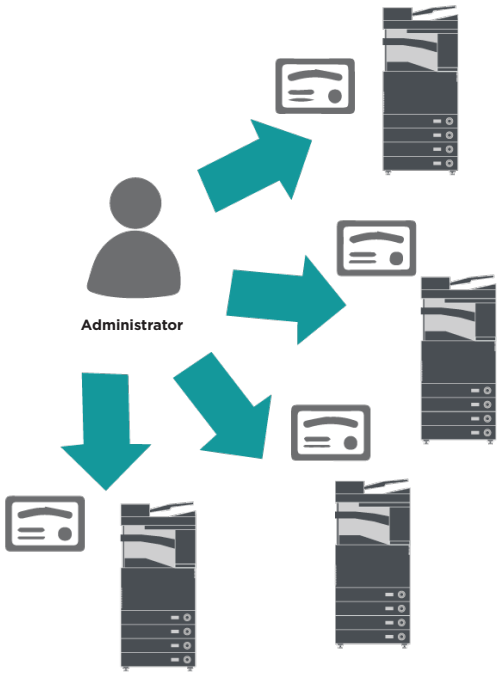



**Figura 4** Inscripción de certificados

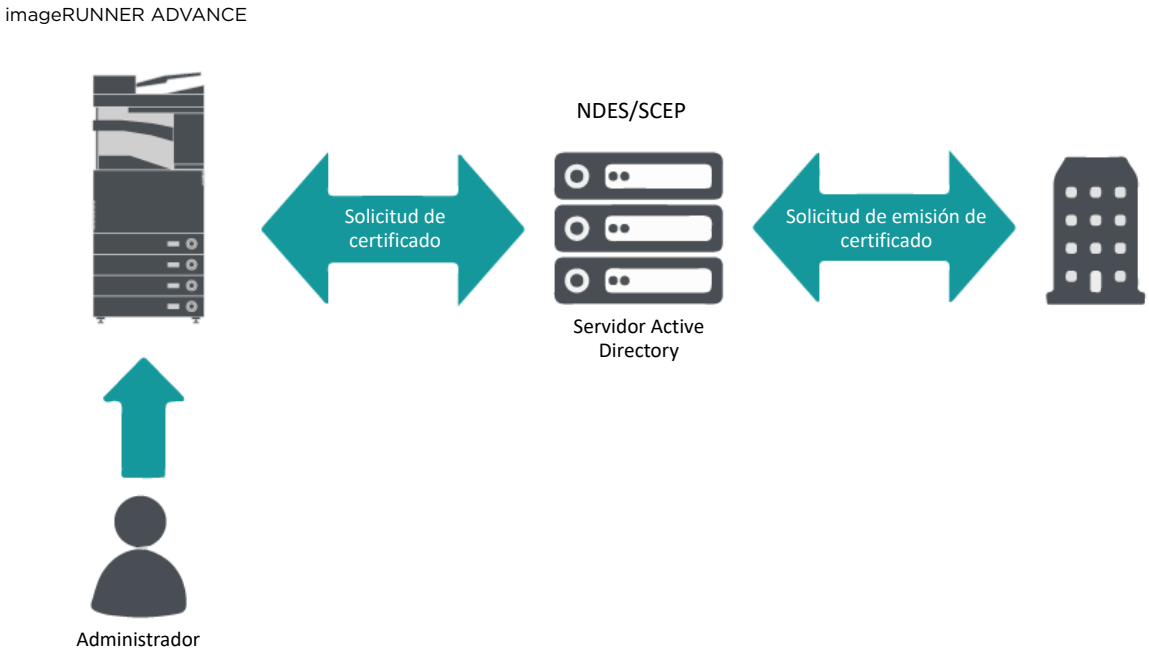



**Figura 5** Proceso de inscripción de certificados

SCEP es un protocolo que admite certificados emitidos por una autoridad de certificación (CA) y NDES permite a los dispositivos de red recuperar o actualizar certificados basados en SCEP.

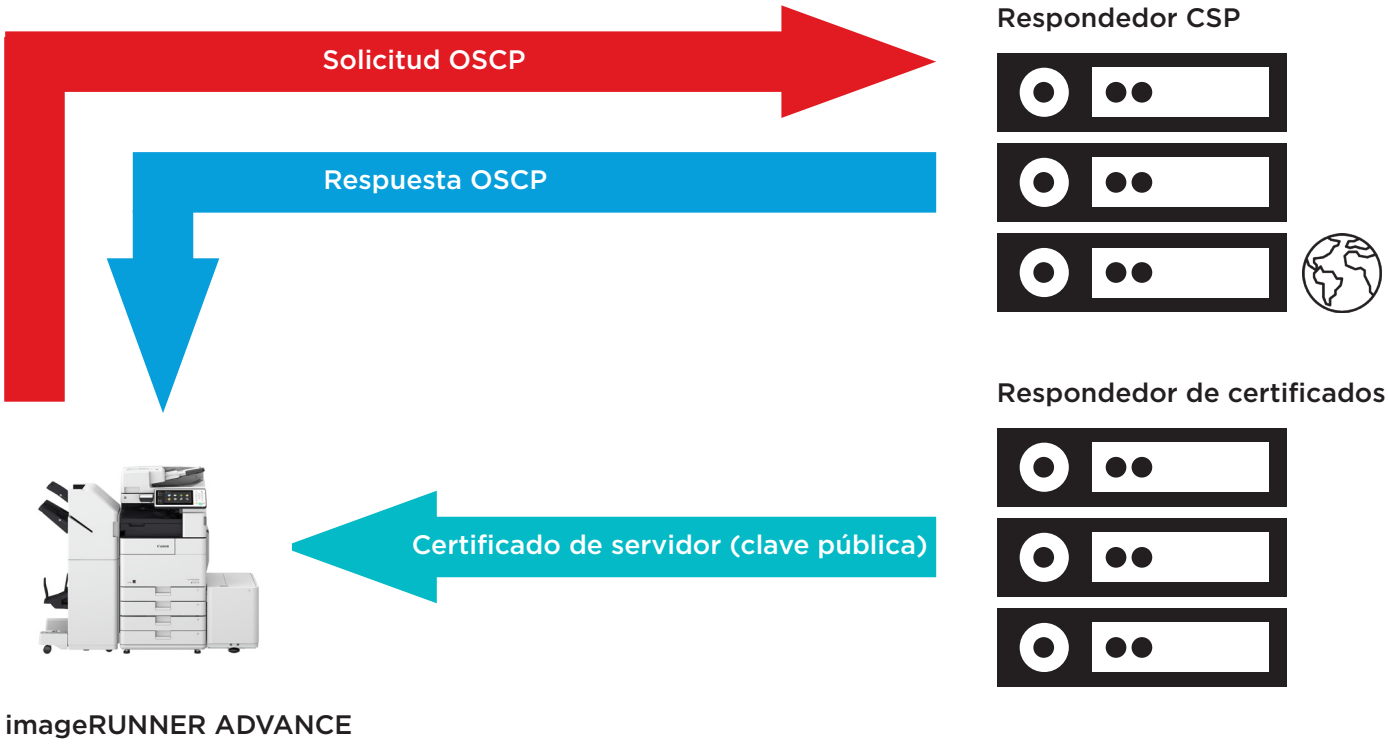
NDES es un servicio de roles de los Servicios de certificados de Active Directory.

## Protocolo de estado de certificados en línea

Existen varias razones por las que puede ser necesario revocar un certificado digital. Algunos ejemplos incluyen la pérdida de la clave privada, su robo o que esta se haya visto comprometida, o el cambio de un nombre de dominio.

El protocolo de estado de certificados en línea (OCSP) es un protocolo de Internet estándar que se utiliza para comprobar el estado de revocación de un certificado digital X.509 proporcionado por el servidor de certificados. Al enviar una solicitud de OCSP al respondedor OCSP (normalmente un emisor de certificados) con un certificado específico, el respondedor OCSP responderá con una confirmación, una revocación o una indicación de desconocido.

**Figura 6** Proceso de establecimiento de comunicación de OCSP




Con imageRUNNER ADVANCE en la versión 3.10 de la plataforma, OCSP proporciona un mecanismo en tiempo real para verificar los certificados digitales X.509 instalados. Las versiones anteriores de la plataforma solo admitían el método de lista de revocación de certificados (CRL), que resultaba ineficiente y generaba una sobrecarga en los recursos de la red.

## Gestión de eventos e información de seguridad

La tecnología imageRUNNER ADVANCE es capaz de distribuir eventos de seguridad en tiempo real mediante el protocolo Syslog que cumple las normas RFC 5424, RFC 5425 y RFC 5426.

Este protocolo lo utiliza una amplia gama de tipos de dispositivos como una forma de recopilar información en tiempo real que se puede utilizar para identificar posibles problemas de seguridad.

Para facilitar la detección de amenazas e incidentes de seguridad, el dispositivo debe configurarse para que apunte a un servidor de Gestión de eventos de seguridad ante incidentes (SIEM) de terceros.

Los eventos Syslog producidos por el dispositivo se pueden utilizar para crear acciones a través de la recopilación y el análisis en tiempo real de eventos procedentes de una amplia variedad de fuentes de datos contextuales (Figura 7). También puede ayudar a la elaboración de informes de conformidad y la investigación de incidentes mediante el uso de soluciones adicionales como un servidor SIEM. En la figura 8 se muestra un ejemplo.

La última generación de dispositivos imageRUNNER ADVANCE proporciona funciones Syslog compatibles con una amplia gama de eventos que se pueden recopilar. Esto se puede utilizar para correlacionar y analizar eventos entre diversas fuentes para identificar tendencias o anomalías.


**Figura 7** Captura de datos Syslog

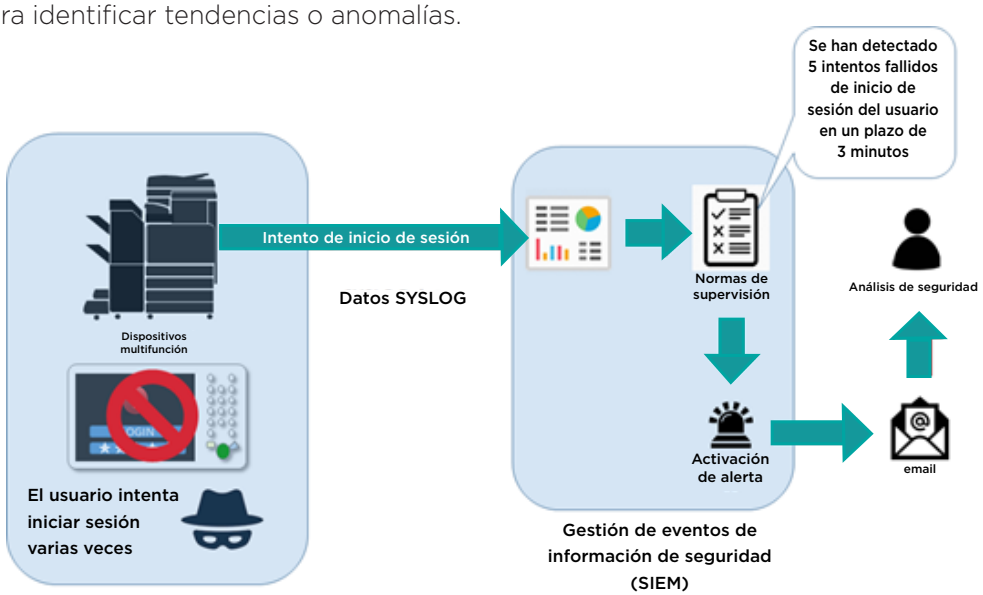



**Figura 8** Ejemplo de uso de datos de Syslog de imageRUNNER ADVANCE

Para consultar la lista de objetivos operativos SIEM, introduce el siguiente enlace en el navegador web y descarga **«SIEM_spec (imageRUNNER ADVANCE)»**.
https://www.canon-europe.com/support/product-specific-security-measures/

## Gestión de registros de dispositivo

Además de la funcionalidad Syslog proporcionada a partir de la versión 3.8 de la plataforma de software del sistema, imageRUNNER ADVANCE dispone de los siguientes registros que se pueden gestionar en el dispositivo. Estos registros se pueden exportar en formato de archivo CSV a través de la interfaz de usuario remoto (RUI).

**Tabla 3** Ejemplos de archivos de registro que puede gestionar el dispositivo multifunción.

| Tipo de registro | Número indicado como «Tipo de registro» en el archivo CSV | Descripción |
|---|---|---|
| Registro | 4098 | Este registro contiene información relacionada con el estado de autenticación del usuario (inicio/cierre de sesión y autenticación de usuario correcta/incorrecta), el registro/cambio/eliminación de información de usuario gestionada con autenticación de usuario y la gestión (adición/edición/eliminación) de roles con el SISTEMA DE GESTIÓN DE ACCESO |
| Registro de trabajos | 1001 | Este registro contiene información relacionada con la finalización de trabajos de copia/fax/escaneado/envío/impresión |
| Registro de transmisión | 8193 | El registro contiene información relacionada con las transmisiones |
| Registro de ahorro de espacio avanzado | 8196 | Este registro contiene información relacionada con el almacenamiento de archivos en el espacio avanzado, la red (espacio avanzado de otros equipos) y los soportes de memoria |
| Registro de operaciones de buzón de correo | 8197 | Este registro contiene información relacionada con las operaciones realizadas en los datos del buzón de correo, la bandeja de entrada de recepción (RX) de memoria y la bandeja de entrada de fax confidencial |
| Registro de autenticación de buzón de correo | 8199 | Este registro contiene información relacionada con el estado de autenticación del buzón de correo, la bandeja de entrada de recepción de memoria y la bandeja de entrada de fax confidencial |
| Registro de operaciones de espacio avanzado | 8201 | Este registro contiene información relacionada con las operaciones de datos en el espacio avanzado |
| Registro de gestión de la máquina | 8198 | Este registro contiene información relacionada con el arranque/apagado del equipo, los cambios realizados en la configuración mediante (Configuración/Registro), los cambios realizados en la configuración mediante la función de Entrega de información del dispositivo, y la configuración de la hora. El registro de gestión de la máquina también registra los cambios en la información del usuario o en los ajustes relacionados con la seguridad cuando el distribuidor local autorizado de Canon inspeccione o repare la máquina |
| Registro de autenticación de red | 8200 | Este registro se almacena cuando falla la comunicación IPSec |
| Exportar/importar todos los registros | 8202 | Este registro contiene información relacionada con la importación/exportación de la configuración mediante la función Exportar todo/Importar todo |
| Registro de copia de seguridad de buzón de correo | 8203 | Este registro contiene información relacionada con las copias de seguridad de los datos de las bandejas de entrada de usuario, la bandeja de entrada de recepción de memoria, la bandeja de entrada de fax confidencial y el espacio avanzado, así como los datos retenidos y el formulario registrado para la función Superponer imágenes |
| Registro de operaciones de la pantalla de gestión de aplicaciones/software | 3101 | Se trata de un registro de operaciones para SMS (Service Management Service, servicio de gestión de servicios), actualizaciones/registro de software e instaladores de aplicaciones MEAP, entre otras |
| Registro de políticas de seguridad | 8204 | Este registro contiene información relacionada con el estado de configuración de la configuración de la política de seguridad |
| Registro de administración de grupos | 8205 | Este registro contiene información relacionada con el estado de configuración (registro, edición y eliminación) de los grupos de usuarios |
| Registro de mantenimiento del sistema | 8206 | Este registro contiene información relacionada con las actualizaciones de firmware y la copia de seguridad/restauración de la aplicación MEAP, etc. |
| Registro de autenticación de impresión | 8207 | Este registro contiene información y el historial de operaciones relacionados con los trabajos de impresión retenida forzada |
| Registro de sincronización de configuración | 8208 | Este registro contiene información relacionada con la sincronización de la configuración de la máquina. Sincronización de la configuración de varias impresoras multifunción Canon |
| Registro de gestión de registros de auditoría | 3001 | Este registro contiene información relacionada con el inicio y el final de esta función (la función de gestión de registros de auditoría), así como la exportación de registros, entre otros aspectos |

Los registros pueden contener hasta 40 000 entradas. Una vez que el número de entradas supera las 40 000, se empiezan a borrar entradas empezando por las más antiguas.

# COMPATIBILIDAD CON DISPOSITIVOS REMOTOS

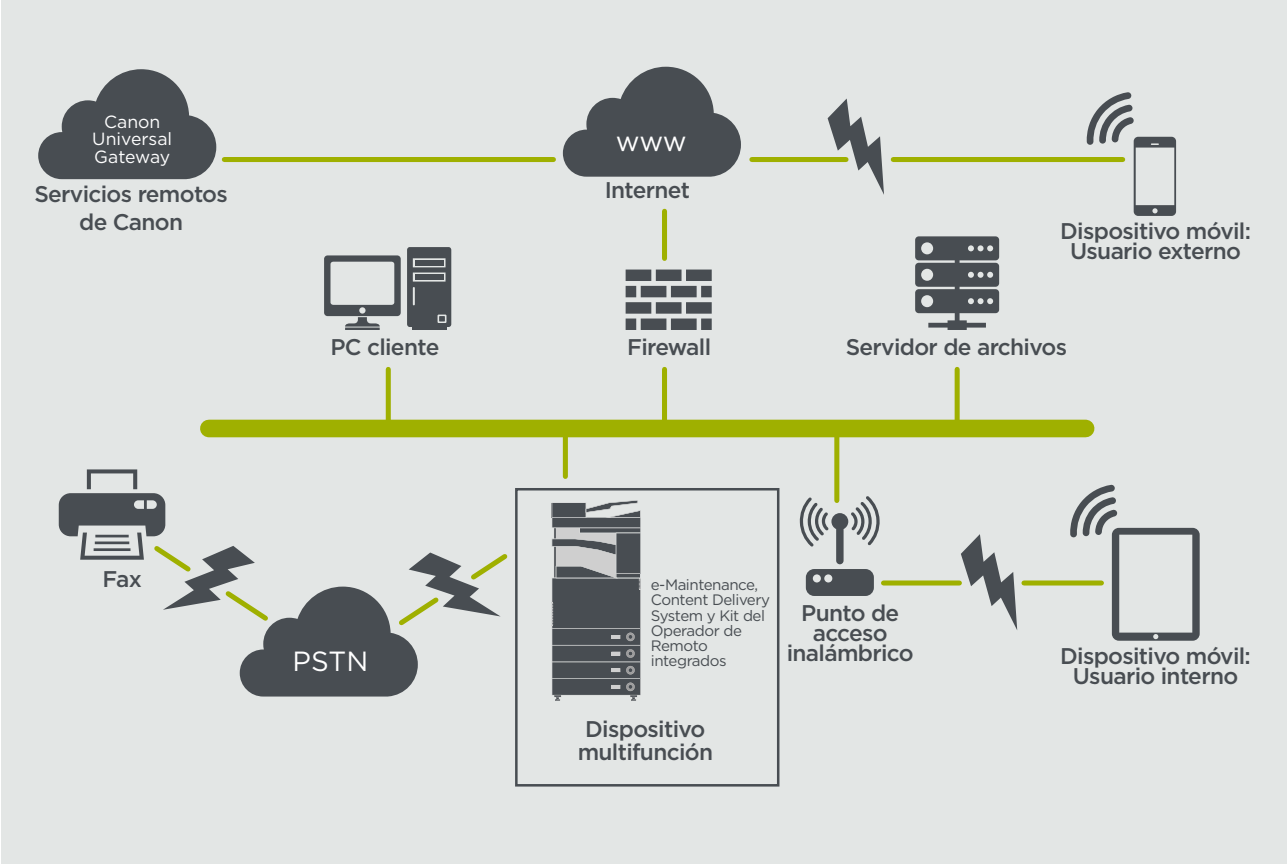
Para que Canon o alguno de sus Partners autorizados pueda prestar un servicio eficiente, la gama imageRUNNER ADVANCE es capaz de transmitir datos de mantenimiento, además de recibir actualizaciones de firmware o aplicaciones de software. Hay que tener en cuenta que no se envían imágenes ni metadatos de imágenes.

Debajo puedes ver dos posibles implantaciones de los Servicios Remotos de Canon dentro de la red de una empresa.

## Entorno de implementación 1: Conexión dispersa

En este entorno, cada dispositivo multifunción permite una conexión directa con el servicio remoto a través de Internet.

**Figura 9** Conexión dispersa




## Entorno de implementación 2: Conexión gestionada centralizada

En un entorno de gran empresa, con varios dispositivos multifunción instalados, es necesario gestionar estos dispositivos de forma eficaz desde un punto central y esto incluye la conexión a los servicios remotos de Canon. Para facilitar un enfoque de gestión integral, cada dispositivo establecería conexiones de administración a través de un solo punto de conexión de iW Management Console (iWMC). Para la comunicación entre el complemento DFU (actualización de firmware de dispositivo) y los dispositivos multifunción se usa el puerto UDP 47545.

**Figura 10** Conexión gestionada centralizada

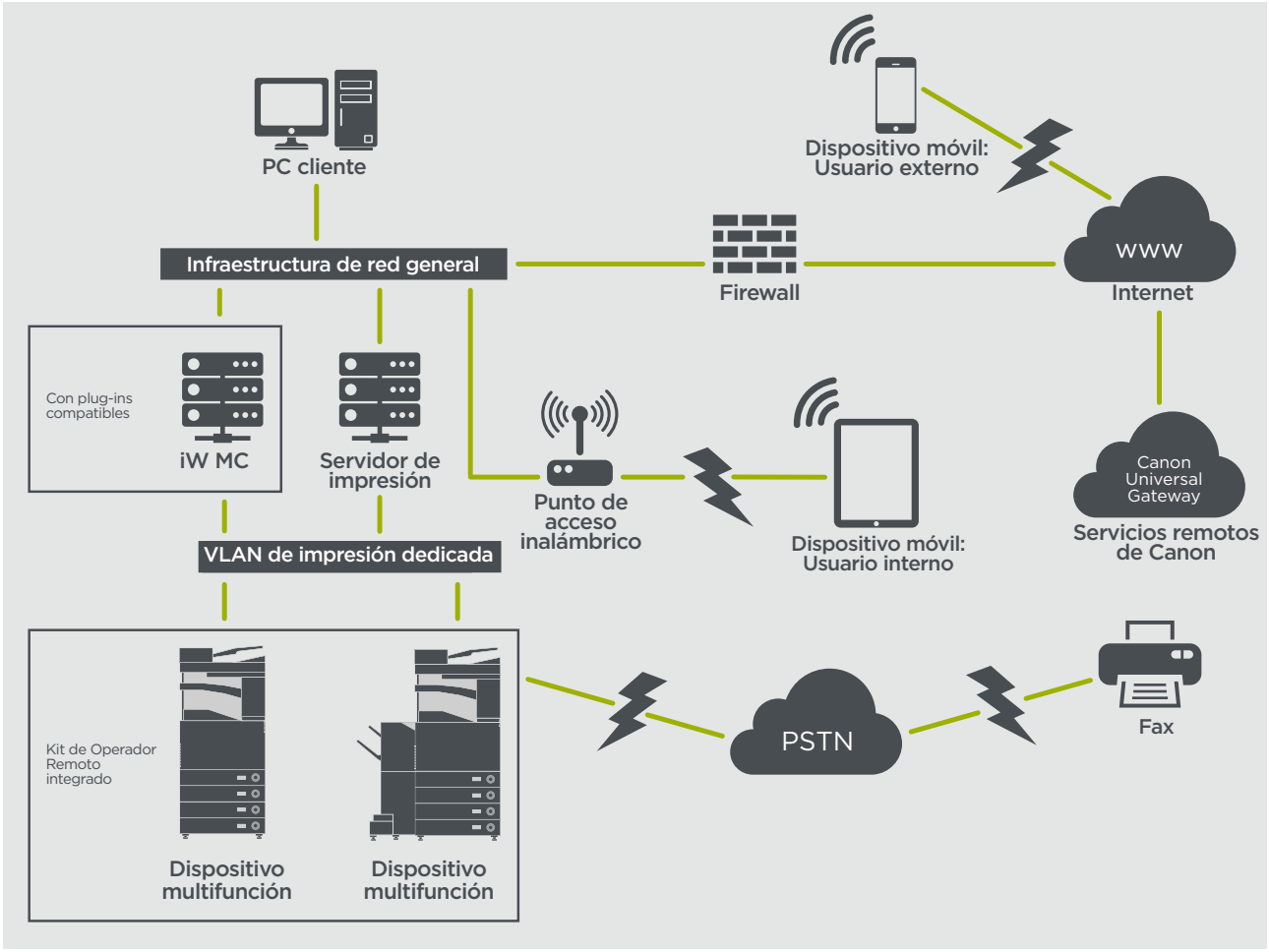



**Figura**
**11a.** Lista de dispositivos (en este caso un solo dispositivo) según se ha notificado en la consola de gestión imageWARE y
**11b.** Datos y parámetros del dispositivo

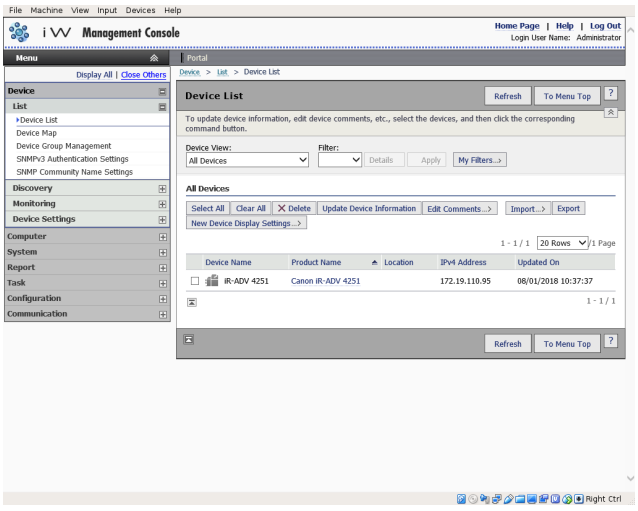



**Figura 11a**

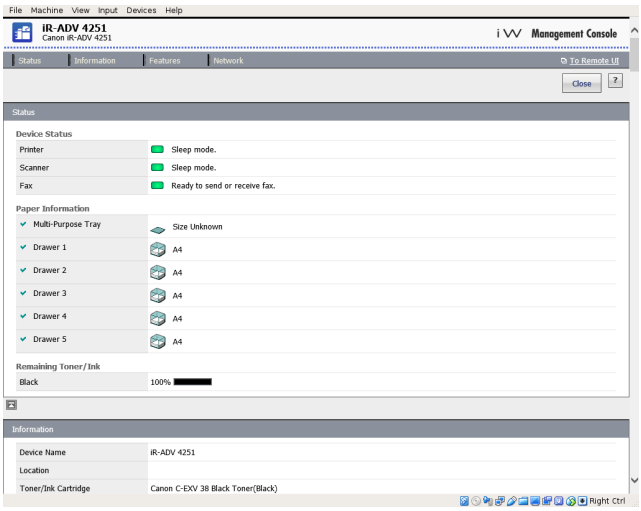



**Figura 11b**

## e-Maintenance

El sistema e-Maintenance ofrece un modo automatizado de recopilar los contadores de consumo del dispositivo para fines de facturación, llevar a cabo la gestión de los consumibles y la supervisión remota del dispositivo mediante alertas de estado y error.

El sistema e-Maintenance está compuesto por un servidor con conexión a Internet (UGW) y un software del dispositivo multifuncional integrado (eRDS) o software basado en servidor (complemento RDS) adicional para recopilar la información sobre mantenimiento del dispositivo. eRDS es un programa de supervisión que se ejecuta dentro de imageRUNNER ADVANCE. Si la opción de supervisión está activada en los ajustes del dispositivo, eRDS obtiene su propia información sobre el dispositivo y la envía al servidor UGW. El complemento RDS es un programa de supervisión que se instala en un PC general y puede supervisar entre 1 y 3000 dispositivos. Obtiene información de cada dispositivo a través de la red y la envía al servidor UGW.

En la tabla 4 se describen los datos transferidos, los protocolos (depende de las opciones seleccionadas durante el diseño y la implantación) y los puertos usados. En ningún momento se transfiere datos de imagen de copia, impresión, escaneado o fax.

**Tabla 4** Descripción de los datos de e-Maintenance

| Descripción | Datos manipulados | Protocolo/Puerto | Puerto |
|---|---|---|---|
| Comunicación entre eMaintenance (complemento RDS o eRDS) y UGW | Dirección de servicio web UGW<br>Dirección de servidor proxy/número de puerto<br>Cuenta/contraseña de proxy<br>Dirección de destino de correo UGW<br>Dirección de servidor SMTP<br>Dirección de servidor POP<br>Información sobre el estado del dispositivo, contador y modelo<br>Número de serie<br>Información sobre tinta/tóner restante<br>Información sobre firmware<br>Información de solicitudes de reparación<br>Información de registro<br>Llamada de servicio<br>Alarma de servicio<br>Atasco<br>Medioambiente<br>Registro de condición | HTTP/HTTPS/SMTP/POP3 | TCP/80 TCP/443 TCP/25 TCP/110 |
| Comunicación entre eMaintenance y el dispositivo (solo el complemento RDS, puesto que el software eRDS está integrado) | | SNMP<br>Propio de Canon<br>SLP/SLP/HTTPS | UDP/161 TCP/47546,<br>UDP/47545, TCP9007 UDP/427<br>UDP/11427 TCP/443 |

## Content Delivery System

Content Delivery System (CDS) crea una conexión entre el dispositivo multifunción y Canon Universal Gateway (UGW). Proporciona actualizaciones de aplicaciones y del firmware del dispositivo.

**Tabla 5** Descripción de los datos de Content Delivery System

| Descripción | Datos enviados | Protocolo/Puerto | Puerto |
|---|---|---|---|
| Comunicación entre el dispositivo multifunción y UGW | Número de serie del dispositivo<br>Versión de firmware<br>Idioma<br>País<br>Información sobre el CLUF del dispositivo | HTTP/HTTPS | TCP/80<br>TCP/443 |
| Comunicación entre UGW y el dispositivo multifunción | Archivo de prueba (datos aleatorios binarios) para la prueba de comunicación<br><br>Datos binarios de aplicación MEAP o firmware | HTTP/HTTPS | TCP/80<br>TCP/443 |

Se predefine una dirección URL de acceso a CDS específica en la configuración del dispositivo. Si es necesario ofrecer administración centralizada de aplicaciones y firmware del dispositivo desde dentro de la infraestructura, será necesaria una instalación local de iWMC con el complemento de actualización de firmware del dispositivo (DFU) y el complemento de gestión de aplicaciones del dispositivo.

## Software de Operador Remoto:

El Software de Operador Remoto (RSOK) ofrece acceso remoto al panel de control del dispositivo. Este sistema servidor-cliente está compuesto por un servidor VNC que se ejecuta en el dispositivo multifunción y la aplicación cliente de Microsoft Windows Remote Operation Viewer VNC.

**Figura 12** Configuración del kit del operador de asistencia remota (RSOK)

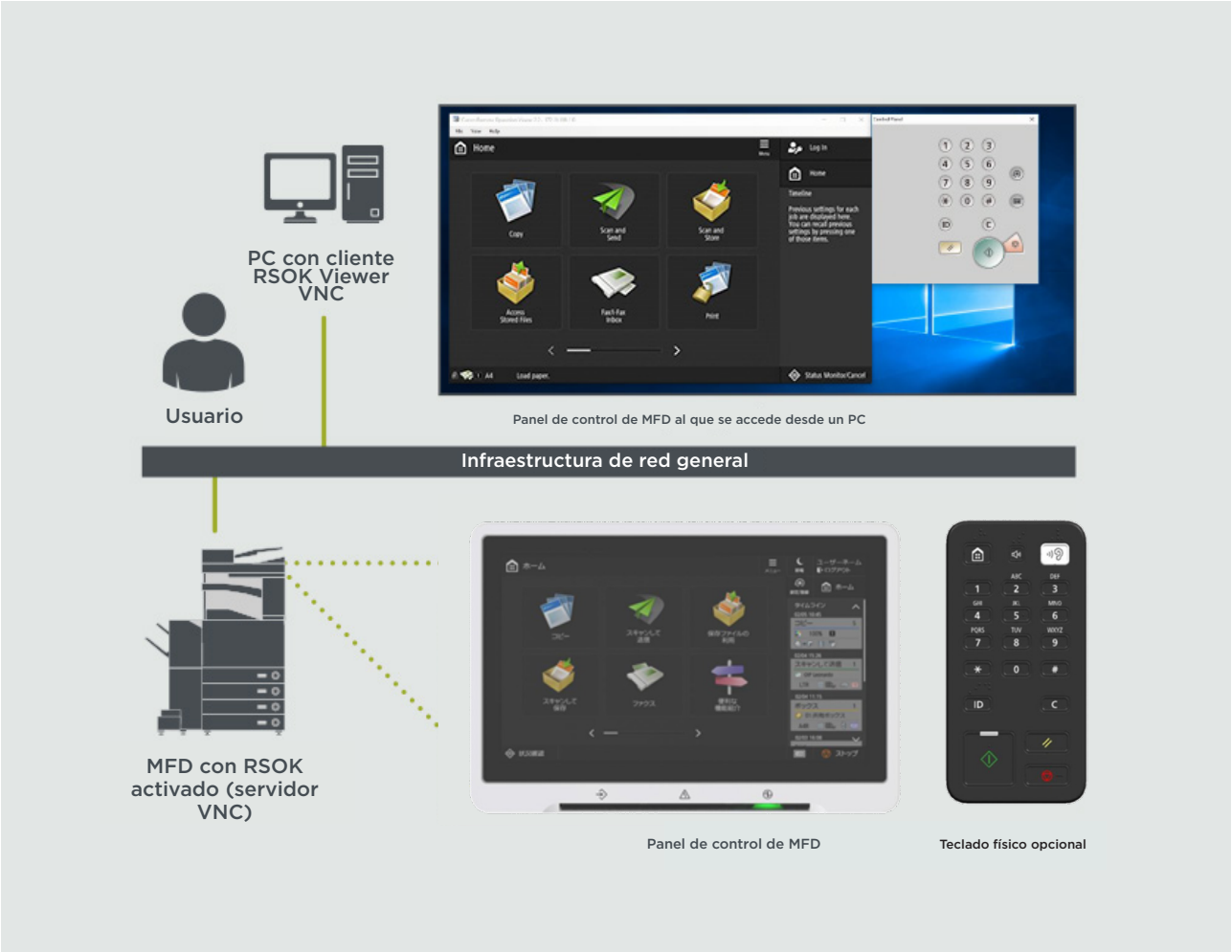



**Figura 6** Descripción de los datos del kit del operador de asistencia remota

| Descripción | Datos enviados | Protocolo/Puerto | Puerto |
|---|---|---|---|
| Autenticación de contraseña de VNC | Contraseña de usuario | Cifrado<br>DES | 5900 |
| Visor de operaciones | Panel de control del dispositivo<br>- datos de pantalla<br>- funcionamiento de teclas de hardware | Versión<br>RFB versión 3.3 | 5900 |

# APÉNDICE

## Funciones de seguridad de Canon imageRUNNER ADVANCE

La plataforma imageRUNNER ADVANCE ofrece configuración remota mediante una interfaz de servicios web conocida como interfaz de usuario remota (RUI). Esta inferfaz ofrece acceso a muchos de los parámetros de configuración del dispositivo y se puede desactivar si así se requiere y proteger mediante contraseña para impedir el acceso no autorizado.

Aunque la mayoría de los parámetros del dispositivo están disponibles a través de la IU remota, hay que usar el panel de control del dispositivo para configurar elementos que no se pueden definir con esta interfaz. Nuestra recomendación es desactivar cualquier servicio que no se utilice y ajustar los controles en aquellos que sean necesarios. Para ofrecer flexibilidad y asistencia, el Software de Operador Remoto (RSOK) ofrece acceso remoto al panel de control del dispositivo. Este acceso se basa en la tecnología VNC compuesta por un servidor (el dispositivo multifunción) y un cliente (un PC de red). Hay disponible un visor de PC cliente de Canon que permite simular el acceso a las teclas del panel de control cuando se requiera.

Esta sección incluye una descripción general de las principales funciones de seguridad de imageRUNNER ADVANCE y sus parámetros de configuración.

Encontrarás los manuales del usuario interactivos en línea en https://oip.manual.canon/, con detalles que van más allá de las funciones relacionadas con la seguridad. Comienza seleccionando el tipo de producto apropiado (por ejemplo, imageRUNNER ADVANCE DX), haz clic en el icono de búsqueda e introduce tus criterios de búsqueda. A continuación, se presentan algunas áreas generales que merece la pena tener en cuenta.

### Gestión del dispositivo

Para reducir el filtrado de información personal o su uso no autorizado se requieren medidas de seguridad constantes y eficaces. Los parámetros de seguridad y la administración de usuarios se pueden restringir solo a las personas autorizadas mediante la designación de un administrador que gestione la configuración del dispositivo.

Introduzca el siguiente enlace en su navegador web y escriba **configuración del administrador** en el cuadro de búsqueda. Accederá a información relacionada con:

- La gestión básica del dispositivo
- La limitación de riesgos por negligencia, error o uso indebido por parte de los usuarios
- La administración de dispositivos
- La gestión de la configuración y los ajustes del sistema

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

### Norma IEEE P2600

Varios modelos de imageRUNNER ADVANCE cumplen con la norma IEEE P2600, que es una norma de seguridad de la información global para los periféricos e impresoras multifunción.

En el siguiente enlace se describen los requisitos de seguridad definidos en la norma IEEE 2600 y cómo cumplen estos requisitos las funciones del dispositivo.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

### Autenticación IEEE 802.1X

Si es necesario conectar con una red 802.1X, el dispositivo debe autenticarse para garantizar que se trata de una conexión autorizada.

Introduzca el siguiente enlace en su navegador web y escriba **802.1X** en el cuadro de búsqueda.
https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

**Aplicación de una política de seguridad al dispositivo**

Los últimos modelos de imageRUNNER ADVANCE permiten la gestión de distintos ajustes de seguridad del dispositivo (la política de seguridad) por lotes mediante la IU remota. Se puede usar una contraseña independiente para permitir solo al administrador de seguridad modificar los parámetros.

Introduzca el siguiente enlace en su navegador web y escriba **Aplicación de una política de seguridad al dispositivo** en el cuadro de búsqueda. Accederá a información relacionada con:

- Cómo usar una contraseña para proteger los parámetros de la política de seguridad
- Cómo configurar los parámetros de la política de seguridad
- Los valores de configuración de la política de seguridad

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

**Gestión de los usuarios**

Los clientes que necesitan un mayor nivel de seguridad y eficiencia pueden utilizar la funcionalidad incorporada o usar una solución de administración de impresión como uniFLOW.

Para obtener más información sobre nuestras soluciones de administración de impresión, es posible contactar a nuestros representantes locales o consultar el catálogo de uniFLOW.

**Configuración de los parámetros de seguridad de la red**

Los usuarios autorizados pueden sufrir pérdidas inesperadas debido a aataques maliciosos de terceros  como la captura de información, la suplantación de identidad y la manipulación de datos a medida que se transmiten por una red. Para proteger su información de estos ataques, el dispositivo admite varias funciones que mejoran la seguridad y la privacidad.

Introduzca el siguiente enlace en su navegador web y escriba **Configuración de los parámetros de seguridad de la red** en el cuadro de búsqueda. Accederá a información relacionada con:

En el siguiente enlace se explica:

•Evitar el acceso no autorizado

•Conectarse a una red LAN inalámbrica

•Configurar el entorno de red

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

**Gestión de datos del disco duro/unidad de estado sólido**

El disco duro del dispositivo se utiliza para almacenar el sistema operativo del dispositivo, los parámetros de configuración y la información de los trabajos. La mayoría de los modelos de dispositivos ofrecen cifrado de disco completo (conforme con FIPS 140-2) emparejado con el dispositivo específico para impedir que lo lean usuarios no autorizados. Un chip de seguridad preliminar Canon MFP Security Chip está certificado como módulo criptográfico en el programa de validación de módulos criptográficos (CMVP) establecido por EE. UU. y Canadá, así como también el Programa de validación de módulos criptográficos de Japón (JCMVP).

Introduzca el siguiente enlace en su navegador web y escriba **Gestión de los datos del disco duro** en el cuadro de búsqueda.
https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

Para obtener información relacionada con la limpieza de datos con productos que utilizan la tecnología SSD, introduce el siguiente enlace en el navegador web y escribe **Inicializar todos los datos** en el cuadro de búsqueda.
https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

# DESCRIPCIÓN DE LOS PARÁMETROS DE CONFIGURACIÓN DE LA POLÍTICA DE SEGURIDAD

Los modelos de la tercera generación de imageRUNNER ADVANCE introducen la configuración de la política de seguridad y el usuario de administración de seguridad. Para esto es necesario un inicio de sesión correcto por parte del administrador y, si está configurado, un inicio de sesión del administrador de seguridad adicional con otra contraseña.

En la siguiente tabla se describen los parámetros disponibles.

| 1. Interfaz | Notas |
|---|---|
| **Política de conexión inalámbrica** | |
| Prohibir el uso de conexión directa | La opción <Use Wi-Fi Direct> (Usar Wi-Fi Direct) está definida en <Off> (desactivada)<br>No se puede acceder a la máquina desde dispositivos móviles |
| Prohibir el uso de LAN inalámbrica | La opción <Select Wired/Wireless LAN> (Seleccionar LAN cableada/inalámbrica) está definida en <Wired LAN> (LAN cableada)<br>No se puede establecer una conexión inalámbrica con el dispositivo mediante un router LAN o punto de acceso inalámbrico |
| **Política de USB** | |
| Prohibir el uso como dispositivo USB | La opción <Use as USB Device> (Usar como dispositivo USB) está definida en <Off> (desactivada)<br>Si está prohibido el uso como dispositivo USB, no se podrán usar las funciones de impresión o escaneado desde PCs conectados mediante USB. |
| Prohibir el uso como dispositivo de almacenamiento USB | La opción <Use USB Storage Device> (Usar como dispositivo de almacenamiento USB) está establecida en <Off> (desactivada)<br>No se pueden usar dispositivos de almacenamiento USB.<br>No obstante, las siguientes funciones de mantenimiento seguirán funcionando incluso si la opción "Prohibit use as USB Storage Device" (Prohibir el uso como dispositivo de almacenamiento USB) está definida en <On> (activada)<br>• Actualización de firmware mediante dispositivo de memoria USB (desde el modo descargar)<br>• Copia de los datos del subregistro desde el dispositivo a USB (LOG2USB)<br>• Copia del informe desde el dispositivo a la memoria USB (RPT2USB) |
| **Política operativa de comunicación en red**<br>Nota: Estos parámetros no son aplicables a la comunicación con redes IEEE 802.1x, incluso si se ha seleccionado la casilla para la opción [Comprobar siempre el certificado del servidor al usar TLS] | |
| Comprobar siempre firmas para las funciones de servidor SMS/WebDAV | En <SMB Server Settings> (Parámetros de servidor SMB), las opciones <Require SMB Signature for Connection> (Pedir firma SMB para conexión) y <Use SMB Authentication> (Usar autenticación SMB) están definidas en <On> (activada), y <Use TLS> (usar TLS) en <WebDAV Server Settings> (Parámetros de servidor WebDAV) está definida en <On> (activada)<br>Cuando el dispositivo se usa como servidor SMB o WebDAV, se verifican las firmas de certificado digital durante la comunicación |
| Comprobar siempre el certificado de servidor al usar TLS | Las opciones <Confirm TLS Certificate for WebDAV TX> (Confirmar certificado TLS para WebDAV TX, <Confirm TLS Certificate for SMTP TX> (Confirmar certificado TLS para SMTP TX), <Confirm TLS Certificate for POP RX> (Confirmar certificado TLS para POP RX), <Confirm TLS Certificate for Network Access> (Confirmar certificado TLS para acceso de red) y <Confirm TLS Certificate Using MEAP Application> (Confirmar certificado TLS al usar la aplicación MEAP) están definidas en <On> (activada) y se añade una marca de verificación a la casilla <CN><br>Asimismo, las opciones <Verify Server Certificate> (Comprobar el certificado del servidor) y <Verify CN> (Verificar CN) en <SIP Settings> (Parámetros SIP) > <TLS Settings> (Parámetros TLS) están definidas en <On> (activadas)<br>Durante la comunicación TLS se realiza la verificación para los certificados digitales y sus nombres comunes |
| Prohibir la autenticación de texto sin cifrar para funciones de servidor | • La opción <Use FTP Printing> (Usar impresión FTP) en <FTP Print Settings> (Configuración de impresión FTP) está definida en <Off> (desactivada).<br>• La opción <Allow TLS (SMTP RX)> (Permitir TLS (SMTP RX)) en <E-Mail/I-Fax Settings> (Configuración de correo electrónico/I-Fax) <Communication Settings> (Parámetros de comunicación) está definida en <Always TLS> (TLS siempre), <Dedicated Port Authentication Method> (Método de autenticación de puerto dedicado) en <Network> (Red) está definida en <Mode 2> (Modo 2),<br>• La opción <Use TLS> (Usar TLS) en <WebDAV Server Settings> (Parámetros de servidor WebDAV) está definida en <On> (activada)<br>Al usar el dispositivo como servidor, no están disponibles las funciones que usan autenticación de texto plano<br>Si está prohibida la autenticación de texto sin cifrar, se usará TLS. Asimismo, no se podrán usar funciones de servidor o aplicaciones, como FTP, que solo admiten autenticación de texto sin cifrar<br>Es posible que no se pueda tener acceso al dispositivo desde el controlador o software de administración del dispositivo |
| Prohibir uso de SNMPv1 | En la opción <SNMP Settings> (Configuración de SNMP), <Use SNMPv1> (Usar SNMPv1) está definida en <Off> (desactivada)<br>Si está prohibido el uso de SNMPv1, es posible que no se pueda recuperar o configurar la información del dispositivo desde el controlador de impresora o software de administración. |
| **Política de uso de puertos** | |
| Restringir el puerto LPD | Número de puerto: 515<br>La opción <LPD Print Settings> (Parámetros de impresión LPD) está definida en <Off> (desactivada)<br>No se puede imprimir con LPD |
| Restringir el puerto RAW | Puerto número 9100<br>La opción <RAW Print Settings> (Parámetros de impresión RAW) está definida en <Off> (desactivada)<br>No se puede imprimir en RAW |
| Restringir el puerto FTP | Puerto número 21<br>En la opción <FTP Print Settings> (Configuración de impresión FTP), la opción <Use FTP Printing> (Usar impresión FTP) está definida en <Off> (desactivada)<br>No se puede imprimir en FTP |
| Restringir el puerto WSD | Puerto número 3702, 60000<br>En la opción <WSD Settings> (Parámetros WSD), las opciones <Use WSD> (Usar WSD), <Use WSD Browsing> (Usar navegación WSD) y <Use WSD Scan> (Usar escaneado WSD) están definidas en <Off> (desactivada)<br>No se pueden usar las funciones WSD |

| | |
|---|---|
| Restringir el puerto BMLinkS | Puerto número 1900<br>No se usa en Europa |
| Restringir el puerto IPP | Puerto número 631<br>Si el puerto IPP está restringido, no se podrán usar Mopria, AirPrint ni IPP |
| Restringir el puerto SMB | Número de puerto: 137, 138, 139, 445<br>En la opción <SMB Server Settings> (Parámetros de servidor SMB), la opción <Use SMB Server> (Usar servidor SMB) está definida en <Off> (desactivada)<br>No se puede usar el dispositivo como servidor SMB |
| Restringir el puerto SMTP | Puerto número 25<br>En la opción <E-Mail/I-Fax Settings (Parámetros de correo electrónico/I-Fax)> > <Communication Settings> (Parámetros de comunicación), la opción <SMTP RX> está definida en <Off> (desactivada)<br>La recepción SMTP no es posible |
| Restringir el puerto dedicado | Número de puerto: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545-47547<br>Si el puerto dedicado está restringido, no se podrán usar las funciones o aplicaciones de copia remota, fax remoto, escaneado remoto, impresión remota, etc. |
| Restringir el puerto de software del operador remoto | Puerto número 5900<br>La opción <Remote Operation Settings> (Parámetros de funcionamiento remoto) está definida en <Off> (desactivada).<br>No se pueden usar las funciones de funcionamiento remoto. |
| Restringir el puerto SIP (Fax IP) | Número de puerto: 5004, 5005, 5060, 5061, 49152<br>Las opciones <Use Intranet> (Usar intranet) en <Intranet Settings> (Configuración de intranet), <Use NGN> (Usar NGN) en <NGN Settings> (Configuración de NGN9) y <Use VoIP Gateway> (Usar puerta de enlace VoIP) en <VoIP Gateway Settings> (Configuración de puerta de enlace VoIP) están definidas en <Off> (desactivadas)<br>No se puede usar fax IP |
| Restringir el puerto mDNS | Puerto número 5353<br>En <mDNS Settings> (Configuración de mDNS), las opciones <Use IPv4 mDNS> (Usar IPv4 mDNS) y <Use IPv6 mDNS> (Usar IPv6 mDNS) están definidas en <Off> (desactivadas).<br>La opción <Use Mopria> (Usar Mopria) está definida en <Off> (apagada)<br>No es posible buscar en la red ni realizar ajustes automáticos mediante mDNS. Tampoco es posible imprimir con Mopria™ o AirPrint |
| Restringir el puerto SLP | Puerto número 427<br>En <Multicast Discovery Settings> (Parámetros de detección multidifusión), la opción <Response> (Respuesta) está definida en <Off> (desactivada)<br>No se puede buscar la red o hacer ajustes automáticos con SLP |
| Restringir el puerto SNMP | Puerto número 161<br>Si está restringido el puerto SNMP, es posible que no se pueda recuperar o configurar la información del dispositivo desde el controlador de impresora o software de administración.<br>En <SNMP Settings> (Configuración de SNMP), las opciones <Use SNMPv1> (Usar SNMPv1) y <Use SNMPv3> (Usar SNMPv3) están definidas en <Off> (desactivadas). |

| 2. Autenticación | Notas |
|---|---|
| **Política operativa de autenticación** | |
| Prohibir los usuarios invitados | • La opción <Advanced Space Settings> > <Authentication Management> (Configuración de espacio avanzado > > Administración de autenticación) está definida en <On> (activada).<br>• La opción <Login Screen Display Settings> (Parámetros de pantalla de inicio de sesión) está definida en <Display When Device Operation Starts> (Mostrar cuando se inicie el funcionamiento del dispositivo)<br>• La opción <Restrict Job from Remote Device without User Auth.> (Restringir trabajo desde dispositivo remoto sin autorización de usuario) está definida en <On> (activada)<br>No es posible que los usuarios no registrados inicien sesión en el equipo. Los trabajos de impresión enviados desde un ordenador también se cancelan |
| Forzar parámetro de cierre de sesión automático | Esta configuración sirve para cerrar sesión desde el panel de control. Esto no se aplica a otros métodos de cierre de sesión (intervalo ajustable de 10 segundos a 9 minutos).<br><Auto Reset Time> (Tiempo de reinicio automático) está activado. El usuario cierra la sesión automáticamente si no se realiza ninguna operación durante un periodo de tiempo especificado<br>En la pantalla de configuración de IU remota, seleccione la opción [Time Until Logout] (Tiempo para cerrar sesión) |
| **Política operativa de contraseñas** | |
| Prohibir el almacenamiento de contraseñas en memoria caché para servidores externos | Este parámetro no se aplica a las contraseñas que guarda explícitamente el usuario, por ejemplo, contraseñas para libretas de direcciones, etc.<br>La opción <Prohibit Caching of Authentication Password> (Prohibir el almacenamiento de contraseñas de autenticación en memoria caché) está definida en <On> (activada)<br>Los usuarios deberán introducir una contraseña para acceder a un servidor externo siempre |
| Mostrar aviso cuando se esté usando la contraseña predeterminada | La opción <Display Warning When Default Password Is in Use> (Mostrar aviso cuando se esté usando la contraseña predeterminada) está definida en <On> (activada)<br>Se mostrará un mensaje de aviso cuando se use la contraseña predeterminada de fábrica del dispositivo |
| Prohibir el uso de contraseña predeterminada para acceso remoto | La opción <Allow Use of Default Password for Remote Access> (Permitir el uso de contraseña predeterminada para acceso remoto) está definida en <Off> (desactivada)<br>No se puede usar la contraseña predeterminada de fábrica al acceder al dispositivo desde un ordenador |
| **Política de configuración de contraseñas (la política no será aplicable a la administración de id. de departamento o PIN)** | |
| Definir el número mínimo de caracteres para la contraseña | El número mínimo de caracteres se puede configurar entre 1 y 32 |
| Definir el periodo de validez de la contraseña | El periodo de validez se puede configurar entre 1 y 180 días |
| Prohibir el uso de 3 o más caracteres consecutivos idénticos | |
| Forzar el uso de un carácter en mayúscula como mínimo | |
| Forzar el uso de un carácter en minúscula como mínimo | |
| Forzar el uso de un carácter numérico como mínimo | |
| Forzar el uso de un símbolo como mínimo | |
| **Política de bloqueo** | |
| Activar bloqueo | No es aplicable a la autenticación de id. de departamento/PIN de buzón de correo, autenticación de PIN o impresión segura, etc.<br>Umbral de bloqueo: ajustable entre 1 y 10 veces<br>Periodo de bloqueo: ajustable entre 1 y 60 minutos |

| 3. Clave/Certificado | Notas |
|---|---|
| Prohibir el uso de cifrado débil | Aplicable a IPSec, TLS, Kerberos, S/MIME, SNMPv3 y LAN inalámbrica<br>Es posible que no se pueda comunicar con dispositivos que solo admitan cifrado débil |
| Prohibir el uso de clave/certificado con cifrado débil | Aplicable a IPSec, TLS y S/MIME<br>Si usa una clave/certificado con cifrado débil para TLS, se cambiará a la clave/certificado preinstalado. Si está usando una clave/certificado con cifrado débil para funciones distintas de TLS, no podrá comunicar |
| Usar TPM para almacenar contraseña y clave | Solo disponible para dispositivos con TPM instalado. Realice siempre una copia de seguridad de las claves TPM cuando TPM esté activado. Consulte el manual de usuario para obtener más información<br>Importante si los parámetros TPM están activados:<br>• Asegúrese de cambiar el valor predeterminado de la contraseña del «administrador» para impedir que un tercero pueda hacer una copia de seguridad de la clave TPM. Si un tercero toma la clave de copia de seguridad de TPM, no podrá restaurar la clave de TPM.<br>• Para que la seguridad sea mejor, solo se puede hacer una copia de seguridad de la clave de TPM una vez. Si están activados los parámetros de TPM, asegúrese de hacer una copia de seguridad de la clave TPM en un dispositivo de memoria USB y guárdelo en un lugar seguro para impedir su pérdida o robo.<br>• Las funciones de seguridad proporcionadas por TPM no garantizan la protección completa de los datos y el hardware. |

| 4. Registro | Notas |
|---|---|
| Forzar la grabación del registro de auditoría | • La opción <Save Operation Log> (Guardar registro de operaciones) está definida en <On> (activada).<br>• La opción <Display Job Log> (Mostrar registro de trabajos) está definida en <On> (activada).<br>• La opción <Retrieve Job Log with Management Software> (Recuperar registro de trabajos con software de administración) en <Display Job Log> (Mostrar registro de trabajos) está definida en <Allow> (Permitir)<br>• La opción <Save Audit Log> (Guardar registro de auditoría) está definida en <On> (activada).<br>• La opción <Retrieve Network Authentication Log> (Recuperar registro de autenticación de red) está definida en <On> (activada).<br>Si este parámetro está activado, se graban siempre los registros de auditoría. |
| Forzar parámetros de SNTP | Introduzca la dirección del servidor SNTP<br>En <SNTP Settings> (Configuración de SNTP), la opción <Use SNTP> (Usar SNTP) está establecida en <On> (Activa). Se necesita la sincronización de hora a través de SNTP. Introduzca un valor para [Server Name] (Nombre de servidor) en la pantalla de configuración de la interfaz de usuario remota |
| Informe de registros de Syslog | Habilite los detalles de destino de Syslog cuando utilice un servidor Syslog o SIEM<br>• <Nombre de usuario y contraseña><br>• <Nombre del servidor SMB><br>• <Ruta de destino><br>• <Ejecutar tiempo de exportación> |

| 5. Trabajo | Notas |
|---|---|
| **Política de impresión** | |
| Prohibir la impresión inmediata de los trabajos recibidos | Si está prohibida la impresión inmediata de los trabajos recibidos, estos se almacenarán en la memoria de fax/I-Fax<br>• La opción <Handle Files with Forwarding Errors> (Gestión de archivos con errores de reenvío) está definida en <Off> (desactivada).<br>• La opción <Use Fax Memory Lock> (Usar bloqueo de memoria de fax) está definida en <On> (activada).<br>• La opción <Use I-Fax Memory Lock> (Usar bloqueo de memoria de I-Fax) está definida en <On> (activada).<br>• La opción <Memory Lock End Time> (Hora de fin de bloqueo de memoria) está definida en <Off> (desactivada).<br>• La opción <Display Print When Storing from Printer Driver> (Mostrar impresión al guardar desde el controlador de la impresora) en <Set/Register Confidential Fax Inboxes> (Definir/registrar buzones de entrada de fax confidencial) está definida en <Off> (desactivada).<br>• La opción <Settings for All Mail Boxes (Parámetros para todos los buzones de correo)> > <Print When Storing from Printer Driver> (Imprimir al guardar desde el controlador de la impresora) está definida en <Off> (desactivada).<br>• La opción <Box Security Settings (Parámetros de seguridad de buzón)> > <Display Print When Storing from Printer Driver> (Mostrar impresión al guardar desde el controlador de la impresora) está definida en <Off> (desactivada).<br>• La opción <Prohibit Job from Unknown User> (Prohibir trabajo desde usuario desconocido) está definida en <On> (activada) y la opción <Forced Hold> (Retención forzada) está definida en <On> (activada)<br>La impresión no se produce inmediatamente, incluso cuando se llevan a cabo operaciones de impresión |
| **Política de envío/recepción** | |
| Permitir el envío solo a direcciones registradas | En la opción <Limit New Destination> (Limitar destino nuevo), las opciones <Fax>, <E-Mail> (Correo electrónico), <I-Fax> y <File> (Archivo) están definidas en <On> (activadas)<br>Solo se puede enviar a destinos que están registrados en la libreta de direcciones |
| Forzar la confirmación del número de fax | Los usuarios deben introducir un número de fax de nuevo como confirmación al enviar un fax |
| Prohibir el reenvío automático | La opción <Use Forwarding Settings> (Usar parámetros de reenvío) está definida en <Off> (desactivada)<br>No se puede reenviar faxes automáticamente |

| 6. Almacenamiento | Notas |
|---|---|
| Forzar el borrado completo de los datos | La opción <Hard Disk Data Complete Deletion> (Borrado completo de datos de disco duro) está definida en <On> (activada). |

Consulte todas las especificaciones de imageRUNNER ADVANCE en el sitio web del producto, en https://www.canon-europe.com/business-printers-and-faxes/imagerunner-advance-dx/.

**Canon Inc.**
Canon.com

**Canon Europe**
canon.es

Spanish edition v1.0