BlackBerry UEM Cloud

Arquitectura y flujos de datos

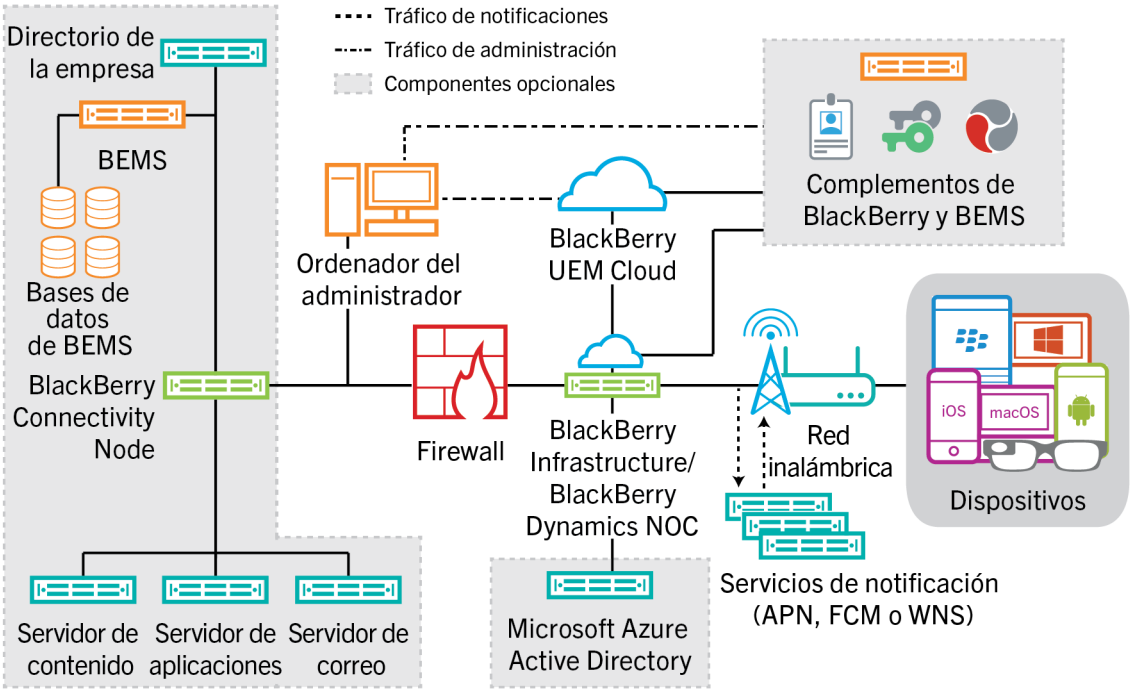
Contents

Arquitectura y flujos de datos de BlackBerry UEM Cloud

BlackBerry UEM Cloud es una solución de gestión de extremos unificada de BlackBerry. Con BlackBerry UEM Cloud puede gestionar dispositivos con iOS, macOS, Android, y Windows 10 mediante una sencilla interfaz basada en la web y proteger la información empresarial en los dispositivos BYOD, COPE y COBO.

La arquitectura de BlackBerry UEM Cloud se ha diseñado para ayudarle a administrar los dispositivos móviles de su empresa en un entorno de nube y proporcionar un enlace seguro para los datos que se desplazan entre los servidores de correo y contenido de su empresa y los dispositivos de sus usuarios.

Arquitectura: solución BlackBerry UEM Cloud



Componente	Descripción
BlackBerry UEM Cloud	BlackBerry UEM Cloud es un servicio que le permite administrar los dispositivos utilizados en el entorno de su empresa.
BlackBerry Infrastructure y BlackBerry Dynamics NOC	BlackBerry Infrastructure registra la información del usuario para la activación del dispositivo y valida la información de licencia para BlackBerry UEM Cloud. Al activar BlackBerry Secure Connect Plus o BlackBerry Secure Gateway, los datos en tránsito que utilizan estos servicios pasan a través de BlackBerry Infrastructure. BlackBerry Dynamics NOC es un NOC con ubicación independiente que ofrece comunicaciones seguras entre las aplicaciones de BlackBerry Dynamics en los dispositivos y el BlackBerry Proxy instalado detrás del firewall, como parte de BlackBerry Connectivity Node.

Componente	Descripción
Dispositivos	BlackBerry UEM Cloud es compatible con los dispositivos con iOS, macOS, Android, y Windows 10.
Servicios de notificación	BlackBerry UEM Cloud envía notificaciones a los dispositivos para que se pongan en contacto con BlackBerry UEM para obtener actualizaciones y proporcionar información para el inventario de dispositivos de la empresa. Estas notificaciones se envían a BlackBerry Infrastructure, desde donde se envían al dispositivo a través del servicio de notificación apropiado: • APN es un servicio que proporciona Apple para enviar notificaciones a los dispositivos iOS y macOS. • FCM es un servicio que proporciona Google para enviar notificaciones a los dispositivos con Android. • WNS es un servicio que proporciona Microsoft para enviar notificaciones a los dispositivos Windows 10.
BlackBerry Connectivity Node	BlackBerry Connectivity Node es un componente opcional que se puede instalar dentro del firewall de la empresa. Incluye cinco componentes que añaden funcionalidad a BlackBerry UEM Cloud: • BlackBerry Cloud Connector conecta BlackBerry UEM Cloud al directorio de la empresa detrás del firewall para permitir la sincronización de atributos básicos, la funcionalidad de búsqueda y los servicios de autenticación de usuarios. Si no instala BlackBerry Connectivity Node y el directorio de su empresa está detrás del firewall, debe crear cuentas de usuario locales en BlackBerry UEM Cloud en lugar de utilizar las cuentas de usuario del directorio de la empresa. BlackBerry Cloud Connector no es necesario para que BlackBerry UEM Cloud se conecte a Microsoft Azure Active Directory. • BlackBerry Proxy mantiene una conexión segura entre su empresa y BlackBerry Dynamics NOC, permitiendo que las aplicaciones de BlackBerry Dynamics puedan comunicarse de forma segura con los recursos de su empresa detrás del firewall. También admite BlackBerry Dynamics Direct Connect, que permite que los datos de aplicaciones omitan BlackBerry Dynamics NOC. • BlackBerry Gatekeeping Service envía los comandos a Exchange ActiveSync para agregar dispositivos a una lista de dispositivos admitidos cuando los dispositivos están activados en BlackBerry UEM Cloud. Los dispositivos no administrados que intentan conectarse a un servidor de correo de la empresa pueden ser revisados, verificados, así como bloqueados o admitidos por un administrador a través de la consola de administración de BlackBerry UEM. • BlackBerry Secure Connect Plus proporciona un túnel IP seguro entre las aplicaciones de trabajo en los dispositivos y la red de la empresa. Se establece un túnel que es compatible con datos IPv4 (TCP y UDP) estándar para cada uno de los dispositivos a través de BlackBerry Infrastructure. • BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y BlackBerry UEM Cloud al servidor de correo de su empresa para dispositivos iOS. BlackBerry Connectivity Node utiliza el puerto 3101 para comunicarse con BlackBerry UEM Cloud.

Componente	Descripción
BlackBerry Enterprise Mobility Server	Si ha instalado BlackBerry Connectivity Node, también puede instalar una versión local de BEMS. BEMS consolida varios servicios utilizados para enviar datos de trabajo hacia y desde las aplicaciones de BlackBerry Dynamics: • BlackBerry Connect proporciona mensajería instantánea, búsqueda en directorios empresariales e información de presencia de usuarios a dispositivos iOS y Android de forma segura. • BlackBerry Presence proporciona estado de presencia en tiempo real a aplicaciones de BlackBerry Dynamics. • BlackBerry Docs permite que los usuarios de aplicaciones de BlackBerry Dynamics accedan, sincronicen y compartan documentos con su servidor de archivos de trabajo, SharePoint, Box y sistemas de gestión de contenido que son compatibles con CMIS, sin necesidad de software de VPN, reconfiguración del firewall o almacenes de datos duplicados.
Bases de datos BlackBerry Enterprise Mobility Server	Las bases de datos de BEMS guardan la información de los usuarios, aplicaciones, políticas y configuraciones.
Directorio de la empresa	BlackBerry UEM Cloud admite la conectividad con Microsoft Active Directory o el directorio LDAP de la empresa detrás del firewall utilizando BlackBerry Connectivity Node.
Microsoft Azure Active Directory	Microsoft Azure Active Directory es un servicio de gestión de directorios basado en la nube. Si su empresa utiliza Azure Active Directory, puede conectarse a él en su lugar o de forma adicional a un directorio de la empresa detrás del firewall.
Contenido, aplicación y servidores de correo	Cuando se activa BlackBerry Secure Connect Plus o si los usuarios tienen aplicaciones de BlackBerry Dynamics, los dispositivos pueden conectarse a los servidores de la empresa sin tener que abrir una conexión directa entre el servidor e Internet. Los datos de trabajo en tránsito entre los servidores y los dispositivos se envían a través de BlackBerry Secure Connect Plus y de BlackBerry Infrastructure. Los datos de la aplicación de BlackBerry Dynamics se envían a través de BlackBerry Proxy y de BlackBerry Dynamics NOC. BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y BlackBerry Connectivity Node entre el servidor de correo de su empresa y los dispositivos iOS.

Componente	Descripción
Complementos de BlackBerry y BEMS	La versión en la nube de BlackBerry Enterprise Mobility Server proporciona BlackBerry Push Notifications, que acepta solicitudes de registro de inserción de dispositivos iOS y Android. A continuación, se comunica con Microsoft Exchange para supervisar si se producen cambios en la cuenta de correo de trabajo del usuario. Cuando se especifica la información del servidor Microsoft Exchange o Microsoft Office 365 local, se especifica la configuración para crear el inquilino de BEMS Cloud para su empresa. También puede integrar la versión en la nube de BEMS con BlackBerry Docs, que le permite que los usuarios de aplicaciones de BlackBerry Dynamics accedan, sincronicen y compartan documentos con su servidor de archivos de trabajo, SharePoint, Box y sistemas de gestión de contenido que son compatibles con CMIS, sin necesidad de software de VPN, reconfiguración del firewall o almacenes de datos duplicados. BlackBerry UEM Cloud funciona con productos empresariales adicionales de BlackBerry, como BlackBerry Enterprise Identity, BlackBerry 2FA y BlackBerry Workspaces, lo que le permite ampliar las capacidades de UEM en su empresa.

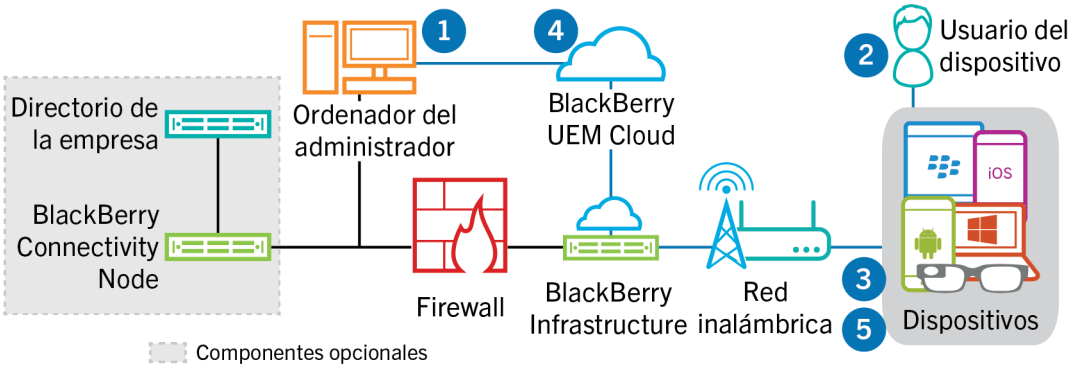
Activación de dispositivos y de las aplicaciones de BlackBerry Dynamics

Cuando un usuario activa un dispositivo con BlackBerry UEM, el dispositivo se asocia con BlackBerry UEM de modo que pueda administrar dispositivos y que los usuarios puedan acceder a los datos de trabajo desde sus dispositivos. Los tipos de activación de dispositivos ofrecen distintos grados de control sobre los datos de trabajo y los datos personales en los dispositivos, que van desde el control total sobre todos los datos al control específico únicamente de los datos de trabajo. Para obtener más información acerca de los tipos de activación, consulte "Activación de dispositivos" en el contenido de Administración.

Dependiendo del tipo de dispositivo y el tipo de activación que especifique, el dispositivo y BlackBerry UEM deben completar varios pasos durante el proceso de activación para que se autentiquen mutuamente, protejan un canal de comunicación y, si es necesario, creen un espacio de trabajo o cifren el dispositivo antes de enviar cualquier configuración y datos de trabajo al dispositivo. Para obtener más información sobre cómo activar dispositivos, consulte "Pasos para activar los dispositivos" en el contenido de Administración.

Las aplicaciones de BlackBerry Dynamics proporcionan acceso a los recursos de trabajo desde el dispositivo. Después de instalar las aplicaciones de BlackBerry Dynamics en un dispositivo, estas también deben activarse para permitir que accedan de forma segura a los recursos de trabajo. Para obtener más información sobre la activación de BlackBerry Dynamics, consulte "Generación de claves de acceso, contraseñas de activación o códigos QR para aplicaciones de BlackBerry Dynamics" en el contenido de Administración.

Flujo de datos: activación de un dispositivo con iOS, Android o Windows 10

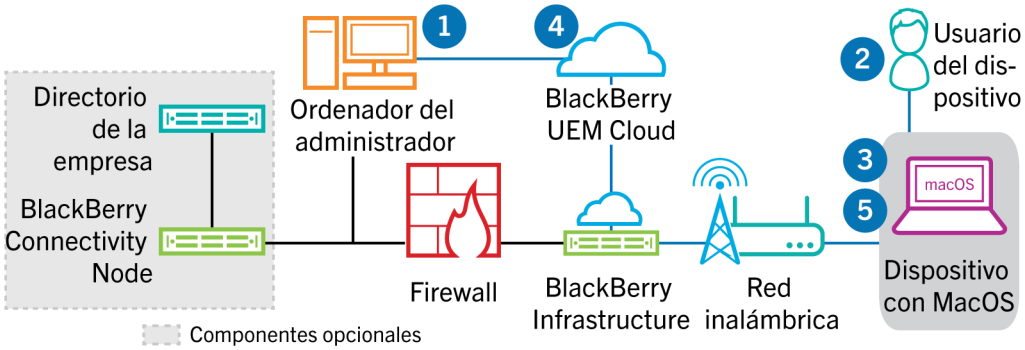


1. Lleve a cabo las acciones siguientes:
   a. Agregue un usuario a BlackBerry UEM Cloud como una cuenta de usuario local o, si ha instalado BlackBerry Connectivity Node, mediante la información de la cuenta recuperada desde el directorio de la empresa.
   b. Asigne un perfil de activación al usuario.
   c. Dependiendo del tipo de dispositivo y las preferencias de su empresa, utilice una de las siguientes opciones para suministrar los datos de activación al usuario:
      - Genere automáticamente una contraseña de activación del dispositivo y, de manera opcional, un código QR y envíe un mensaje de correo electrónico con las instrucciones de activación al usuario
      - Establezca una contraseña de activación del dispositivo, y comunique el nombre de usuario y la contraseña al usuario directamente o por correo.

- Anule la configuración de la contraseña de activación y comunique la dirección de BlackBerry UEM Self-Service al usuario para que pueda establecer su propia contraseña de activación o ver un código QR.

2. El usuario realiza las siguientes acciones:
   a. Si se activa un dispositivo con iOS o Android, se descarga e instala BlackBerry UEM Client.
   b. Introduce su nombre de usuario y la contraseña de activación o escanea el código QR en su dispositivo.
3. El dispositivo envía una solicitud de activación a BlackBerry UEM.
4. BlackBerry UEM Cloud verifica las credenciales de activación del usuario y envía los detalles de activación al dispositivo, incluida la información de configuración del dispositivo.
5. El dispositivo recibe los detalles de la activación de BlackBerry UEM Cloud y completa la configuración. A continuación, el dispositivo envía a BlackBerry UEM Cloud la confirmación de que la activación se realizó correctamente.

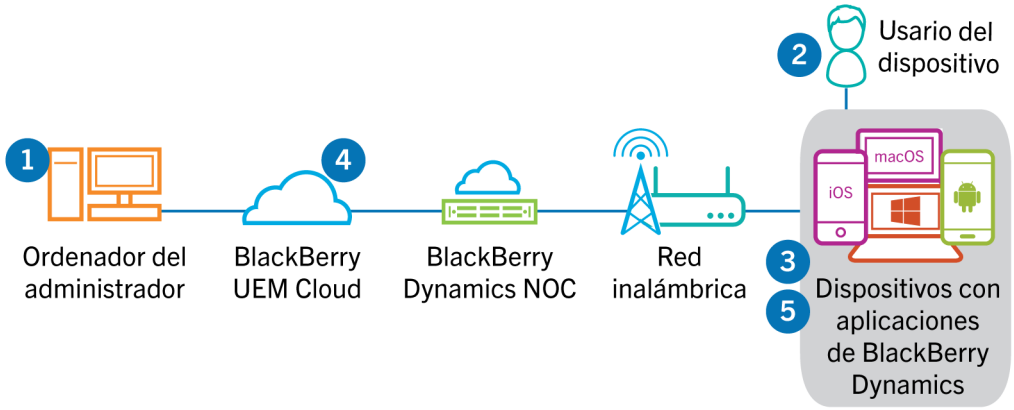
Flujo de datos: activación de un dispositivo macOS



1. Lleve a cabo las acciones siguientes:
   a. Agregue al usuario a BlackBerry UEM Cloud como una cuenta de usuario local o, si ha instalado BlackBerry Connectivity Node, mediante la información de la cuenta recuperada desde el directorio de la empresa.
   b. Asigne un perfil de activación al usuario.
   c. Asegúrese de que el usuario tenga la información de inicio de sesión de BlackBerry UEM Self-Service, incluidos:
      - Dirección web de BlackBerry UEM Self-Service
      - Nombre de usuario y contraseña
      - Nombre de dominio
2. El usuario inicia sesión en BlackBerry UEM Self-Service desde su dispositivo macOS y activa el dispositivo.
3. El dispositivo envía una solicitud de activación a BlackBerry UEM Cloud.
4. BlackBerry UEM Cloud verifica las credenciales de activación y envía los detalles de activación al dispositivo, incluida la información de configuración del dispositivo.
5. El dispositivo recibe los detalles de la activación de BlackBerry UEM Cloud y completa la configuración. A continuación, el dispositivo envía a BlackBerry UEM Cloud la confirmación de que la activación se realizó correctamente.

Flujo de datos: activación de una aplicación de BlackBerry Dynamics por primera vez en un dispositivo

En este flujo de datos se describe cómo se desplazan los datos cuando se activa una aplicación de BlackBerry Dynamics en un dispositivo que no tiene otra aplicación de BlackBerry Dynamics ni BlackBerry UEM Client activados.

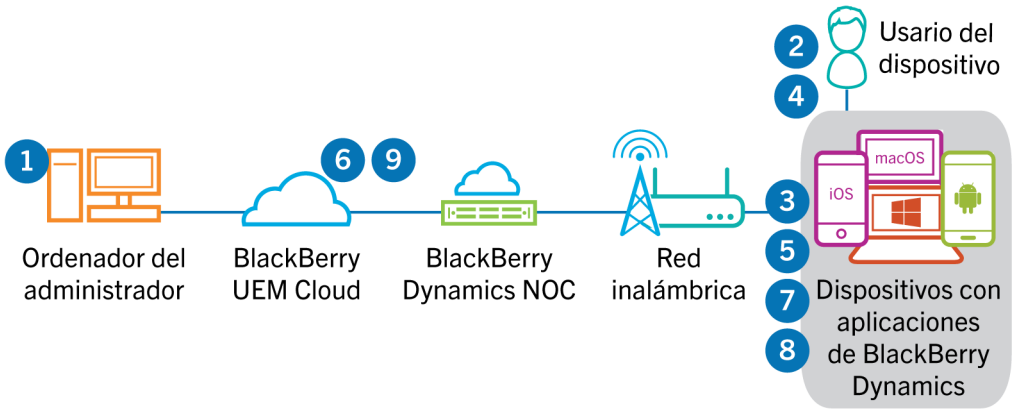


1. Un administrador realiza las siguientes acciones:
   a. Asigna una o más aplicaciones de BlackBerry Dynamics a un usuario.
   b. Emite las credenciales de activación (clave de acceso, contraseña de activación o código QR), o bien usa un proveedor de identidad de terceros, y las envía al usuario o indica al usuario que genere las credenciales desde BlackBerry UEM Self-Service.
2. El usuario realiza las siguientes acciones:
   a. Instala la aplicación en el dispositivo.
   b. Obtiene e introduce las credenciales de activación proporcionadas.
3. La aplicación de BlackBerry Dynamics realiza las acciones siguientes:
   a. Se conecta a BlackBerry Dynamics NOC y completa la activación.
   b. Obtiene la dirección de BlackBerry UEM mediante uno de los siguientes métodos:
      - Si el usuario introdujo manualmente las credenciales, la aplicación obtiene la dirección de BlackBerry Infrastructure.
      - Si el usuario ha escaneado un código QR, la aplicación recibe la dirección del código QR.
   c. Se conecta a BlackBerry UEM a través de BlackBerry Infrastructure y establece una sesión cifrada de manera integral con BlackBerry UEM mediante el protocolo EC-SPEKE.

      Esta sesión solo puede descifrarse mediante la instancia de BlackBerry UEM que emitió las credenciales de activación.
   d. Envía la solicitud de activación a través de la sesión segura.
4. BlackBerry UEM comprueba la solicitud de activación y envía una respuesta de activación cifrada a la aplicación. La respuesta de activación incluye los datos que necesita la aplicación para comunicarse con BlackBerry UEM, incluido un certificado de cliente, una clave de sesión principal, una lista de instancias de BlackBerry Proxy y autoridades de certificación de confianza.
5. La aplicación solicita al usuario que establezca una contraseña para la aplicación y que la registre como delegado de activación sencillo con BlackBerry Dynamics NOC para permitir que la siguiente aplicación de BlackBerry Dynamics se active en el dispositivo sin que el usuario tenga que obtener manualmente nuevas credenciales.

Flujo de datos: activación de una aplicación de BlackBerry Dynamics cuando ya hay una activada en el dispositivo

En este flujo de datos se describe cómo se desplazan los datos cuando se activa una aplicación de BlackBerry Dynamics en un dispositivo que ya tiene BlackBerry UEM Client u otra aplicación de BlackBerry Dynamics activados y funcionando como delegado de activación sencillo.



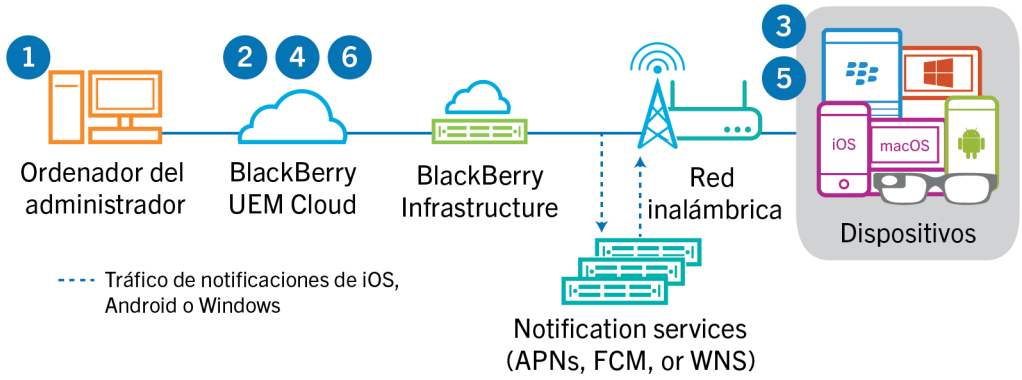
1. Un administrador asigna una o más aplicaciones de BlackBerry Dynamics a un usuario.
2. El usuario instala la aplicación en el dispositivo.
3. La aplicación realiza las acciones siguientes:
   a. Consulta BlackBerry Dynamics NOC e identifica otra aplicación que esté activada en el dispositivo.
   b. Solicita las credenciales de activación de la aplicación activada anteriormente.
4. El usuario aprueba la solicitud de activación de la aplicación activada anteriormente en el dispositivo.
5. La aplicación activada anteriormente envía las credenciales a BlackBerry UEM.
6. BlackBerry UEM envía la solicitud de credenciales y la URL de BlackBerry UEM a la aplicación existente.
7. La aplicación activada anteriormente devuelve las credenciales y la URL a la nueva aplicación.
8. La nueva aplicación realiza las acciones siguientes:
   a. Se activa con BlackBerry Dynamics NOC.
   b. Se conecta a BlackBerry UEM a través de BlackBerry Infrastructure y establece una sesión cifrada de manera integral con BlackBerry UEM mediante el protocolo EC-SPEKE.

      Esta sesión solo puede descifrarse mediante la instancia de BlackBerry UEM que emitió las credenciales de activación.
   c. Envía la solicitud de activación a través de la sesión segura.
9. BlackBerry UEM comprueba la solicitud de activación y envía una respuesta de activación cifrada a la aplicación. La respuesta de activación incluye los datos que necesita la aplicación para comunicarse con BlackBerry UEM, incluido un certificado de cliente, una clave de sesión principal, una lista de instancias de BlackBerry Proxy y autoridades de certificación de confianza.

Flujo de datos: recepción de actualizaciones de configuración en un dispositivo

Cuando se utiliza la consola de administración para enviar comandos del dispositivo como, por ejemplo, bloquear el dispositivo o eliminar datos de trabajo, o cuando se llevan a cabo otras tareas de administración del dispositivo, por ejemplo, la actualización de políticas, perfiles y configuración o asignación de aplicaciones, se desencadena una actualización de configuración para el dispositivo.

Cuando es necesario enviar una actualización de configuración a un dispositivo, BlackBerry UEM Cloud notifica al dispositivo que tiene una actualización de configuración pendiente. Los dispositivos también sondean BlackBerry UEM Cloud periódicamente para saber qué acciones deben ejecutarse en el dispositivo con el fin de evitar la pérdida de cualquier actualización de configuración en el caso de no recibir la notificación en el dispositivo.



1. Utilice la consola de administración para enviar comandos del dispositivo como, por ejemplo, bloquear el dispositivo o eliminar datos de trabajo, o para llevar a cabo tareas de administración del dispositivo, por ejemplo, la actualización de políticas de TI, perfiles, y configuración o asignación de aplicaciones, y desencadenar una actualización de configuración para el dispositivo.
2. BlackBerry UEM Cloud asigna la actualización e identifica los objetos que tienen que compartirse con el dispositivo y, a continuación, realiza una de las siguientes acciones:
   - Para los dispositivos Android, BlackBerry UEM Cloud notifica al BlackBerry UEM Client en el dispositivo de que hay una actualización pendiente mediante el FCM. FCM envía una notificación al dispositivo para que se ponga en contacto con BlackBerry UEM Cloud.
   - Para los dispositivos iOS y OS X, BlackBerry UEM Cloud notifica al MDM Daemon en el dispositivo de que hay una actualización pendiente mediante los APN. Los APN envían una notificación al dispositivo para que se ponga en contacto con BlackBerry UEM Cloud.
   - Para los dispositivos con Windows 10, BlackBerry UEM Cloud notifica al MDM Daemon en el dispositivo de que hay una actualización pendiente mediante el WNS. El WNS envía una notificación al dispositivo para que se ponga en contacto con BlackBerry UEM Cloud.
3. El dispositivo se pone en contacto con BlackBerry UEM Cloud para solicitar la implementación de acciones y comandos pendientes en el dispositivo.
4. BlackBerry UEM Cloud responde con la acción de mayor prioridad.

   Se da prioridad a los comandos de administración de TI, como Bloquear dispositivo, seguido de las solicitudes de información del dispositivo, aplicaciones instaladas y así sucesivamente. BlackBerry UEM Cloud envía un comando a la vez. Si es necesario, se incluye información adicional en la respuesta.
5. El dispositivo realiza las siguientes acciones:

   a. Inspecciona la respuesta de BlackBerry UEM Cloud
   b. Programa el comando para que se procese y espera a que el comando se ejecute.

c. Envía una respuesta a BlackBerry UEM Cloud para que actualice el estado del comando. El estado indica si el comando se ha ejecutado correctamente y proporciona un mensaje de error en caso de fallo.

6. Si hay más acciones o comandos pendientes para el dispositivo, BlackBerry UEM Cloud responde con la acción de mayor prioridad.

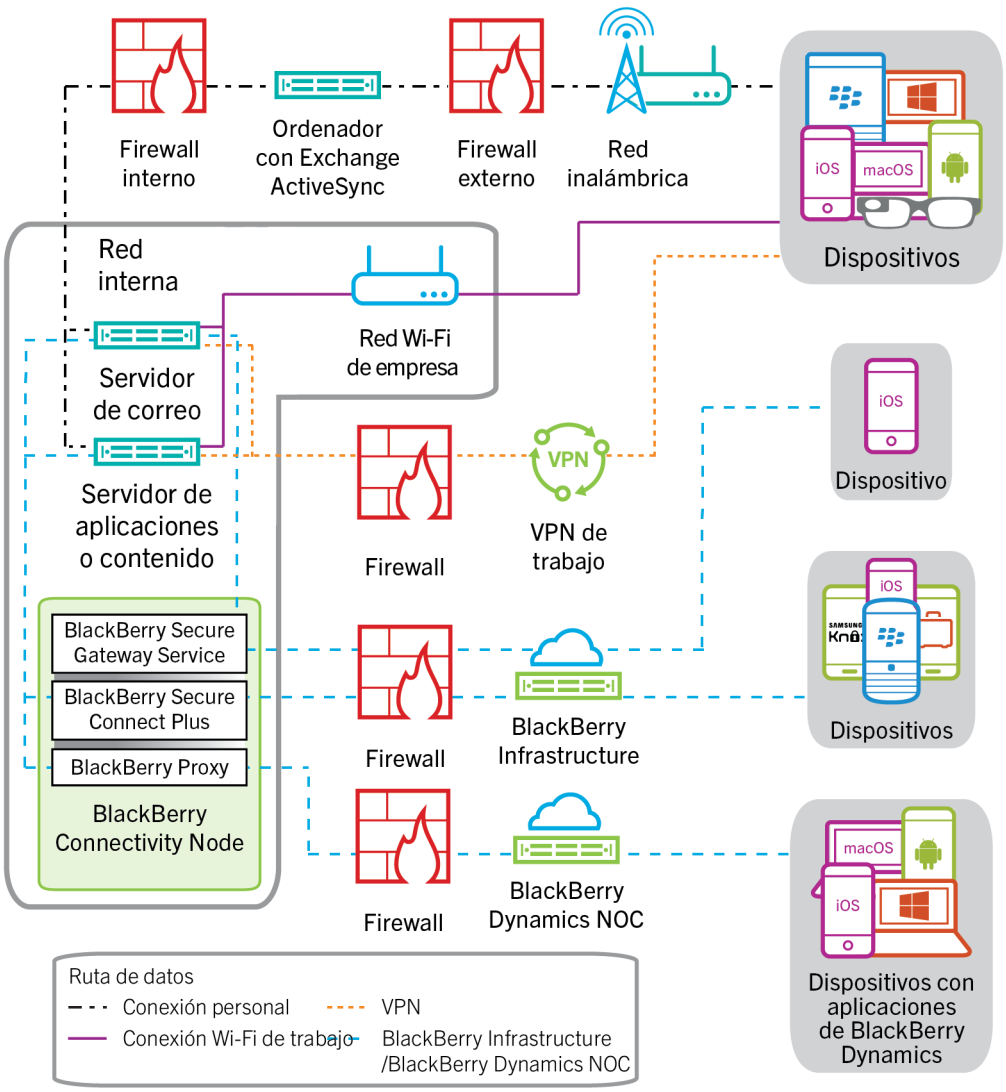
   Los pasos del 4 al 6 se repiten hasta que no haya más acciones o comandos pendientes y BlackBerry UEM Cloud responde con un comando inactivo.

Envío y recepción de datos de trabajo

Cuando los usuarios envían y reciben datos de trabajo en un dispositivo, los datos pueden transferirse entre el dispositivo y sus recursos mediante las siguientes conexiones:

- Un dispositivo puede utilizar una conexión directa a través de la red inalámbrica desde el dispositivo al servidor de correo, contenido o aplicaciones (por ejemplo, un servidor de Exchange ActiveSync que se coloca en una DMZ o se expone a la red pública).
- El dispositivo puede utilizar una conexión directa a través de la red VPN o la red Wi-Fi de trabajo de la empresa con el servidor de correo, contenido o aplicaciones. Usted u otro usuario pueden configurar el VPN del dispositivo o perfil Wi-Fi.
- Al instalar BlackBerry Connectivity Node, BlackBerry Secure Connect Plus puede proporcionar un túnel IP seguro a través de BlackBerry Infrastructure entre las aplicaciones en los dispositivos con iOS, Android Enterprise y Samsung Knox Workspace y la red de su empresa.
- Si se instala BlackBerry Connectivity Node, BlackBerry Proxy puede proporcionar una conexión segura entre las aplicaciones de BlackBerry Dynamics en los dispositivos y la red de su empresa.
- Si se instala BlackBerry Connectivity Node, BlackBerry Secure Gateway puede proporcionar una conexión segura a través de BlackBerry Infrastructure y BlackBerry UEM al servidor de correo de su empresa para los dispositivos iOS.

Este diagrama muestra las posibles rutas de datos.

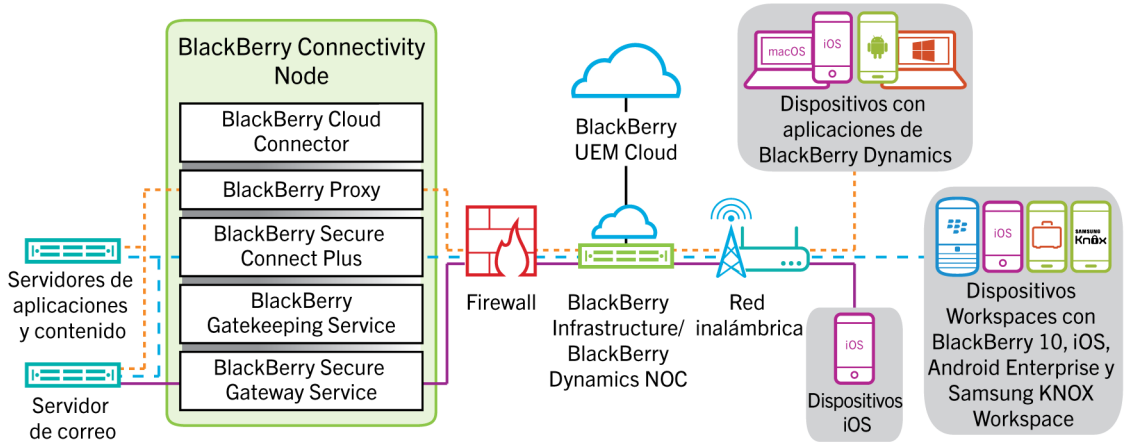

Firewall interno
Ordenador con Exchange ActiveSync
Firewall externo
Red inalámbrica
iOS
macOS
Dispositivos
Red interna
Red Wi-Fi de empresa
Servidor de correo
Servidor de aplicaciones o contenido
Firewall
VPN
VPN de trabajo
iOS
Dispositivo
BlackBerry Secure Gateway Service
BlackBerry Secure Connect Plus
BlackBerry Proxy
BlackBerry Connectivity Node
Firewall
BlackBerry Infrastructure
iOS
Dispositivos
Firewall
BlackBerry Dynamics NOC
macOS
iOS
Dispositivos con aplicaciones de BlackBerry Dynamics
Ruta de datos
Conexión personal
VPN
Conexión Wi-Fi de trabajo
BlackBerry Infrastructure /BlackBerry Dynamics NOC

Envío y recepción de datos de trabajo mediante BlackBerry UEM Cloud y BlackBerry Infrastructure

Al instalar BlackBerry Connectivity Node, los dispositivos pueden conectarse a los recursos de la empresa a través de BlackBerry UEM Cloud y BlackBerry Infrastructure o BlackBerry Dynamics NOC, utilizando los siguientes servicios:

Servicio	Descripción
BlackBerry Secure Connect Plus	BlackBerry Secure Connect Plus proporciona un túnel IP seguro a través del BlackBerry Infrastructure para transferir datos entre las aplicaciones y la red de su empresa: Para dispositivos con Android Enterprise, BlackBerry Secure Connect Plus, proporciona un túnel seguro entre todas las aplicaciones del espacio de trabajo y la red de su empresa. Para dispositivos Samsung Knox Workspace, BlackBerry Secure Connect Plus puede proporcionar un túnel seguro entre la red de su empresa y todas las aplicaciones de trabajo o solo las aplicaciones de trabajo especificadas. Para dispositivos iOS, BlackBerry Secure Connect Plus puede proporcionar un túnel seguro entre la red de su empresa y todas las aplicaciones o solo las aplicaciones especificadas.
BlackBerry Proxy	BlackBerry Proxy proporciona una conexión segura entre las aplicaciones de BlackBerry Dynamics en los dispositivos y los recursos de su empresa detrás del firewall. También admite BlackBerry Dynamics Direct Connect, que permite que los datos de aplicaciones omitan BlackBerry Dynamics NOC.
BlackBerry Secure Gateway	BlackBerry Secure Gateway proporciona una conexión segura a través de BlackBerry Infrastructure y BlackBerry UEM al servidor de correo de su empresa para dispositivos iOS.

El diagrama siguiente muestra cómo se pueden conectar los dispositivos a los recursos de su empresa a través de BlackBerry Infrastructure y BlackBerry UEM Cloud.

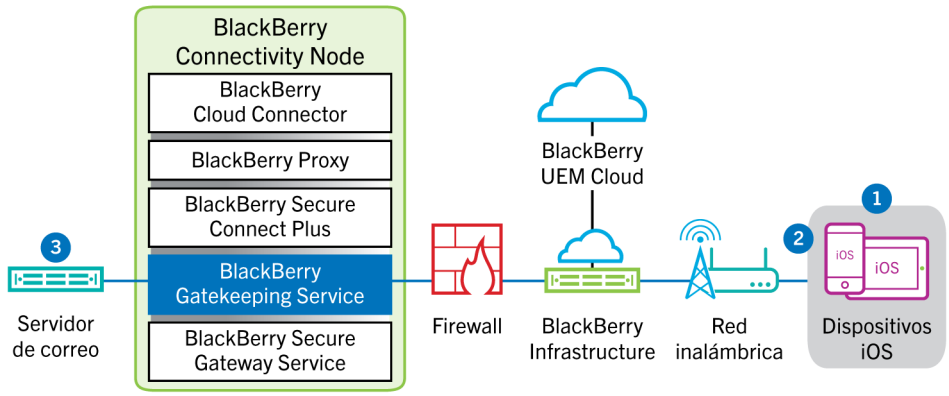


Para obtener más información sobre la activación de BlackBerry Secure Connect Plus, consulte "Activación y configuración de BlackBerry Secure Connect Plus" en el contenido de Administración.

Para obtener más información sobre la activación de BlackBerry Secure Gateway, consulte "Protección de los datos de correo electrónico con BlackBerry Secure Gateway" en el contenido de Administración.

Flujo de datos: envío de correo desde un dispositivo iOS con BlackBerry Secure Gateway

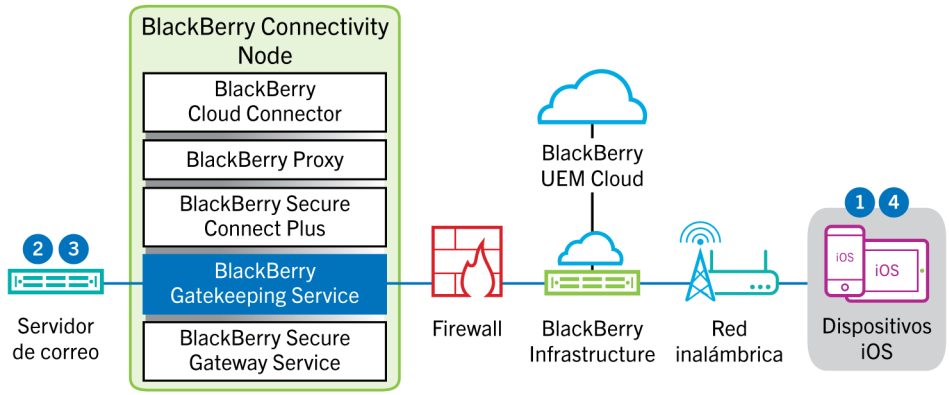
Este flujo de datos describe cómo se desplazan los datos del correo y del calendario de trabajo de dispositivos iOS al servidor de Exchange ActiveSync mediante BlackBerry Secure Gateway.



1. El usuario crea un mensaje de correo o actualiza un elemento del organizador en el espacio de trabajo.
2. El dispositivo envía el elemento nuevo o modificado a través de BlackBerry Infrastructure y BlackBerry Secure Gateway al servidor de correo.
3. El servidor de correo actualiza los datos del organizador en el buzón de correo del usuario o envía el elemento de correo al destinatario y envía una confirmación al dispositivo.

Flujo de datos: recepción de correo en un dispositivo iOS con BlackBerry Secure Gateway

Este flujo de datos describe cómo se desplazan los datos del correo y del calendario de trabajo entre dispositivos iOS y el servidor Exchange ActiveSync mediante BlackBerry Secure Gateway.

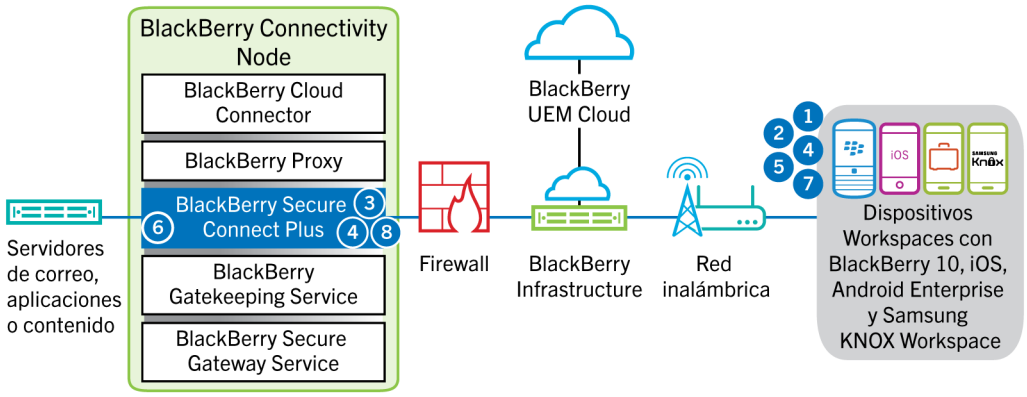


1. El dispositivo envía una solicitud HTTPS al servidor de correo y solicita que este notifique al dispositivo en el caso de que se modifique cualquier elemento en las carpetas que están configuradas para su sincronización. La solicitud se desplaza a través del canal cifrado y autenticado establecido entre BlackBerry Infrastructure y BlackBerry Secure Gateway con el servidor de correo.
2. Si no hay elementos nuevos ni modificados durante este intervalo, el servidor de correo envía un mensaje "HTTP 200 OK" al dispositivo. El dispositivo envía una nueva solicitud y el proceso comienza de nuevo.

3. Si hay elementos nuevos o modificados para el dispositivo, por ejemplo, un mensaje de correo nuevo o una entrada del calendario actualizada, el servidor de correo envía las actualizaciones al dispositivo a través del canal seguro establecido entre BlackBerry Secure Gateway y BlackBerry Infrastructure con la aplicación de correo o de organizador en el dispositivo.
4. Cuando la sincronización finaliza, el dispositivo envía otra solicitud para comenzar de nuevo el proceso.

Flujo de datos: envío y recepción de datos de trabajo mediante BlackBerry Secure Connect Plus

Este flujo de datos describe cómo se desplazan los datos cuando una aplicación en un dispositivo que está configurado para utilizar BlackBerry Secure Connect Plus accede a un servidor de aplicaciones o de contenido de la empresa.



1. El usuario abre una aplicación para acceder a los datos de trabajo desde un servidor de aplicaciones o de contenido detrás del firewall de la empresa.
   - En los dispositivos con Android Enterprise y Samsung Knox Workspace, todas las aplicaciones de trabajo pueden utilizar BlackBerry Secure Connect Plus.
   - En los dispositivos iOS, debe especificar si todas las aplicaciones o solo algunas pueden utilizar BlackBerry Secure Connect Plus.
2. El dispositivo determina que un túnel IP seguro es el método más directo y eficaz para conectarse con el servidor de aplicaciones o de contenido y recuperar los datos, y envía una solicitud a BlackBerry Infrastructure a través de un túnel TLS, por el puerto 443, para obtener un túnel seguro a la red de trabajo. De forma predeterminada, la señal se cifra con bibliotecas Certicom certificadas mediante FIPS-140. El túnel de señalización se somete a un cifrado integral.
3. BlackBerry Secure Connect Plus recibe la solicitud de BlackBerry Infrastructure a través del puerto 3101.
4. El dispositivo y BlackBerry Secure Connect Plus negocian los parámetros del túnel y establecen un túnel seguro para el dispositivo a través de BlackBerry Infrastructure. El túnel se autentica y se cifra de forma integral con DTLS.
5. La aplicación utiliza el túnel para conectarse con el servidor de aplicaciones o de contenido mediante protocolos estándar IPv4 (TCP y UDP).
6. BlackBerry Secure Connect Plus envía y recibe los datos de la IP desde la red de su empresa. BlackBerry Secure Connect Plus cifra y descifra el tráfico a través de bibliotecas Certicom certificadas mediante FIPS-140.
7. La aplicación recibe y muestra los datos en el dispositivo.
8. Mientras el túnel esté abierto, las aplicaciones compatibles lo utilizarán para acceder a los recursos de red. Cuando el túnel deja de ser el mejor método disponible para conectarse a la red de su empresa, BlackBerry Secure Connect Plus lo finaliza.

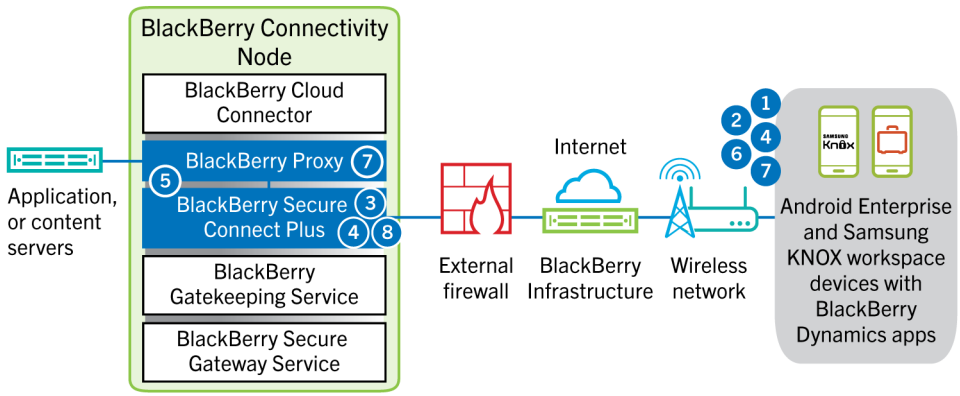
   En los dispositivos iOS, si configura una VPN por aplicación para BlackBerry Secure Connect Plus, el túnel finaliza cuando no se utiliza ninguna de las aplicaciones configuradas.

Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics en un dispositivo Android utilizando BlackBerry Secure Connect Plus

Este flujo de datos describe cómo viajan los datos cuando una aplicación de BlackBerry Dynamics en un dispositivo Android Enterprise o Samsung Knox Workspace utiliza BlackBerry Secure Connect Plus.

Si está utilizando BlackBerry Secure Connect Plus con aplicaciones de BlackBerry Dynamics en un dispositivo Android Enterprise, es recomendable restringir las aplicaciones de BlackBerry Dynamics para que no utilicen BlackBerry Secure Connect Plus con el fin de evitar la latencia de la red. No se pueden restringir aplicaciones específicas en dispositivos Samsung Knox Workspace.

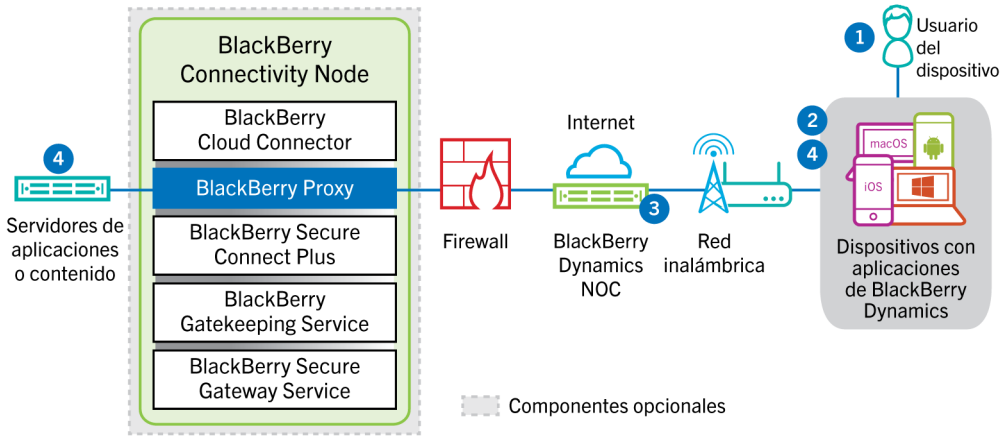
Si está utilizando BlackBerry Secure Connect Plus con aplicaciones de BlackBerry Dynamics en un dispositivo Android Enterprise o un dispositivo Samsung Knox Workspace, es recomendable que configure BlackBerry UEM para que no envíe los datos de las aplicaciones de BlackBerry Dynamics a través de BlackBerry Dynamics NOC con el fin de reducir la latencia de la red.



1. El usuario abre una aplicación de BlackBerry Dynamics para acceder a los datos de trabajo.
2. El dispositivo envía una solicitud a través de túnel TLS, a través del puerto 443, a BlackBerry Infrastructure para solicitar un túnel seguro a la red de trabajo. La señal se cifra de forma predeterminada con bibliotecas Certicom certificadas mediante FIPS-140. El túnel de señalización se somete a un cifrado integral.
3. BlackBerry Secure Connect Plus recibe la solicitud de BlackBerry Infrastructure a través del puerto 3101.
4. El dispositivo y BlackBerry Secure Connect Plus negocian los parámetros del túnel y establecen un túnel seguro para el dispositivo a través de BlackBerry Infrastructure. El túnel se autentica y se cifra de forma integral con DTLS.
5. BlackBerry Secure Connect Plus establece una conexión con BlackBerry Proxy.
6. La aplicación de BlackBerry Dynamics establece una conexión con BlackBerry Proxy utilizando el túnel de BlackBerry Secure Connect Plus.
7. BlackBerry Proxy se autentica en la aplicación de BlackBerry Dynamics utilizando su certificado de servidor. BlackBerry Proxy valida la aplicación mediante una clave MAC con una clave de sesión que solo conoce BlackBerry Proxy y la aplicación.
8. Cuando se establece la conexión segura entre BlackBerry Proxy y la aplicación, los datos de trabajo se pueden desplazar entre el dispositivo y los servidores de aplicaciones o de contenido detrás del firewall utilizando el túnel de BlackBerry Secure Connect Plus a BlackBerry Proxy. BlackBerry Secure Connect Plus cifra y descifra el tráfico a través de bibliotecas Certicom certificadas mediante FIPS-140.

Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics

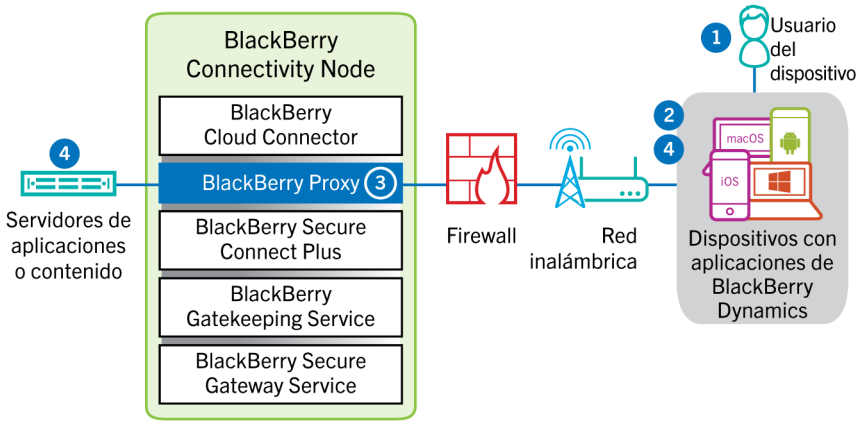
En este flujo de datos se describe cómo se desplazan los datos cuando una aplicación de BlackBerry Dynamics accede a un servidor de aplicaciones o de contenido en la empresa.



1. El usuario abre una aplicación de BlackBerry Dynamics para acceder a los datos de trabajo.
2. La aplicación de BlackBerry Dynamics establece una conexión con BlackBerry Dynamics NOC. La conexión está autenticada con la clave de enlace maestro que se creó cuando la aplicación se activó.
3. BlackBerry Dynamics NOC realiza cualquiera de las acciones siguientes:
   a. Se comunica con BlackBerry Proxy a través de una conexión segura establecida previamente para establecer una conexión integral a través del puerto 443 entre la aplicación de BlackBerry Dynamics y BlackBerry Proxy que transporta los datos de trabajo. Los datos de trabajo se cifran con una clave de sesión que BlackBerry Dynamics NOC no conoce.
   b. Si BlackBerry Connectivity Node no está configurado, se comunica directamente con sus contenidos de aplicaciones o de contenido a través del puerto que se haya abierto en el firewall de la empresa.
4. Si BlackBerry Connectivity Node está configurado, cuando se establece la conexión integral entre BlackBerry Dynamics NOC y BlackBerry Proxy, los datos de trabajo pueden desplazarse entre el dispositivo y los servidores de aplicaciones o de contenido detrás del firewall mediante BlackBerry Proxy.

Flujo de datos: envío y recepción de datos de trabajo desde una aplicación de BlackBerry Dynamics mediante BlackBerry Dynamics Direct Connect

En este flujo de datos se describe cómo se desplazan los datos cuando una aplicación de BlackBerry Dynamics accede a un servidor de aplicaciones o de contenido en la empresa mediante BlackBerry Dynamics Direct Connect y BlackBerry Proxy.



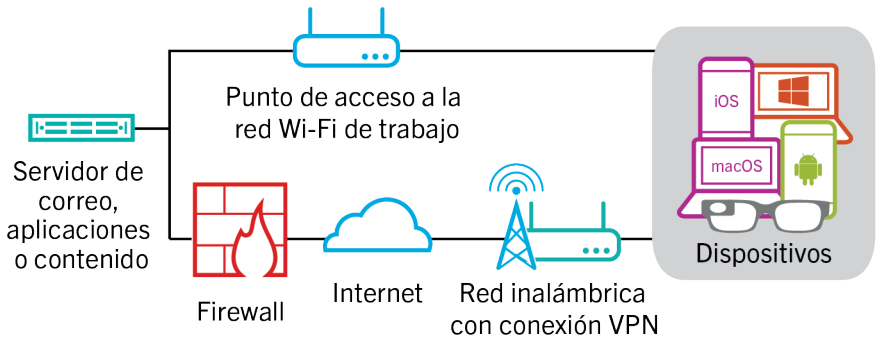
1. El usuario abre una aplicación de BlackBerry Dynamics para acceder a los datos de trabajo.
2. La aplicación de BlackBerry Dynamics establece una conexión TLS con BlackBerry Proxy a través del puerto 17533.

3. BlackBerry Proxy se autentica con la aplicación de BlackBerry Dynamics. BlackBerry Proxy se autentica con la aplicación utilizando su certificado de servidor. BlackBerry Proxy valida la aplicación mediante una clave MAC con una clave de sesión que solo conoce BlackBerry Proxy y la aplicación.
4. Cuando se establece la conexión integral, los datos de trabajo se desplazan entre el dispositivo y los servidores de aplicaciones o de contenido detrás del firewall mediante BlackBerry Proxy.

Envío y recepción de datos de trabajo mediante una VPN o red Wi-Fi de trabajo

Es posible que los dispositivos que tienen perfiles VPN o Wi-Fi configurados por usted u otro usuario puedan obtener acceso a los recursos de la empresa a través de la VPN de la empresa o la red Wi-Fi del trabajo. Para utilizar la VPN de la empresa, los usuarios con un dispositivo con Android que tenga el tipo de activación de Controles de MDM o Samsung Knox Workspace, deberán configurar manualmente un perfil de VPN en sus dispositivos.

Este diagrama muestra cómo se desplazan los datos cuando un dispositivo se conecta a los recursos de la empresa mediante la VPN de la empresa o la red Wi-Fi del trabajo.

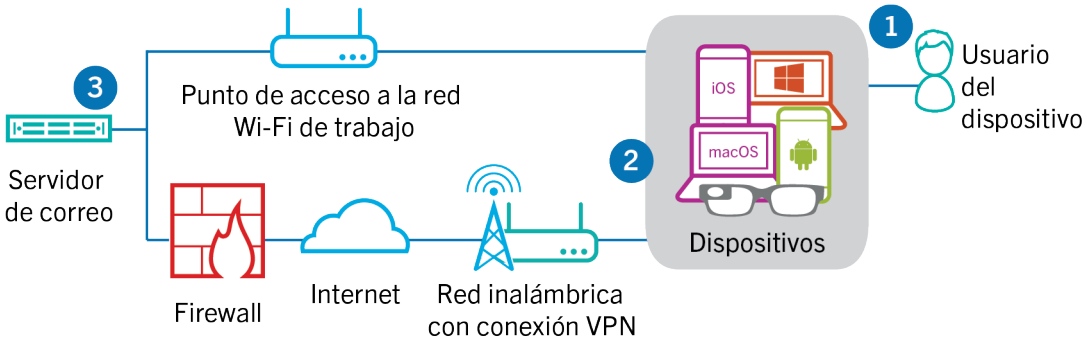


La siguiente tabla describe cuándo la red VPN de la empresa o la red Wi-Fi de trabajo utilizan dispositivos para conectarse a la red de su empresa.

Tipo de dispositivo	Descripción
Dispositivos con Android Enterprise y dispositivos con Knox Workspace	De forma predeterminada, los dispositivos con Android Enterprise y Knox Workspace utilizan la VPN de la empresa o la red Wi-Fi del trabajo para enviar y recibir datos de trabajo solo cuando BlackBerry Secure Connect Plus no está activado.
Dispositivos Windows y macOS, y dispositivos Android con el tipo de activación Controles de MDM	Los dispositivos Windows y macOS, y los dispositivos Android con el tipo de activación Controles de MDM utilizan la VPN de su empresa o la red Wi-Fi de trabajo para enviar y recibir datos de trabajo. Para utilizar la VPN de la empresa, los usuarios de los dispositivos Android deben configurar manualmente un perfil VPN en sus dispositivos.
iOS	Los dispositivos iOS utilizan la VPN de su empresa o la red Wi-Fi de trabajo para enviar y recibir datos de Exchange ActiveSync si BlackBerry Secure Gateway no está activado. El resto de datos de trabajo utilizan la red VPN de su empresa o la red Wi-Fi de trabajo.

Flujo de datos: envío de correo desde un dispositivo mediante una red VPN o una red Wi-Fi de trabajo

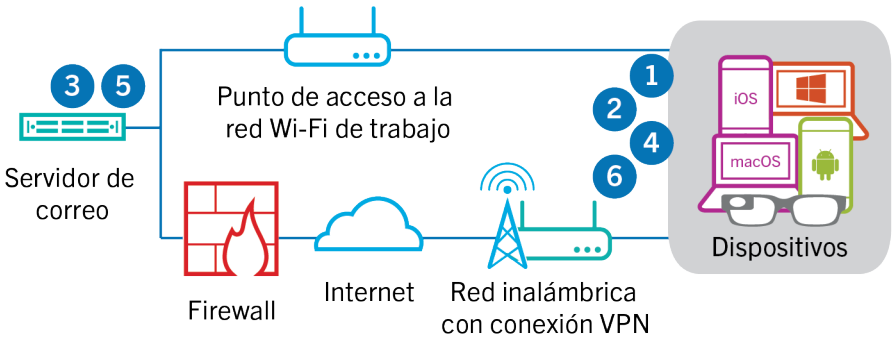
Este flujo de datos describe cómo se desplazan los datos del correo electrónico del trabajo y los datos del calendario desde el dispositivo al servidor de correo a través de la VPN o la red Wi-Fi de trabajo de la empresa mediante Exchange ActiveSync.



1. El usuario crea un mensaje de correo o actualiza un elemento del organizador en el espacio de trabajo.
2. El dispositivo envía el elemento nuevo o modificado al servidor de correo electrónico a través de la VPN o la red Wi-Fi de trabajo de la empresa.
3. El servidor de correo actualiza los datos del organizador en el buzón de correo del usuario o envía el elemento de correo al destinatario y envía una confirmación al dispositivo.

Flujo de datos: recepción de correo en un dispositivo mediante una red VPN o una red Wi-Fi de trabajo

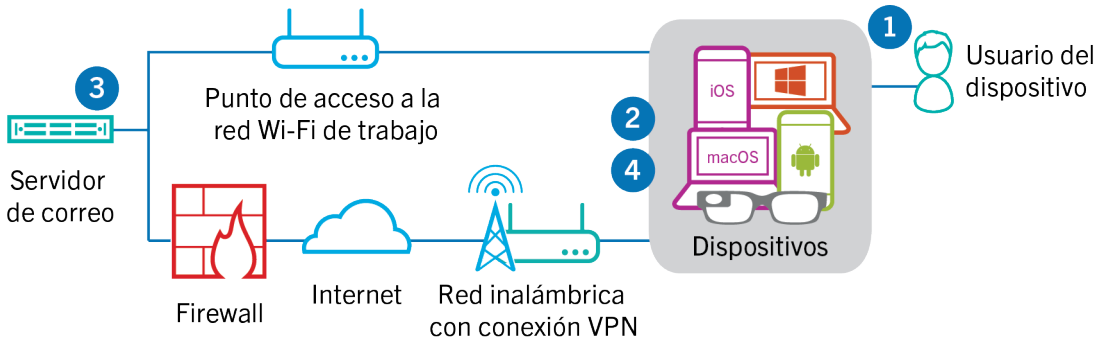
Este flujo de datos describe cómo se desplazan los datos del correo electrónico del trabajo y los datos del calendario desde el dispositivo al servidor de correo a través de la VPN o la red Wi-Fi de trabajo de la empresa mediante Exchange ActiveSync.



1. El dispositivo envía una solicitud HTTPS al servidor de correo y solicita que el servidor de correo notifique al dispositivo en el caso de que se modifique cualquier elemento en las carpetas que están configuradas para su sincronización. La solicitud se desplaza a través de la VPN de la empresa o red Wi-Fi del trabajo hasta el servidor de correo.
2. El dispositivo permanece en espera.
3. Cuando hay elementos nuevos o modificados para el dispositivo, por ejemplo, un mensaje de correo electrónico nuevo o una entrada actualizada del calendario, el servidor de correo envía las actualizaciones al dispositivo. Los elementos nuevos o modificados se desplazan a través de la VPN de la empresa o red Wi-Fi de trabajo a la aplicación de correo electrónico o de datos del dispositivo en el dispositivo.
4. Cuando la sincronización finaliza, el dispositivo envía otra solicitud para comenzar de nuevo el proceso.
5. Si no hay elementos nuevos ni modificados durante este intervalo, el servidor de correo o de aplicaciones envía un mensaje al dispositivo mediante el protocolo de Exchange ActiveSync.
6. El dispositivo envía una nueva solicitud y el proceso comienza de nuevo.

Flujo de datos: acceso a un servidor de aplicaciones o de contenido mediante una red VPN o una red Wi-Fi de trabajo

Este flujo de datos describe cómo se transfieren los datos entre un servidor de aplicaciones o de contenido de la empresa y una aplicación en un dispositivo a través de una conexión VPN o la red Wi-Fi de trabajo.



1. El usuario abre una aplicación de trabajo para ver los datos de trabajo. Por ejemplo, el usuario abre el navegador de trabajo para desplazarse por la intranet o utiliza una aplicación desarrollada de forma interna para acceder a los datos de los clientes de la empresa.
2. La aplicación establece una conexión con el servidor de aplicaciones o de contenido para recuperar los datos. La solicitud se desplaza a través de la VPN o red Wi-Fi de trabajo de la empresa hasta el servidor de aplicaciones o de contenido.
3. El servidor de aplicaciones o de contenido responde con los datos de trabajo. Los datos del trabajo se desplazan a través de la VPN o red Wi-Fi de trabajo a la aplicación en el espacio de trabajo del dispositivo.
4. La aplicación recibe y muestra los datos en el dispositivo.

Aviso legal

Esta documentación, incluida cualquier documentación que se incorpore mediante referencia como documento proporcionado o disponible en el sitio web de BlackBerry, se proporciona o se pone a disposición "TAL CUAL" y "SEGÚN SU DISPONIBILIDAD" sin ninguna condición, responsabilidad ni garantía de ningún tipo por parte de BlackBerry Limited y sus empresas afiliadas ("BlackBerry"), y BlackBerry no asume ninguna responsabilidad por los errores tipográficos, técnicos o cualquier otra imprecisión, error u omisión contenidos en esta documentación. Con el fin de proteger la información confidencial y propia de BlackBerry, así como los secretos comerciales, la presente documentación describe algunos aspectos de la tecnología de BlackBerry en líneas generales. BlackBerry se reserva el derecho a modificar periódicamente la información que contiene esta documentación, si bien tampoco se compromete en modo alguno a proporcionar cambios, actualizaciones, ampliaciones o cualquier otro tipo de información que se pueda agregar a esta documentación.

Esta documentación puede contener referencias a fuentes de información, hardware o software, productos o servicios, incluidos componentes y contenido como, por ejemplo, el contenido protegido por copyright y/o sitios Web de terceros (conjuntamente, los "Productos y servicios de terceros"). BlackBerry no controla ni es responsable de ningún tipo de Productos y servicios de terceros, lo que incluye, sin restricciones, el contenido, la exactitud, el cumplimiento de copyright, la compatibilidad, el rendimiento, la fiabilidad, la legalidad, la decencia, los vínculos o cualquier otro aspecto de los Productos y servicios de terceros. La inclusión de una referencia a los Productos y servicios de terceros en esta documentación no implica que BlackBerry se haga responsable de dichos Productos y servicios de terceros ni de dichos terceros en modo alguno.

EXCEPTO EN LA MEDIDA EN QUE LO PROHÍBA ESPECÍFICAMENTE LA LEY DE SU JURISDICCIÓN, QUEDAN EXCLUIDAS POR LA PRESENTE TODAS LAS CONDICIONES, APROBACIONES O GARANTÍAS DE CUALQUIER TIPO, EXPLÍCITAS O IMPLÍCITAS, INCLUIDA, SIN NINGÚN TIPO DE LIMITACIÓN, CUALQUIER CONDICIÓN, APROBACIÓN, GARANTÍA, DECLARACIÓN DE GARANTÍA DE DURABILIDAD, IDONEIDAD PARA UN FIN O USO DETERMINADO, COMERCIABILIDAD, CALIDAD COMERCIAL, ESTADO DE NO INFRACCIÓN, CALIDAD SATISFACTORIA O TITULARIDAD, O QUE SE DERIVE DE UNA LEY O COSTUMBRE O UN CURSO DE LAS NEGOCIACIONES O USO DEL COMERCIO, O RELACIONADO CON LA DOCUMENTACIÓN O SU USO O RENDIMIENTO O NO RENDIMIENTO DE CUALQUIER SOFTWARE, HARDWARE, SERVICIO O CUALQUIER PRODUCTO O SERVICIO DE TERCEROS MENCIONADOS AQUÍ. ASIMISMO, PODRÍA DISPONER DE OTROS DERECHOS QUE VARÍAN SEGÚN EL ESTADO O LA PROVINCIA. ES POSIBLE QUE ALGUNAS JURISDICCIONES NO PERMITAN LA EXCLUSIÓN O LA LIMITACIÓN DE GARANTÍAS Y CONDICIONES IMPLÍCITAS. EN LA MEDIDA EN QUE LO PERMITA LA LEY, CUALQUIER GARANTÍA IMPLÍCITA O CONDICIONES EN RELACIÓN CON LA DOCUMENTACIÓN NO SE PUEDEN EXCLUIR TAL Y COMO SE HA EXPUESTO ANTERIORMENTE, PERO PUEDEN SER LIMITADAS, Y POR LA PRESENTE ESTÁN LIMITADAS A NOVENTA (90) DÍAS DESDE LA FECHA QUE ADQUIRIÓ LA DOCUMENTACIÓN O EL ELEMENTO QUE ES SUJETO DE LA RECLAMACIÓN.

EN LA MEDIDA MÁXIMA EN QUE LO PERMITA LA LEY DE SU JURISDICCIÓN, EN NINGÚN CASO BLACKBERRY ASUMIRÁ RESPONSABILIDAD ALGUNA POR CUALQUIER TIPO DE DAÑOS RELACIONADOS CON ESTA DOCUMENTACIÓN O SU USO, O POR EL RENDIMIENTO O NO RENDIMIENTO DE CUALQUIER SOFTWARE, HARDWARE, SERVICIO O PRODUCTOS Y SERVICIOS DE TERCEROS AQUÍ MENCIONADOS INCLUIDOS SIN NINGÚN TIPO DE LIMITACIÓN CUALQUIERA DE LOS SIGUIENTES DAÑOS: DIRECTOS, RESULTANTES, EJEMPLARES, INCIDENTALES, INDIRECTOS, ESPECIALES, PUNITIVOS O AGRAVADOS, DAÑOS POR PÉRDIDA DE BENEFICIOS O INGRESOS, IMPOSIBILIDAD DE CONSEGUIR LOS AHORROS ESPERADOS, INTERRUPCIÓN DE LA ACTIVIDAD COMERCIAL, PÉRDIDA DE INFORMACIÓN COMERCIAL, PÉRDIDA DE LA OPORTUNIDAD DE NEGOCIO O DAÑO O PÉRDIDA DE DATOS, IMPOSIBILIDAD DE TRANSMITIR O RECIBIR CUALQUIER DATO, PROBLEMAS ASOCIADOS CON CUALQUIER APLICACIÓN QUE SE UTILICE JUNTO CON PRODUCTOS Y SERVICIOS DE BLACKBERRY, COSTES DEBIDOS AL TIEMPO DE INACTIVIDAD, PÉRDIDA DE USO DE LOS PRODUCTOS Y

SERVICIOS DE BLACKBERRY O PARTE DE ELLOS O DE CUALQUIER SERVICIO DE USO, COSTE DE SERVICIOS SUSTITUTIVOS, COSTES DE COBERTURA, INSTALACIONES O SERVICIOS, COSTE DEL CAPITAL O CUALQUIER OTRA PÉRDIDA MONETARIA SIMILAR, TANTO SI DICHOS DAÑOS SE HAN PREVISTO COMO SI NO, Y AUNQUE SE HAYA AVISADO A BLACKBERRY DE LA POSIBILIDAD DE DICHOS DAÑOS.

EN LA MEDIDA MÁXIMA EN QUE LO PERMITA LA LEY DE SU JURISDICCIÓN, BLACKBERRY NO TENDRÁ NINGÚN OTRO TIPO DE OBLIGACIÓN O RESPONSABILIDAD CONTRACTUAL, EXTRACONTRACTUAL O CUALQUIER OTRA, INCLUIDA CUALQUIER RESPONSABILIDAD POR NEGLIGENCIA O RESPONSABILIDAD ESTRICTA.

LAS LIMITACIONES, EXCLUSIONES Y DESCARGOS DE RESPONSABILIDAD SE APLICARÁN: (A) INDEPENDIENTEMENTE DE LA NATURALEZA DE LA CAUSA DE LA ACCIÓN, DEMANDA O ACCIÓN POR SU PARTE, INCLUIDA PERO NO LIMITADA AL INCUMPLIMIENTO DEL CONTRATO, NEGLIGENCIA, AGRAVIO, RESPONSABILIDAD ESTRICTA O CUALQUIER OTRA TEORÍA DEL DERECHO Y DEBERÁN SOBREVIVIR A UNO O MÁS INCUMPLIMIENTOS ESENCIALES O AL INCUMPLIMIENTO DEL PROPÓSITO ESENCIAL DE ESTE CONTRATO O CUALQUIER SOLUCIÓN CONTENIDA AQUÍ; Y (B) A BLACKBERRY Y A SUS EMPRESAS AFILIADAS, SUS SUCESORES, CESIONARIOS, AGENTES, PROVEEDORES (INCLUIDOS LOS PROVEEDORES DE SERVICIOS DE USO), DISTRIBUIDORES AUTORIZADOS POR BLACKBERRY (INCLUIDOS TAMBIÉN LOS PROVEEDORES DE SERVICIOS DE USO) Y SUS RESPECTIVOS DIRECTORES, EMPLEADOS Y CONTRATISTAS INDEPENDIENTES.

ADEMÁS DE LAS LIMITACIONES Y EXCLUSIONES MENCIONADAS ANTERIORMENTE, EN NINGÚN CASO NINGÚN DIRECTOR, EMPLEADO, AGENTE, DISTRIBUIDOR, PROVEEDOR, CONTRATISTA INDEPENDIENTE DE BLACKBERRY O CUALQUIER AFILIADO DE BLACKBERRY ASUMIRÁ NINGUNA RESPONSABILIDAD DERIVADA DE O RELACIONADA CON LA DOCUMENTACIÓN.

Antes de instalar, usar o suscribirse a cualquiera de los Productos y servicios de terceros, es su responsabilidad asegurarse de que su proveedor de servicios de uso ofrezca compatibilidad con todas sus funciones. Es posible que algunos proveedores de servicios de uso no ofrezcan la función de exploración de Internet con una suscripción a BlackBerry® Internet Service. Consulte con su proveedor de servicios acerca de la disponibilidad, arreglos de itinerancia, planes de servicio y funciones. La instalación o el uso de Productos y servicios de terceros con productos y servicios de BlackBerry pueden precisar la obtención de una o más patentes, marcas comerciales, derechos de autor u otras licencias para evitar que se vulneren o infrinjan derechos de terceros. Usted es el único responsable de determinar si desea utilizar Productos y servicios de terceros y si se necesita para ello cualquier otra licencia de terceros. En caso de necesitarlas, usted es el único responsable de su adquisición. No instale o utilice Productos y servicios de terceros hasta que se hayan adquirido todas las licencias necesarias. Cualquier tipo de Productos y servicios de terceros que se proporcione con los productos y servicios de BlackBerry se le facilita para su comodidad "TAL CUAL" sin ninguna condición expresa e implícita, aprobación, garantía de cualquier tipo por BlackBerry, y BlackBerry no asume ninguna responsabilidad en relación con ellos. El uso de los Productos y servicios de terceros estará sujeto a la aceptación de los términos de las licencias independientes aplicables en este caso con terceros, excepto en los casos cubiertos expresamente por una licencia u otro acuerdo con BlackBerry.

Los términos de uso de cualquier producto o servicio de BlackBerry se presentan en una licencia independiente o en otro acuerdo con BlackBerry aplicable según corresponda. NADA DE LO DISPUESTO EN LA PRESENTE DOCUMENTACIÓN SUSTITUIRÁ NINGÚN ACUERDO EXPRESO POR ESCRITO NI NINGUNA GARANTÍA QUE PROPORCIONE BLACKBERRY PARA PARTES DE CUALQUIER PRODUCTO O SERVICIO DE BLACKBERRY QUE NO SEA ESTA DOCUMENTACIÓN.

BlackBerry Enterprise Software incluye software de terceros. La información de licencia y copyright asociada a este software está disponible en http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canadá N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
Reino Unido

Publicado en Canadá