# Política de uso de datos aceptable de TWG

| | |
|---|---|
| **Área geográfica:** | Todo el mundo |
| **Propietario de la política:** | Gerente de seguridad informática de TWG |
| **Título de la política:** | Política de uso de datos aceptable de TWG |
| **Fecha de entrada en vigencia:** | 15 de junio de 2016 |
| **Versión:** | 4.0 |
| **Fecha de la próxima revisión:** | 15 de junio de 2020 |
| Todas las políticas están sujetas a las leyes de los lugares donde opera la empresa. Estas políticas están sujetas a cambio sin previo aviso | |

Solo para uso INTERNO Y CONFIDENCIAL

# Índice

## Antecedentes

The Warranty Group, Inc. (en adelante “TWG”) reconoce que los empleados necesitan acceder a los datos y a los recursos informáticos de TWG para desempeñar sus funciones laborales. Esta Política describe las condiciones bajo las cuales los empleados pueden acceder a los datos de TWG mediante el uso de los recursos informáticos de TWG, así como también los dispositivos móviles personales de los empleados.

## Objetivo

La finalidad de esta Política de uso de datos aceptable de TWG es brindar una comprensión cabal de los términos y las condiciones bajo los cuales se proporciona el acceso a los recursos informáticos de TWG. Además, esta Política establece los requisitos y las restricciones para acceder a los datos de TWG a través de un dispositivo móvil que sea o no propiedad de TWG.

## Alcance

Esta Política rige para todos los empleados de TWG a nivel mundial, lo que incluye contratistas, consultores, empleados temporales y otras personas que actúan en nombre de TWG o que tienen acceso a los recursos informáticos de TWG.

## Definiciones

*Los titulares de cuenta* son personas a las que se les han concedido los permisos de cuentas de computadoras para acceder y utilizar los recursos informáticos de TWG.

*Dispositivo propiedad del empleado:* se refiere a cualquier teléfono celular o móvil, tableta, asistente portátil de datos (Portable data assistant, PDA), computadora de escritorio, computadora portátil u otro dispositivo que un empleado utilice para acceder a los datos de TWG que es de propiedad personal del empleado y que no fue suministrado por TWG.

*Cifrado*: procedimiento usado para convertir data a partir de su formato original a un formato ilegible y/o inutilizable para cualquier persona que no posea las herramientas/la información requerida para reversar el proceso de cifrado.

*Malware*: software definido como un programa (de intención o impacto) malicioso como un virus, gusano y spyware.

*Información personal:* es cualquier dato o información que, en forma aislada o en combinación con otra información en poder del destinatario de la información, pueda utilizarse para establecer razonablemente la identidad única de una persona, y en algunas jurisdicciones, la información comercial de una persona o la identidad de una organización. Los ejemplos de información personal incluyen: nombre completo, domicilio, dirección de correo electrónico, matrícula del vehículo, fecha de nacimiento, número de teléfono, lugar de nacimiento, identidad digital, religión, información sexual, raza u origen étnico, género, información de salud, información de tarjeta de pago, número de licencia de conducir, número de seguro social, número de identificación nacional.

*Medios extraíbles:* dispositivos o medios que pueden ser leídos o reescritos por el usuario final y que pueden ser trasladados de computador en computador sin modificación al computador. Incluye los dispositivos de memoria como pendrives, tarjetas SD, reproductores de MP3, discos duros extraíbles (incluyendo dispositivos de MP3 con disco duro), discos ópticos como los CD o DVD; y discos de software no suministrados por TWG.

*Información personal delicada:* es un tipo de información personal que, por lo general, implica mayores obligaciones en virtud de la ley aplicable. Las definiciones de datos delicados varían según el país y estado. Por ejemplo, en Europa, la definición de información personal delicada, por lo general, abarca información sobre raza u origen étnico, afiliaciones y opiniones políticas, creencias religiosas o filosóficas, membresía en sindicatos e información sobre salud o sexualidad. En los Estados Unidos, por lo general, se considera información personal delicada la información médica, el número del Seguro Social, la información de tarjetas de pagos, la información de la licencia de conducir y la información de cuentas financieras.

*Datos de TWG* se refiere a cualquier información relacionada con los asuntos comerciales o actividades de TWG, o su trabajo en TWG, incluidos, entre otros, la información personal o la información personal delicada definida arriba y en el estándar global de privacidad.

*Los recursos tecnológicos de TWG* o *Recursos de TI de TWG* incluyen computadoras centrales, servidores, computadoras de escritorio y portátiles, dispositivos móviles, redes, software, archivos de datos, instalaciones, almacenamiento en la nube autorizado por TWG, de acuerdo a la definición del Apéndice A.

## Declaraciones y principios de la política

**Condiciones de uso de los datos de TWG:**

Todos los titulares de cuenta son responsables del acceso y el uso adecuados de los datos de TWG. Los titulares de cuenta deben cumplir con los procedimientos y las políticas de TWG relacionados con los activos y datos de TWG, incluidos el Código de conducta y ética comercial, el estándar global de privacidad y la Política de retención de registros aplicable.

TWG se reserva el derecho (con o sin motivo alguno) para controlar, acceder y revelar todos los datos creados, enviados, recibidos, procesados y almacenados en los recursos de TI de TWG. En algunos casos, es posible que el personal y la Seguridad de TI controlen los Recursos de TI de TWG para garantizar la integridad del sistema y para realizar tareas relacionadas con la gestión de recursos. En caso de una investigación de uso indebido de los recursos de TI de TWG, TWG puede inspeccionar, sin previo aviso, los contenidos de los archivos, correos de voz, correos electrónicos y cualquier material relacionado almacenado o generado por la computadora, como la impresión de documentos.

**Responsabilidades de los titulares de cuenta:**

- Un titular de cuenta será el único usuario de su cuenta. Un titular de cuenta no puede compartir una cuenta con otro usuario y el titular de cuenta es el único responsable del trabajo realizado en la cuenta.
- Una cuenta solo se puede usar con el fin expreso de respaldar las operaciones comerciales de TWG.
- Los titulares de cuenta son responsables de la protección de sus contraseñas. Debe resguardarse la confidencialidad de las contraseñas y nunca se las debe compartir con ninguna persona por ningún motivo. Cualquier titular de cuenta que se sienta presionado por cualquier otra persona para revelar una contraseña o sospecha que su cuenta está en peligro debe comunicarse inmediatamente con el equipo de seguridad de TI o el funcionario de cumplimiento de normas internacionales.
- Las contraseñas no pueden escribirse ni enviarse por correo electrónico sin cifrarse. Si la empresa tiene un requisito para almacenar contraseñas, estas deben almacenarse de forma segura.
- Los titulares de cuenta son responsables de bloquear y etiquetar cualquier recurso informático de TWG cuando no se utilice o cuando el titular de cuenta se haya alejado de su

escritorio. El titular de cuenta es responsable si una persona no autorizada tiene acceso a la cuenta o si la cuenta se utiliza para realizar una función no autorizada.

- El acceso a los datos de TWG debe estar limitado a la menor cantidad de personas posible con la menor cantidad de privilegios necesarios (*p. ej.*, solo lectura).
- Todos los titulares de cuenta que usen cifrado deben conservar las claves, las contraseñas u otros medios necesarios para descifrar la información. Los métodos y los medios para descifrar deben ser provistos al supervisor, gerente, propietario de los datos, gerente de unidad de negocios correspondiente, Seguridad de TI y/o a Recursos Humanos previa solicitud. El uso del cifrado debe estar autorizado y debe cumplir con las normas de cifrado de la empresa que se detallan en la sección Normas de cifrado.

**Actividades prohibidas:**

- Los titulares de cuenta no pueden utilizar ningún dato o recurso tecnológico de TWG para fines ilegales o no autorizados ni para infringir las leyes locales, estatales o federales ni las políticas de TWG.
- Los titulares de cuenta no pueden participar en ningún comportamiento malicioso que dañe o interfiera con el uso de los recursos tecnológicos de TWG de otros titulares de cuenta.
- Los titulares de cuenta no pueden usar los recursos tecnológicos ni los datos de TWG para fines comerciales.
- Los titulares de cuenta no pueden interrumpir los servicios de red o alterar las restricciones o protecciones de software, lo que incluye la introducción de programas maliciosos en los sistemas de TWG.
- Los titulares de cuenta no pueden realizar ofertas fraudulentas de productos, artículos o servicios originados de y mientras utilizan cualquier recurso tecnológico de TWG.
- Los titulares de cuenta no pueden realizar ningún tipo de monitoreo de la red, incluidos, entre otros, robots web, registradores de teclas, etc., que interceptará los datos que no serán usados para el fin específico del titular de cuenta.
- Los titulares de cuenta no pueden utilizar material registrado o protegido por derechos de autor que aparezca en los recursos tecnológicos de TWG, a menos que: (i) TWG sea propietario de los materiales; (ii) TWG haya cumplido con las leyes de propiedad intelectual que existen sobre los materiales, incluidas las restricciones de exportación; o (iii) el titular de cuenta haya obtenido autorización para usar el material o la aprobación del Departamento de TI de TWG. Los titulares de cuenta deben cumplir con todas las condiciones de cualquier licencia que obtengan.
- Los titulares de cuenta no deben transmitir información personal delicada sin cifrar por Internet. Los métodos y las instrucciones para el cifrado se detallan en el Apéndice B.
- El sistema de correo electrónico de TWG se debe usar para toda la correspondencia de correo electrónico comercial de TWG. Los empleados no pueden utilizar cuentas de correo electrónico externas o que no sean de TWG para los correos electrónicos con fines comerciales. Esto incluye enviar datos de TWG a una dirección de correo electrónico personal de un titular de cuenta por comodidad.

**Normas que rigen para los dispositivos propiedad del empleado:**

Por comodidad, los titulares de cuenta pueden optar por usar un dispositivo propiedad del empleado para acceder a los datos de TWG para desempeñar sus funciones laborales. Se aplican las siguientes nomas para el uso de los dispositivos propiedad del empleado:

*Acceso a los datos de TWG:*

- Los titulares de cuenta que son empleados exentos pueden usar un dispositivo propiedad del empleado para acceder a los datos de TWG. Los empleados no exentos solo pueden acceder a los datos de TWG a través de un dispositivo propiedad del empleado durante el

horario de trabajo habitual, a menos que esté autorizado por escrito por el gerente del empleado.

- Los usuarios de dispositivos propiedad del empleado deben respetar todas las disposiciones detalladas anteriormente en relación con los recursos tecnológicos de TWG, que incluyen el cumplimiento con todas las políticas aplicables de TWG.
- Los titulares de cuenta no pueden almacenar los datos de TWG (*es decir*, guardar los documentos, archivos, fotos de TWG, etc.) en un dispositivo propiedad del empleado ni en un almacenamiento en la nube que no esté aprobado por TWG. Todos los datos originales de TWG deben almacenarse en los recursos tecnológicos de TWG.
- Los usuarios de dispositivos propiedad del empleado deben velar por que no se produzca un acceso no autorizado a los datos de TWG en dicho dispositivo.
- Todos los dispositivos propiedad del empleado deben estar protegidos con una contraseña o un código.
- Al acceder a los datos de TWG desde un dispositivo propiedad del empleado, los titulares de cuenta aceptan que TWG puede:
    - acceder de forma remota a dicho en caso de una investigación o retención legales que involucre a un titular de cuenta; y
    - bloquear de forma remota, el acceso o eliminar los datos de TWG del dispositivo, que puede ocasionar la pérdida involuntaria de sus elementos personales (*p. ej.*, correos electrónicos, correos de voz, fotografías, *etc.*) en caso de pérdida o robo de un dispositivo propiedad del empleado, o al terminar la relación laboral.
- Los titulares de cuenta deben mantener los dispositivos propiedad del empleado actualizados con todas las definiciones de antimalware (dentro de los últimos 3 días), todas las actualizaciones pertinentes a la seguridad y a los parches para el sistema operativo (dentro de los 2 últimos meses) y todas las actualizaciones de las aplicaciones centrales (dentro de los últimos 2 meses).
- Los titulares de cuenta solo pueden usar un dispositivo propiedad del empleado que utilice un sistema operativo autorizado por TWG. Los titulares de cuenta son responsables de mantener el sistema operativo del dispositivo propiedad del empleado actualizado. Los sistemas operativos autorizados de TWG están detallados en el Apéndice C.
- Los dispositivos propiedad del empleado deben tener el cifrado activado en el dispositivo (*es decir,* Microsoft Bitlocker para dispositivos con sistema operativo Windows).
- Si fuera exigido por orden judicial, el dispositivo propiedad del empleado y/o los medios de almacenamiento deben ser entregados al Departamento Legal de TWG como parte de la retención legal.

*Cambio en los dispositivos propiedad del empleado:*

Cuando un titular de cuenta reemplaza o actualiza su dispositivo propiedad del empleado, el dispositivo propiedad del empleado debe ser ¨restablecido a condiciones de fábrica¨ antes de realizar el reemplazo o la actualización para así eliminar cualquier dato de TWG que pueda ser almacenado automáticamente por el dispositivo (datos de la ¨memoria caché¨). Un dispositivo propiedad del empleado no puede ser vendido, donado, descartado ni desechado sin ser ¨restablecido a condiciones de fábrica¨ para asi eliminar todos los datos de TWG. Si un titular de cuenta desea obtener ayuda para reestablecer su dispositivo a las condiciones de fábrica, él/ella debe contactar al servicio de asistencia informática local.

En el caso de que un dispositivo propiedad del empleado se pierda o sea robado, el titular de cuenta debe informar inmediatamente la pérdida o el robo al equipo de seguridad de la información de TWG y cambiar todas las contraseñas relacionadas con TWG. El equipo de seguridad de la información de TWG tomará las medidas adecuadas para bloquear o eliminar los datos de TWG del dispositivo extraviado en medida de lo posible, y puede solicitar una copia de un informe policial en caso del robo del dispositivo.

*Soporte de los departamentos de TWG:*

El soporte para los dispositivos propiedad del empleado se limita al soporte de acceso básico. No se brindará ningún soporte para el mantenimiento de los dispositivos propiedad del empleado además del software compatible de TWG.

TWG no será responsable de ninguna pérdida o daño de la información personal almacenada en un dispositivo propiedad del empleado.

*Terminación del contrato o la relación laboral:*

Al momento de terminarse el contrato o la relación laboral con el empleado, el titular de la cuenta debe eliminar cualquier aplicación usada para acceder a los datos de TWG. En el caso de aplicaciones utilizadas con múltiples cuentas, como Outlook móvil, el titular de la cuenta debe eliminar la cuenta de TWG de dichas aplicaciones.

*Medios extraíbles:*

El personal de TWG sólo puede usar medios extraíbles en sus computadoras de trabajo cuando sea necesario para el cumplimiento de las funciones asignadas o cunado responda a solicitudes legítimas de información. El equipo de seguridad de la información de TWG debe aprobar su uso antes de que cualquier dato sea almacenado en el medio extraíble. Cualquier dato almacenado en medios extraíbles debe ser encriptado en cumplimiento de la política de encriptado de TWG.

Para prevenir la violación accidental de esta política, los puertos USB de todas las computadoras de TWG estarán inhabilitados para el uso de dispositivos extraíbles.

También debe tomar en consideración que cualquier dato de TWG almacenado en un medio extraíble debe cumplir con la política global de retención de registros y cualquier política local de retención de registros aplicables.

**Excepciones**:

Cualquier pregunta o solicitud relacionada con las excepciones de esta política deben ser enviadas al Gerente de seguridad de la información de TWG.

## Revisión y aprobación de la política

Esta política será aprobada por la oficina del director de seguridad de la información (Chief Information Security Officer, CISO). Esta política se revisará y actualizará dos veces al año o según sea necesario debido a cambios en las normativas o en los asuntos comerciales.

## Documentos relacionados

- Código de conducta y ética comercial
- Estándar global de privacidad
- Política global de retención de registros y cualquier política local de retención de registros

## Planilla de control de documentos

**Modificaciones**

- **Este documento ha sido modificado por:**

| Nombre | Firma | Cambios realizados | Fecha de aprobación | Versión/ Estado |
|---|---|---|---|---|
| Khai Waterman | | Inclusión de la sección de medios extraíbles y actualización general | 19 de febrero de 2018 | 4.0 |

**Aprobaciones**

- **Este documento ha sido aprobado por:**

| Nombre | Firma | Cambios realizados | Fecha de aprobación | Versión/ Estado |
|---|---|---|---|---|
| Oficina del CISO | | Inclusión de la sección de medios extraíbles y actualización general | 19 de febrero de 2018 | 4.0 |

## Apéndice A: almacenamiento en la nube autorizado por TWG

La lista a continuación describe los sistemas de almacenamiento en la nube que actualmente están autorizados para el uso con los datos de TWG. Esta lista se puede actualizarse o modificarse oportunamente, a medida que se realicen cambios en la tecnología utilizada por TWG. Antes de usar el almacenamiento en la nube con los datos de TWG, asegúrese de haber consultado la versión más actualizada de este Apéndice A.

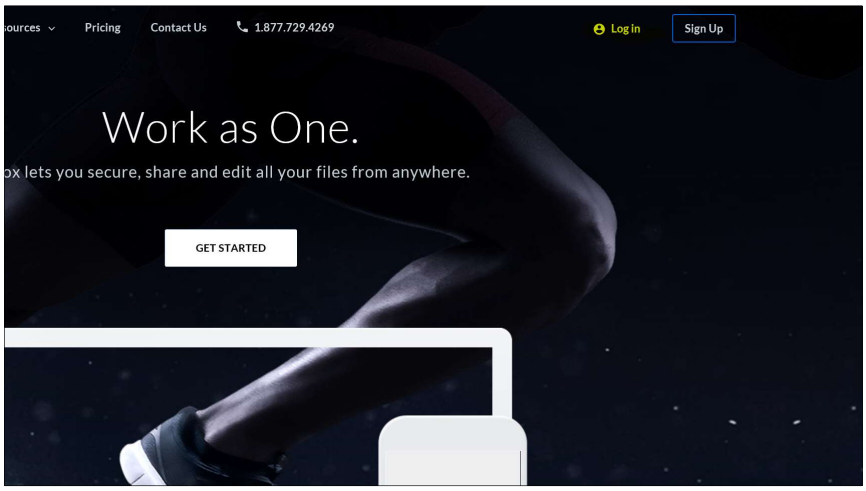
- Box
- Office 365 (incluye OneDrive)
- Salesforce
- Workday
- Cornerstone
- Host Analytics
- SpringCM
- AWS
- Azure
- DrawLoop

Última actualización: 12 de febrero de 2018

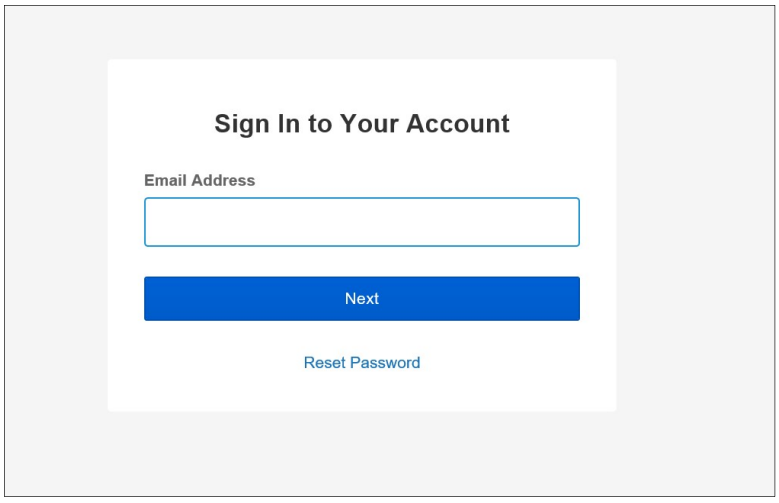
## Apéndice B: métodos e instrucciones de cifrado

Según se detalla en la política, toda la información personal delicada debe ser transmitida de forma segura por Internet. Como primera opción, use Box para transmitir cualquier información personal delicada fuera de la empresa (vea las instrucciones detalladas a continuación). Si se requiere de un método alternativo (como MoveIt o correo electrónico seguro), comuníquese con el Gerente de seguridad informática de TWG.

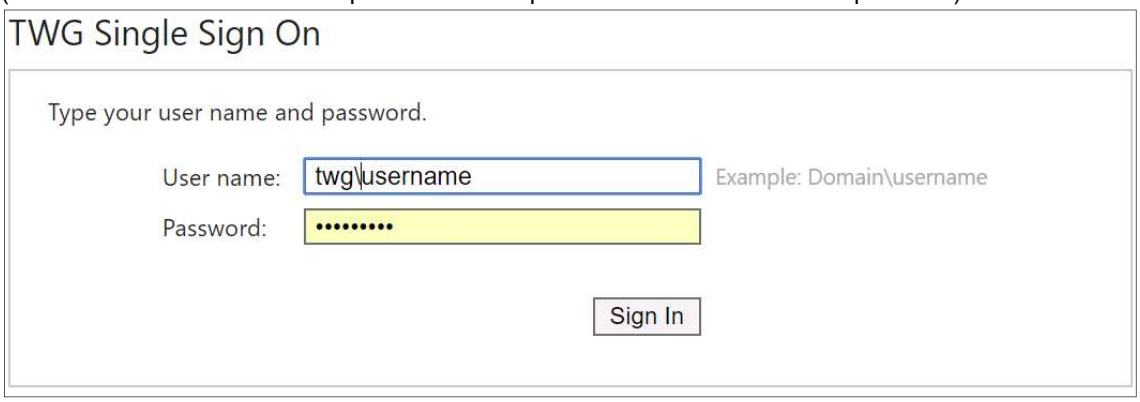
- Box
  1. Visite www.box.com
  2. Haga clic en el enlace en la parte superior derecha **Iniciar sesión**



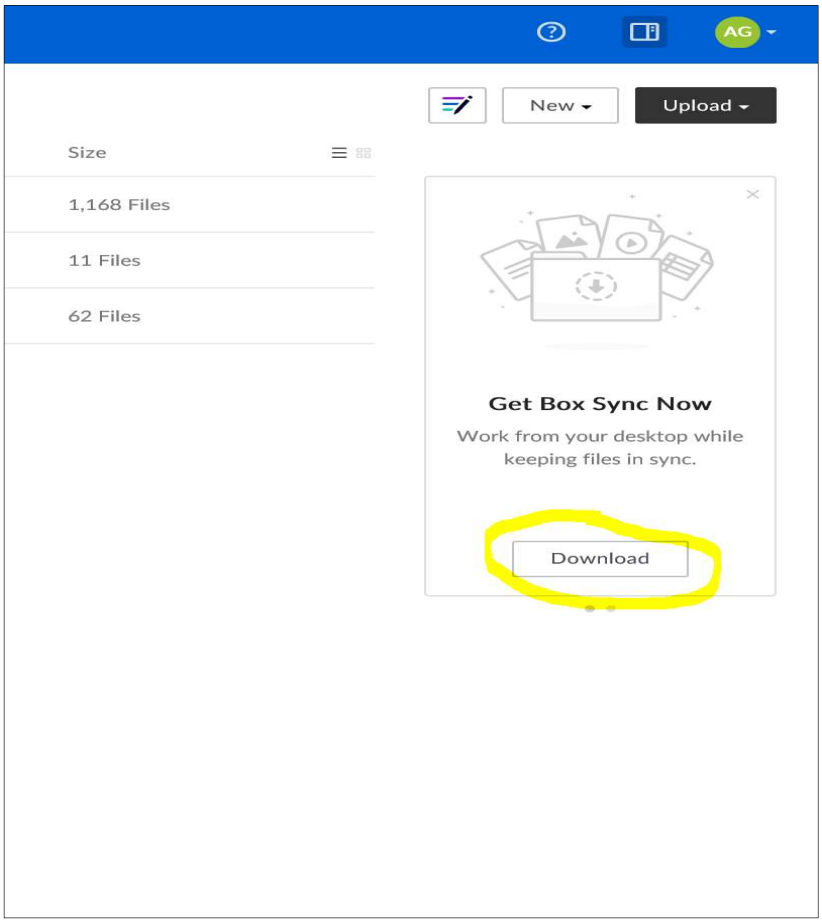

  3. Ingrese su dirección de correo electrónico de TWG o haga clic en **Siguiente**



4. Ingrese su información de inicio de sesión en el siguiente formato: **twg\Nombredeusuario** (Este es el nombre de usuario que usted utiliza para iniciar sesión en su computadora)




5. Ahora usted debe iniciar sesión en Box.com
6. Para sincronizar los archivos almacenados en Box.com con su computadora, usted necesita descargar e instalar **Box Sync.** Haga clic en el botón de **Descarga** debajo de su nombre.




7. Si utiliza IE, haga clic en “Ejecutar” y siga las instrucciones que aparecen en la pantalla. Si utiliza Chrome, se guardará en su carpeta de Descargas. Haga doble clic en el archivo para ejecutarlo y siga las instrucciones que aparecen en la pantalla para instalarlo.

## Apéndice C: sistemas operativos autorizados de TWG para los dispositivos propiedad del empleado

La lista a continuación describe los sistemas operativos que están autorizados actualmente para los dispositivos propiedad del empleado. Ocasionalmente, esta lista se puede actualizar o modificar a medida que se realicen cambios en la tecnología. Antes de usar un dispositivo propiedad del empleado para acceder a los datos de TWG, asegúrese de haber consultado la versión más actualizada de este Apéndice C.

Versiones más actualizadas y completamente parcheadas de:

- iOS
- Apple OSX
- Android
- Windows 10