CERTIFICADOS TÉRMINOS DE USO - CERTIFICATE TERMS OF USE

Las presentes condiciones de uso de los certificados digitales (**"Certificate Terms of Use "**) se aplican a cada certificado digital (**"Certificado"**), independientemente del tipo de Certificado, ya sean Certificados TLS/SSL de confianza pública, Client Certificates (según se definen en la Sección 9), Certificados Cualificados (según se definen en la Sección 10), Certificados X9 (según se definen en la Sección 29), u otros tipos, emitidos por DigiCert, Inc., una corporación de Utah o cualquiera de sus filiales, incluidos sus prestadores cualificados de servicios de confianza (colectivamente, **"DigiCert"**) a una entidad o persona (**"Cliente"**), según se identifica en el portal de gestión de servicios de DigiCert y/o API relacionada puesta a disposición del Cliente (**"Portal"**) o Certificado emitido. Los Certificate Terms of Use se aplican independientemente de cuándo el Cliente solicitó el Certificado o cuándo se emitió el Certificado. La cuenta para acceder y utilizar el Portal en nombre del Cliente se denomina en el presente documento la "**Cuenta del Portal**".

Al aceptar o firmar un acuerdo que incorpora estos Certificate Terms of Use por referencia (dicho acuerdo, junto con estos términos, colectivamente, el "**Acuerdo**"), el aceptador o firmante (el "**Firmante**") declara y garantiza que (i) actúa como representante autorizado del Cliente en cuyo nombre el Firmante acepta este Acuerdo, y está expresamente autorizado a firmar el Acuerdo y vincular al Cliente al Acuerdo, (ii) tiene la facultad de obtener el equivalente digital del sello, el timbre o la firma de un directivo de la empresa para acreditar (x) la autenticidad del sitio web del Cliente y (y) que el Cliente es responsable de todos los usos del Certificado; (iii) está expresamente autorizado por el Cliente para aprobar solicitudes de Certificados en nombre de este, y (iv) ha confirmado o confirmará el derecho exclusivo del Cliente a utilizar el dominio o dominios que se incluirán en cualquier Certificado emitido.

Con respecto a cualquiera de los Certificados expedidos por DigiCert al Cliente en virtud del presente Acuerdo, las partes reconocen y convienen que juntos, los Certificate Terms of Use y el presente Acuerdo constituyen el acuerdo de suscriptor, tal y como exigen las normas, directrices y requisitos aplicables del sector referentes a la emisión de Certificados (incluidas las Directrices de Validación Extendida [EV, por sus siglas en inglés], en la forma en que se definen a continuación).

El Cliente y DigiCert acuerdan lo siguiente:

1. **Usuarios de la cuenta.**

El Cliente autoriza a cada persona enumerada como administrador en la Cuenta del Portal a actuar como Solicitante de Certificado, Aprobador de Certificado y Firmante de Acuerdo (según se define en las Directrices de EV) y a comunicarse con DigiCert en relación con la gestión de Certificados y conjuntos de claves. Por **"Directrices de EV"** se entienden las Extended Validation Guidelines publicadas por el CA/Browser Forum (**"CAB Forum"**) y disponibles públicamente en www.cabforum.org. El Cliente puede revocar esta autoridad enviando una notificación a DigiCert. El Cliente es responsable de revisar y reconfirmar periódicamente qué personas tienen autoridad para solicitar y aprobar Certificados. Si el Cliente desea eliminar un usuario de la Cuenta del Portal, el Cliente tomará las medidas necesarias para evitar el acceso de dicho usuario al Portal, incluido el cambio de su contraseña y otros mecanismos de autenticación para su Cuenta del Portal. El Cliente debe notificar a DigiCert inmediatamente si se detecta cualquier uso no autorizado del Portal o de la Cuenta del Portal. El cliente afirma que: (i) el Cliente autoriza a DigiCert a escanear, recopilar y recabar datos pertinentes a los servicios de DigiCert y a automatizar la renovación y actualización del Certificado; (ii) el Cliente utilizará los servicios para escanear y automatizar solo los dominios, direcciones IP o activos que el Cliente posee o controla; (iii) el Cliente utilizará los servicios solo para su propósito previsto descrito y comercializado por DigiCert y de acuerdo con la Política de uso aceptable de DigiCert ubicada en https://www.digicert.com/legal-repository.

2. **Solicitudes.**

El Cliente solo podrá solicitar certificados para nombres de dominio registrados a su nombre, a nombre de una empresa asociada suya o de otra entidad que autorice expresamente a DigiCert a permitir que el cliente obtenga y gestione certificados para dicho nombre de dominio. DigiCert puede limitar el número de nombres de dominio que el Cliente puede incluir en un único Certificado a la entera discreción de DigiCert.

3. **Verificación.**

Después de recibir una solicitud de Certificado por parte de un Cliente, DigiCert revisará la solicitud e intentará verificar la información relevante de acuerdo con la Certification Practices Statement de DigiCert y las normas, directrices y requisitos aplicables del sector, incluidas las leyes y normativas relacionadas con la emisión de Certificados ("**Normas del sector**").

La verificación de dichas solicitudes está sujeta a la entera discreción de DigiCert, y DigiCert puede negarse a emitir un Certificado por cualquier motivo o sin motivo. DigiCert notificará al Cliente si se rechaza una solicitud de Certificado, pero no se requiere que DigiCert proporcione un motivo para el rechazo. **"Certification Practices Statement "** o **"CPS"** se refiere a las declaraciones escritas aplicables de las políticas y prácticas utilizadas por DigiCert para operar su infraestructura de clave pública (**"PKI"**), incluidas las Políticas y Declaraciones de sello de tiempo aplicables. Los CPS de DigiCert están disponibles en https://www.digicert.com/legal-repository. Los CPS para servicios emitidos por un QTSP (ya sea actuando en su calidad de QTSP o de otro modo) o una entidad afiliada están disponibles en https://www.quovadisglobal.com/repository.

4. Ciclo de vida del certificado.

El ciclo de vida de un Certificado emitido depende de la selección realizada por el Cliente al solicitar el Certificado, los requisitos del CPS y el uso previsto del Certificado. DigiCert puede modificar los ciclos de vida de los Certificados no emitidos según sea necesario para cumplir con los requisitos de: (i) el Acuerdo; (ii) las Normas del sector; (iii) los auditores de DigiCert; o (iv) un Proveedor de software de aplicación. "**Proveedor de software de aplicación**" es una entidad que muestra o utiliza Certificados en relación con una Root store distribuida en la que participa o participará DigiCert. El Cliente acepta dejar de utilizar un Certificado y su Private Key relacionada (definida a continuación) después de la fecha de vencimiento del Certificado o después de que DigiCert revoque un Certificado según lo permitido en el Acuerdo.

5. Emisión.

Si la verificación de un certificado se lleva a cabo a satisfacción de DigiCert, esta emitirá y entregará el certificado solicitado al cliente mediante cualquier medio de entrega razonable. Por lo general, DigiCert entregará los Certificados por correo electrónico a una dirección indicada por el Cliente, mediante descarga electrónica en el Portal o en respuesta a una llamada a la API realizada por el Cliente a través del Portal. Los Certificados de confianza pública se emiten a partir de un Root Certificate o un Intermediate Certificate seleccionado por DigiCert. DigiCert puede cambiar en cualquier momento y sin previo aviso al Cliente el Root Certificate o el Intermediate Certificate que utiliza para emitir Certificados. El Cliente cumplirá con todas las leyes, reglamentos y Normas del sector aplicables al solicitar y utilizar Certificados, incluidas las leyes y reglamentos de control de exportaciones y sanciones económicas de los Estados Unidos. El Cliente reconoce que los Certificados no están disponibles en países o regiones restringidos por la Oficina de Control de Activos Extranjeros del Departamento del Tesoro de los Estados Unidos, el Departamento de Comercio de los Estados Unidos, la Comisión Europea, la Oficina de Implementación de Sanciones Financieras del Tesoro del Reino Unido HM u otras agencias gubernamentales aplicables que tengan jurisdicción sobre DigiCert.

6. Licencia de Certificado.

Con efecto inmediato al iniciar una solicitud de un Certificado y hasta que el Certificado caduque o se revoque, el Cliente solo podrá utilizar, en beneficio del sujeto del Certificado, cada Certificado emitido y los servicios relacionados (ya sean realizados antes o después de la emisión del Certificado) y el Conjunto de claves correspondiente para los fines descritos en el CPS, de acuerdo con todas las leyes, reglamentos, Normas del sector y con los términos del presente documento. Todos los certificados en los que confían los proveedores de software de aplicación están sujetos a todos los requisitos de las normas del sector aplicables, incluidos los que figuran en las políticas de Root store de los proveedores de software de aplicación y en el CPS, independientemente del uso que se haga de dichos certificados. Queda prohibido todo uso que no esté permitido por los Normas del sector aplicables o el CPS. DigiCert desaconseja encarecidamente el anclaje ([g1]pinning[/g1]) de certificados o claves, el uso de certificados de confianza para la web con una PKI no web, o cualquier otro uso de los certificados que dificulte al cliente el cumplimiento de los plazos de revocación u otros requisitos de la CPS, y dicho uso no se considerará una razón suficiente para retrasar la revocación. Por **"Conjunto de claves"** se entiende un conjunto de dos o más claves matemáticamente relacionadas, denominadas Private Keys o fragmentos de clave, junto con una Public Key. (i) Con la Public Key se puede cifrar un mensaje que solo se puede descifrar con la Private Key o las Private Keys. (ii) Aun conociendo la Public Key, no es viable computacionalmente descubrir la Private Key o las Private Keys. El Cliente informará de inmediato a DigiCert si tiene conocimiento de un uso indebido de un Certificado, una Private Key o el Portal. El Cliente es responsable de obtener y mantener cualquier autorización o licencia necesaria para solicitar, usar y distribuir un Certificado a los usuarios finales y sistemas, incluida cualquier licencia requerida por las leyes de exportación de los Estados Unidos.Los certificados SSL pueden utilizarse en uno o más servidores o dispositivos físicos a la vez; sin embargo, DigiCert puede cobrar una tarifa por el uso de certificados en servidores o dispositivos adicionales.

7. Juegos de claves.

Una **"Private Key"** es la clave que el Cliente mantiene en secreto y que se utiliza para crear firmas digitales, descifrar registros o archivos electrónicos cifrados con la Public Key correspondiente, o ambas cosas. Una **"Public Key"** es la clave del Cliente divulgada públicamente que figura en su Certificado y corresponde a la Private Key que el Cliente mantiene en secreto. El Cliente deberá (i) generar Conjuntos de claves con sistemas fiables, (ii) utilizar Conjuntos de claves que ofrezcan como mínimo un nivel de seguridad equivalente al de las claves RSA de 2048 bits y (iii) mantener la confidencialidad de todas las Private Keys. El Cliente es el único responsable de cualquier incumplimiento en la protección de sus Private Keys. El cliente declara que solo generará y almacenará conjuntos de claves para Signing Certificates de Adobe y EV Code Signing Certificates en un dispositivo FIPS 140-2 Nivel 2. Todos los demás tipos de certificados pueden almacenarse en sistemas de software o hardware seguros. El Cliente es responsable de garantizar que la adquisición, el uso o la aceptación por parte del Cliente de los Conjuntos de claves generados por DigiCert de conformidad con el Acuerdo cumpla con las leyes, normas y reglamentos locales aplicables, incluidas, entre otras, las leyes, normas y reglamentos de exportación e importación, en la jurisdicción en la que el Cliente adquiera, utilice, acepte o reciba de otro modo dichos Conjuntos de claves. Si se permite al Cliente importar o exportar Private Keys (incluidas copias) en relación con su uso de servicios específicos de DigiCert, DigiCert no será responsable ante el Cliente del uso o almacenamiento por parte del Cliente de Private Keys (incluidas copias) que no se creen en el Portal o servicio aplicable o que se utilicen fuera de dicho Portal o servicio, incluso después de que se exporten desde el Portal o servicio aplicable.

8. Publicación de la información de los Certificados.

Sin perjuicio de cualquier disposición en contrario contenida en las presentes Certificate Terms of Use o en cualquier otro acuerdo entre el Cliente y DigiCert, el Cliente da su consentimiento para: (i) que DigiCert divulgue públicamente la información (como el nombre de dominio del Cliente, la jurisdicción de constitución o la información de contacto) incluida en un certificado emitido; y (ii) que los certificados del Cliente y la información incluida en ellos sean registrados por DigiCert o en su nombre en bases de datos de transparencia de certificados de acceso público con el fin de detectar y prevenir ataques de phishing y otras formas de fraude, y el Cliente acepta que dicha información, una vez registrada, no podrá ser eliminada del servidor de registros. Dicha publicación de la información de Certificación se realizará de acuerdo con el CPS aplicable.

9. Client Certificates .

"Client Certificate " es un Certificado que contiene cualquier valor de extendedKeyUsage distinto de codeSigning, timestamping o serverAuthentication. Los usos del Client Certificate son variados y están definidos por el perfil del Client Certificate . Algunos de los posibles usos definidos en un perfil del Client Certificate pueden incluir firma digital, cifrado de correo electrónico y autenticación criptográfica. Si el Cliente desea solicitar Client Certificates , el Cliente debe (i) confirmar la identidad y afiliación del solicitante utilizando la documentación interna adecuada según lo prescrito en el CPS, y (ii) confirmar que la información proporcionada y las declaraciones relacionadas con o incorporadas en cualquier Client Certificate son verdaderas, completas y precisas en todos los aspectos sustanciales.

10. Certificados cualificados.

"Certificado Cualificado" se refiere a un Certificado (i) emitido por un prestador cualificado de servicios de confianza de conformidad con los requisitos de la legislación aplicable de la UE o de Suiza en materia de certificación y firma electrónica, y (ii) que cuente con el nivel de garantía más alto, es decir, "cualificado", de conformidad con dichos requisitos.

"**Qualified Trust Service Provider**" o "**QTSP**" se refiere a una entidad afiliada de DigiCert que está certificada por las autoridades gubernamentales para emitir Certificados Cualificados. Los QTSP de DigiCert son los siguientes:

Entidad QTSP	**Lista de confianza**	**Jurisdicción del organismo de supervisión**
QuoVadis Trustlink B.V.	Lista de confianza de los Países Bajos	Países Bajos
DigiCert Europe Belgium B.V.	Lista de confianza de Bélgica	Bélgica
QuoVadis Trustlink Schweiz AG	Lista de confianza Suiza	Suiza

"**Servicios QTSP**" se refiere a los Servicios emitidos por el QTSP de DigiCert (según se define anteriormente) (ya sea actuando en su calidad de QTSP o de otro modo) o sus Filiales.

Si el Cliente adquiere Servicios QTSP, entonces el CPS aplicable para ciertos Servicios QTSP se encuentra en https://www.quovadisglobal.com/repository/. Con respecto a los Certificados Cualificados, el Cliente (i) cuando los Normas del sector exijan el uso de un Dispositivo de Creación de Firma Cualificado (QSCD), solo utilizará sus Certificados

Cualificados para las firmas electrónicas generadas utilizando el QSCD que almacena los Certificados Cualificados, (ii) si el Cliente es una persona física, mantendrá y utilizará sus Private Keys solo bajo su control exclusivo; y (iii) si el Cliente es una entidad u organización jurídica, mantendrá y utilizará sus Private Keys solo bajo su control y dirección.

11. Gestión.

Por lo general, DigiCert emitirá, gestionará, renovará y revocará un Certificado de acuerdo con las instrucciones enviadas por el Cliente a través del Portal y puede confiar en la precisión de dichas instrucciones. El Cliente proporcionará información precisa y completa cuando se comunique con DigiCert y notificará a DigiCert en un plazo de 5 días hábiles si cambia cualquier información relacionada con su cuenta en el Portal. El Cliente responderá a cualquier consulta de DigiCert con respecto a la validez de la información proporcionada por el Cliente en un plazo de 5 días hábiles después de que el Cliente reciba la notificación de la consulta. El Cliente revisará y verificará los datos del Certificado antes de utilizar el Certificado para verificar su exactitud. Los Certificados se consideran aceptados por el Cliente treinta (30) días después de la emisión del Certificado, o antes tras el uso del Certificado cuando existan pruebas de que el Cliente utilizó el Certificado. Aunque DigiCert puede enviar un recordatorio sobre los Certificados que vencen, DigiCert no tiene ninguna obligación de hacerlo y el Cliente es el único responsable de garantizar que los Certificados se renueven antes de su vencimiento. Por "**día hábil**" se entiende de lunes a viernes, excluidos los días festivos federales de EE. UU., tal y como se establecen en el artículo 6103 del título 5 del Código de los Estados Unidos (5 U.S.C. § 6103).

12. Registration Authority .

A excepción de los Certificados TLS/SSL de confianza pública y los Certificados Cualificados, el Cliente es designado como Registration Authority (y por el presente el Cliente acepta dicho nombramiento) de conformidad con los términos del CPS aplicable. En relación con los Certificados TLS/SSL de confianza pública, el Cliente es designado como Enterprise RA (y por el presente el Cliente acepta dicho nombramiento) de conformidad con los términos del CPS aplicable. En la medida en que el Cliente desempeñe cualquier función de una Registration Authority o Enterprise RA, lo hará de conformidad con el CPS aplicable, y DigiCert puede confiar en las acciones del Cliente cuando actúe como Registration Authority o Enterprise RA. En la medida en que una reclamación, demanda, procedimiento o resolución judicial de terceros se derive de que el Cliente no haya cumplido estrictamente las obligaciones de una Registration Authority o Enterprise RA, el Cliente deberá defender, mantener indemnes e indemnizar a DigiCert y a sus directores, directivos, agentes, empleados, sucesores y cesionarios frente a dicha reclamación. Si opera como una Registration Authority o Enterprise RA, el Cliente hará que sus suscriptores que reciban los Certificados en virtud del presente cumplan con los términos del contrato de suscriptor de DigiCert, que se encuentra en https://www.digicert.com/subscriber-agreement. Los suscriptores del Cliente deben aceptar el contrato del suscriptor antes de recibir los Certificados. "**Enterprise RA**" tiene el significado que se le da en la versión actual de los Requisitos básicos del Foro CAB, disponibles en https://cabforum.org/baseline-requirements-documents/, según se actualicen ocasionalmente.

13. Seguridad y uso de conjuntos de claves.

El Cliente generará y protegerá de forma segura los Conjuntos de claves asociados con un Certificado y tomará todas las medidas necesarias para evitar el compromiso, la pérdida o el uso no autorizado de una Private Key asociada con un Certificado. El Cliente utilizará contraseñas que cumplan con los requisitos especificados por los requisitos de seguridad de la red del foro CAB y otros requisitos relevantes para cumplir con las mejores prácticas. El Cliente solo permitirá que sus empleados, agentes y contratistas accedan a las Private Keys o las utilicen si dichos empleados, agentes o contratistas han sido sometidos a una verificación de antecedentes por parte del Cliente (en la medida en que lo permita la ley) y cuentan con formación o experiencia en PKI y otros ámbitos de la seguridad de la información. El Cliente notificará a DigiCert, solicitará la revocación de un Certificado y su Private Key asociada, dejará de utilizar dicho Certificado y su Private Key asociada, y eliminará el Certificado de todos los dispositivos en los que esté instalado si: (i) cualquier información del Certificado es o se vuelve incorrecta o inexacta, o (ii) existe cualquier uso indebido o compromiso real o sospechado de la Private Key asociada con la Public Key incluida en el Certificado. Para los Code Signing Certificates , el Cliente dejará de utilizar de inmediato un Certificado y su Private Key asociada y solicitará de inmediato la revocación del Certificado si el Cliente cree que (a) cualquier información del Certificado es, o se vuelve, incorrecta o inexacta, (b) la Private Key asociada con la Public Key contenida en el Certificado se utilizó indebidamente o se vio comprometida, o (c) hay evidencia de que el Certificado se utilizó para firmar el Código sospechoso. "**Código sospechoso**" se refiere al código que contiene funcionalidad dañina o maliciosa de cualquier tipo o que contiene vulnerabilidades graves, incluido spyware, malware y otro código que se instala sin el consentimiento del usuario y/o se resiste a su propia eliminación, y código que puede explotarse de formas no previstas por sus diseñadores para comprometer la fiabilidad de las plataformas en las que ejecuta. El cliente no utilizará

la misma Private Key para diferentes tipos de certificados. Por ejemplo, el Cliente no utilizará una Private Key destinada a Code signing para solicitar un Certificado que no sea un Code Signing Certificate . Si DigiCert detecta que una Private Key que se ha utilizado para un determinado tipo de certificado o acción (por ejemplo, Code signing) se está utilizando para solicitar un tipo de certificado diferente (por ejemplo, TLS/SSL o un Client Certificate), DigiCert estará obligada a revocar todos los certificados asociados a dicha Private Key o al conjunto de claves relacionado que se encuentren en la Cuenta del Portal del Cliente o que hayan sido emitidos de cualquier otra forma por DigiCert. El Cliente responderá a las instrucciones de DigiCert relativas al compromiso del Conjunto de claves o al uso indebido del Certificado en un plazo de 24 horas. El Cliente dejará de utilizar de inmediato el Conjunto de claves correspondiente a un Certificado cuando (I) se revoque el Certificado y (II) venza el período de uso permitido para el Conjunto de claves, lo que ocurra primero. Después de la revocación, el Cliente debe dejar de utilizar el Certificado.

Si el Cliente almacena una Private Key que se ha generado para un Code Signing Certificate en un HSM (según se define en el CPS aplicable), el Cliente acepta con respecto a cada una de dichas Private Keys que (w) el Cliente almacena su Private Key de forma segura en un HSM que impide la eliminación de la Private Key, (x) el HSM está bajo el control exclusivo del Cliente o se utiliza a través de una nube auditada (p. ej., Azure o AWS), (y) el Cliente no tiene motivo para creer que dicha Private Key se haya utilizado o se vaya a utilizar fuera del HSM, y (z) la Private Key está protegida en un módulo criptográfico que cumpla o supere el nivel 2 de FIPS 140-2 (o equivalente) o los Criterios comunes EAL4+.

14. Certificados defectuosos.

El único recurso del Cliente por un defecto en un Certificado ("**Defecto**") es exigir a DigiCert que haga todo lo comercialmente posible para subsanar el defecto después de recibir la notificación del Cliente de dicho Defecto. DigiCert no está obligado a corregir un Defecto si (i) el Cliente hizo un uso indebido, dañó o modificó el Certificado, (ii) el Cliente no informó inmediatamente del Defecto a DigiCert, o (iii) el Cliente ha incumplido alguna disposición del Acuerdo.

15. Garantía de la parte confiante.

El Cliente reconoce que la Garantía de la Parte Confiante es solo para beneficio de las Partes Confiantes. "**Garantía de la Parte Confiante**" significa una garantía ofrecida a una Parte Confiante que cumple con las condiciones que se encuentran en el Acuerdo de Parte Confiante y Garantía Limitada publicada en el sitio web de DigiCert en https://www.digicert.com/legal-repository. La Garantía de la Parte Confiante para certificados emitidos por un QTSP o una filial de DigiCert se publica en https://www.quovadisglobal.com/repository. El Cliente no tiene derechos en virtud de la Garantía de la Parte Confiante, incluido cualquier derecho a hacer cumplir los términos de la Garantía de la Parte Confiante o a presentar una reclamación en virtud de la Garantía de la Parte Confiante. "**Parte Confiante**" tiene el significado establecido en la Garantía de la Parte Confiante. Un proveedor de software de aplicación no es una Parte Confiante cuando el software distribuido por el proveedor de software de aplicación simplemente muestra información sobre un certificado o facilita el uso del Certificado o la firma digital.

16. Declaraciones.

Para cada Certificado solicitado, el Cliente declara y garantiza que:

a. El Cliente tiene derecho a utilizar o es el propietario legal de (i) cualquier nombre(s) de dominio especificado en el Certificado, y (ii) cualquier nombre común o nombre de organización especificado en el Certificado;

b. El Cliente utilizará el Certificado únicamente para fines autorizados y legales, incluido no utilizar el Certificado para firmar el Código sospechoso y utilizará el Certificado y la Private Key únicamente de conformidad con todas las leyes aplicables y únicamente de conformidad con el propósito del Certificado, el CPS, cualquier política de certificados aplicable y el Acuerdo;

c. El Cliente ha leído, comprende y acepta el CPS;

d. El Cliente informará inmediatamente por escrito a DigiCert de cualquier incumplimiento del CPS o los Requisitos de referencia; y

e. la organización incluida en el certificado y el titular del nombre de dominio registrado conocen y aprueban cada solicitud de certificado.

17. Restricciones.

El Cliente solo utilizará un Certificado TLS/SSL en los servidores accesibles a los nombres de dominio enumerados en el Certificado emitido. Además, se prohíbe al Cliente:

a. modificar, sublicenciar o crear obras derivadas de un Certificado TLS/SSL (salvo cuando sea necesario para utilizarlo para el fin previsto) o una Private Key;

b. cargar o distribuir archivos o software que puedan dañar el funcionamiento del ordenador de otra persona;

c. hacer declaraciones sobre un Certificado TLS/SSL o utilizarlo, salvo en los casos permitidos en el CPS;

d. suplantar a otra persona o entidad, o falsear la vinculación del Cliente con cualquier entidad;

e. utilizar un certificado o cualquier software o servicio relacionado (como el Portal) de una forma que pudiera dar lugar, de manera razonable, a que se emprendieran acciones civiles o penales contra el Cliente o contra DigiCert;

f. utilizar un Certificado o cualquier software relacionado para quebrantar la confidencialidad de un tercero o para enviar o recibir correspondencia masiva no solicitada;

g. utilizar Code Signing Certificates para firmar Código Sospechoso;

h. solicitar un Code Signing Certificate si la Public Key del Certificado se utiliza o se utilizará con un Certificado que no sea un Code Signing Certificate ;

i. interferir en el funcionamiento del sitio web de DigiCert o en las transacciones realizadas a través de él;

j. intentar utilizar un Certificado para emitir otros Certificados;

k. supervisar la implementación técnica de los sistemas o el software de DigiCert, interferir en ella, aplicar ingeniería inversa a dicha implementación o comprometer deliberadamente de cualquier otro modo la seguridad de esos sistemas o ese software;

l. enviar a DigiCert información de un Certificado que infrinja los derechos de propiedad intelectual de terceros; o

m. crear intencionadamente una Private Key sustancialmente similar a una Private Key de DigiCert o de un tercero.

n. A menos que DigiCert lo autorice expresamente, por escrito, el Cliente no utilizará ningún Certificado de entidad final para firmar ningún Certificado.

18. Revocación de certificados.

DigiCert puede revocar un Certificado sin previo aviso por los motivos indicados en el CPS, incluso si DigiCert cree razonablemente que:

a. El Cliente solicitó la revocación del Certificado o no autorizó la emisión del Certificado;

b. El Cliente está utilizando los Servicios para publicar o hacer accesible cualquier material que infrinja los derechos de DigiCert o de cualquier tercero;

c. El Cliente ha incumplido el Acuerdo o una obligación que tiene en virtud del CPS;

d. cualquier disposición de un acuerdo con el Cliente que contenga una declaración u obligación relacionada con la emisión, uso, gestión o revocación del Certificado se extingue o se considera inválida;

e. El cliente se añade a una lista de personas o entidades prohibidas por el gobierno o está operando desde un destino prohibido según las leyes de los Estados Unidos;

f. el Certificado contiene información inexacta o engañosa;

g. el Certificado se utilizó sin autorización, fuera de su propósito previsto o se utilizó para firmar el Código sospechoso;

h. la Private Key asociada con el Certificado fue divulgada o comprometida;

i. el Certificado fue (i) utilizado indebidamente, (ii) utilizado o emitido en contra de la ley, el CPS o los Normas del sector, o (iii) utilizado, directa o indirectamente, para fines ilegales o fraudulentos, como ataques de phishing, fraude o la distribución de malware, otros fines ilegales o fraudulentos, o cualquier otra infracción según se describe en la Política de uso aceptable de DigiCert; o

j. Las Normas del sector o CPS de DigiCert requieren la revocación del Certificado, o la revocación es necesaria para proteger los derechos, la información confidencial, las operaciones o la reputación de DigiCert o de un tercero.

19. Intercambio de información.

El Cliente reconoce y acepta que si (i) el Certificado o el Cliente se identifica como fuente del Código Sospechoso, (ii) la autoridad para solicitar el Certificado no puede verificarse, o (iii) el Certificado se revoca por motivos distintos a la solicitud del Cliente (p. ej., como resultado de la vulneración de una Private Key, descubrimiento de malware, etc.), DigiCert está autorizado a compartir información sobre el Cliente, cualquier aplicación u objeto firmado con el Certificado, el Certificado y las circunstancias circundantes con otras autoridades de certificación o grupos del sector, incluido el Foro CAB.

20. Normas del sector.

Ambas partes cumplirán con todos los Normas del sector y las leyes aplicables a los Certificados; si dicha ley aplicable o Estándar del sector cambia y ese cambio afecta a los Certificados u otros servicios proporcionados en virtud del Acuerdo, DigiCert podrá alterar los servicios o modificar o rescindir el Acuerdo en la medida necesaria para cumplir con el cambio.

21. Equipo.

El Cliente es responsable, a expensas del Cliente, de (i) todos los ordenadores, equipos de telecomunicaciones, software, acceso a Internet y redes de comunicaciones (si las hubiera) necesarios para utilizar los Certificados y el software o servicios relacionados de DigiCert; y (ii) la conducta del Cliente, así como el mantenimiento, el funcionamiento, el desarrollo y el contenido de su sitio web.

22. Beneficiarios del certificado.

Las Partes Confiantes y los Proveedores de software de aplicación son terceros beneficiarios expresos de las obligaciones y declaraciones del Cliente relacionadas con el uso o la emisión de un Certificado. Las Partes Confiantes y los Proveedores de software de aplicación no son terceros beneficiarios expresos con respecto a ningún software de DigiCert.

23. Intermediate Certificate .

Esta Sección 23 solo se aplica si el Cliente adquiere un Root Certificate y/o Intermediate Certificate dedicado para la emisión de Certificados privados o Certificados de confianza pública según se especifica en un Formulario de pedido.

a. Creación. En un plazo de 60 días tras recibir el pago aplicable en virtud del Acuerdo y la información requerida por DigiCert para crear el Root Certificate y/o el Intermediate Certificate como se describe en el apartado (b) a continuación, DigiCert creará un Root Certificate y/o un Intermediate Certificate para emitir (i) Certificados de confianza no pública a través del Portal o (ii) Certificados de confianza pública como se especifica en un Formulario de pedido. Un "**Certificado privado**" significa un Certificado que no está integrado en ningún almacén de confianza. Un **"Root Certificate "** es un Certificado autofirmado que se almacena de forma segura sin conexión y se utiliza para emitir otros Certificados. **"Intermediate Certificate "** significa un Certificado que está firmado por una Private Key correspondiente a un Root Certificate y que se utiliza para emitir Certificados para su uso por parte del Cliente.

b. Índice. DigiCert y el Cliente trabajarán juntos de buena fe para determinar el contenido adecuado del Root Certificate y/o Intermediate Certificate . El Cliente debe proporcionar a DigiCert toda la información requerida por DigiCert para la creación del Root Certificate y/o Intermediate Certificate dentro de los doce (12) meses posteriores a la conclusión de un acuerdo para la creación de dicho Root Certificate y/o Intermediate Certificate . Si el Cliente no proporciona toda la información requerida dentro de ese plazo, perderá el derecho a solicitar el Root Certificate y/o Intermediate Certificate y DigiCert retendrá cualquier tarifa pagada por la creación del Root Certificate y/o Intermediate Certificate . Después de crear un Intermediate Certificate , el Cliente no podrá modificar el contenido de dicho Intermediate Certificate , pero podrá crear tantas copias idénticas del Intermediate Certificate como sea necesario. Los Intermediate Certificates tienen un ciclo de vida de diez años, tras el cual caducan sin renovación. El Cliente es responsable de garantizar que todos los

Certificados emitidos desde un Intermediate Certificate caduquen al menos dos años antes de la expiración del Intermediate Certificate . DigiCert tiene derecho a revocar cualquier Certificado emitido a partir de un Intermediate Certificate que siga vigente dentro de los dos años siguientes al vencimiento de dicho Intermediate Certificate .

c. Propiedad. DigiCert conserva la propiedad exclusiva del Intermediate Certificate , pero, salvo que se disponga lo contrario en el presente documento, utilizará el Intermediate Certificate emitido en relación con este Acuerdo únicamente de acuerdo con las instrucciones proporcionadas por el Cliente a través del Portal. El Cliente puede generar copias del Intermediate Certificate y distribuir copias del Intermediate Certificate a sus propios usuarios finales y clientes.

d. Alojamiento. DigiCert alojará la Private Key del Intermediate Certificate en los sistemas PKI seguros de DigiCert. El Cliente no puede retirar ni hacer que un tercero retire la Private Key del Intermediate Certificate de los sistemas PKI de DigiCert por ningún motivo. DigiCert proporcionará y alojará servicios CRL/OCSP para el Cliente. DigiCert continuará proporcionando los servicios CRL/OCSP después de la rescisión del Acuerdo hasta que todos los Certificados emitidos en virtud del mismo caduquen o se revoquen. En el caso de un Intermediate Certificate que emita certificados de confianza pública, dado que dicho Intermediate Certificate emite certificados de confianza pública, está alojado en la PKI de DigiCert y es gestionado por el personal de DigiCert, dicho Intermediate Certificate estará incluido en la auditoría WebTrust de DigiCert. Si los Normas del sector o las políticas de un Proveedor de software de aplicación cambian de una manera que requiera una auditoría independiente del Intermediate Certificate , DigiCert y el Cliente trabajarán juntos de buena fe para obtener la auditoría requerida.

e. Revocación. DigiCert tendrá derecho a revocar el Intermediate Certificate si: (i) el Cliente solicita la revocación por escrito a DigiCert, citando una infracción específica de las normas del sector; (ii) DigiCert tiene motivos razonables para creer que el Intermediate Certificate se ha visto comprometido; (iii) el Cliente incumple sustancialmente el Acuerdo y no subsana el incumplimiento en un plazo de 30 días tras recibir la notificación del incumplimiento; (iv) el Cliente continúa utilizando el Intermediate Certificate después de que el derecho del Cliente a utilizar el Intermediate Certificate termine, o (v) DigiCert cree razonablemente que la revocación es requerida por los Normas del sector.

f. Restricciones. El Cliente (i) no creará o intentará crear Intermediate Certificates adicionales a partir del Intermediate Certificate ; (ii) no venderá, distribuirá, alquilará, arrendará, licenciará, cederá o transferirá de otro modo el Intermediate Certificate a un tercero; (iii) no utilizará un Intermediate Certificate proporcionado por DigiCert después de su vencimiento, revocación o rescisión del presente Acuerdo; (iv) no alterará, modificará o revisará un Intermediate Certificate proporcionado por DigiCert; o (v) no utilizará el Intermediate Certificate si el Cliente tiene motivos para creer que la Private Key del Intermediate Certificate se ha visto comprometida.

24. Licencia de marca y Condiciones de terceros.

a. DigiCert podrá poner a disposición del Cliente algunas de sus marcas comerciales y logotipos (cada uno de ellos, una "**Marca**") para que el Cliente pueda indicarlo, con el fin de que este pueda señalar que un certificado concreto expedido en virtud del presente contrato ha sido emitido por DigiCert para un activo concreto del Cliente. Con validez a partir de la emisión del Certificado aplicable, y solo durante el período en que dicho Certificado esté vigente y el Cliente cumpla plenamente todas las condiciones relacionadas con él, DigiCert otorga al Cliente una licencia limitada y revocable durante el período de vigencia del Certificado aplicable para exhibir la Marca correspondiente (en la forma facilitada por DigiCert al Cliente) con el fin de indicar de manera exacta y no engañosa el Certificado aplicable en los productos, nombres de dominio o servicios del Cliente. El Cliente se compromete a no modificar las Marcas de ningún modo (incluido el compromiso de no eliminar ni modificar los avisos de marcas registradas que DigiCert pueda aplicar a dichas marcas) ni utilizar o exhibir las Marcas con fines inadecuados o de cualquier manera que pudiera falsear la relación entre las partes o mermar o dañar la reputación de DigiCert o el prestigio asociado a cualquier Marca u otras marcas registradas o marcas de servicio de DigiCert, lo que incluye utilizar una Marca o Certificado en un sitio web que pueda considerarse asociado a actos de delincuencia, fraude, engaño, difamación, calumnia, obscenidad, apropiación indebida o infracción, o sobre el que DigiCert tenga otros motivos para presentar objeciones. Todo el prestigio logrado en relación con el uso de las Marcas redundará en beneficio de DigiCert y, si el Cliente obtiene cualquier derecho,

título o interés respecto de cualquier Marca como resultado del uso de esta, el Cliente asigna a DigiCert irrevocablemente en virtud del presente documento la totalidad de tal derecho, título e interés.

b. El Cliente reconoce y acepta que si el Certificado del Cliente incluye un identificador de entidad legal ("**LEI**") proporcionado porUbisecure Oy, los Términos de servicio de Ubisecure Oy – RapidLEI disponibles en https://rapidlei.com/documents/global-lei-system-terms/ se aplicarán al LEI del Cliente y al uso del Sistema de gestión de identificadores de entidad legal de RapidLEI o del servicio sucesor.

c. El Cliente reconoce y acepta que el uso por parte del Cliente del kit de herramientas criptográficas postcuánticas (PQC) de DigiCert (el **"PQC Toolkit"**) se regirá por los siguientes términos, además de los términos de cualquier otro acuerdo de licencia aplicable: (i) la licencia otorgada al Cliente en relación con el PQC Toolkit es una licencia no exclusiva y terminable que se utilizará solo en relación con un certificado DigiCert que incluya una firma y Public Key generadas por o con el PQC Toolkit o actividades de prueba y configuración relacionadas; (ii) el Cliente no adquiere ninguna propiedad intelectual u otros derechos de propiedad en el PQC Toolkit o propiedad intelectual relacionada con él; (iii) el Cliente no realizará ingeniería inversa, traducirá, desensamblará, descompilará, descifrará o deconstruirá el PQC Toolkit; (iv) el Cliente dejará de utilizar el PQC Toolkit al finalizar los servicios relacionados de DigiCert; (v) ISARA Corporation no será responsable ante el Cliente por ningún daño; (vi) el cliente importará, exportará y reutilizará el PQC Toolkit únicamente de conformidad con la legislación aplicable de los países o territorios en los que se utilice o importe el PQC Toolkit, o desde los que se exporte o reexporte; (vii) DigiCert no ofrece garantía alguna, ni expresa ni implícita, en relación con el PQC Toolkit en nombre de ISARA Corporation; y (viii) el cliente no modificará ningún aviso de derechos de autor, marca registrada o patente incluido en el PQC Toolkit o en cualquier material relacionado con el mismo.

25. **Requisitos de flujo descendente.** El Cliente no debe supervisar, interferir, realizar ingeniería inversa en la implementación técnica ni comprometer de forma consciente la seguridad de ningún sistema o software DigiCert, y debe imponer la misma restricción a sus fabricantes designados, si los hubiera.

26. **Obligaciones suplementarias requeridas por Adobe**

Si al Cliente se le emiten Signing Certificates de Adobe, el Cliente acepta:

a. Cumplir la AATL Certificate Policy 2.0 de Adobe Systems Inc., disponible actualmente en https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf, lo que incluye, entre otros: (1) generar y almacenar conjuntos de claves para los Signing Certificates de Adobe únicamente en un dispositivo que cumpla con la norma FIPS 140-2 Nivel 2; y (2) al dar de alta una nueva cuenta, o en cualquier momento en que se inicie el proceso de emisión de un nuevo certificado AATL para un suscriptor, facilitar información veraz y precisa a DigiCert, lo que requiere que (A) un administrador de la cuenta lleve a cabo una verificación de identidad rigurosa basada en una reunión presencial con DigiCert o en un procedimiento que ofrezca una garantía equivalente (por ejemplo, mediante una comunicación por vídeo segura), (B) que un administrador de la cuenta lleve a cabo una verificación rigurosa de la identidad basada en una reunión presencial con sus suscriptores (es decir, los usuarios finales), y almacene la grabación localmente para respaldar las auditorías, hasta que DigiCert proporcione un mecanismo en línea para que el administrador suba las certificaciones y las grabaciones; y (C) el proceso de verificación de identidad, tanto si lo lleva a cabo un administrador como un suscriptor, debe incluir la grabación del suscriptor mostrándose a sí mismo y un documento de identidad oficial válido (por ejemplo, permiso de conducir, pasaporte, documento nacional de identidad, etc.) en el que figure una fotografía que coincida con la del suscriptor; y

b. los términos del CPS aplicable.

27. **Restricciones adicionales para Code Signing Certificates** El Cliente no debe utilizar un Code Signing Certificate : (i) para distribuir el Código sospechoso; o (ii) de una manera que exponga o exporte la Private Key relacionada con el Certificado fuera del módulo de seguridad de hardware correspondiente.

Para todos los OV Code Signing Certificates emitidos a partir del 1 de junio de 2023, incluidos los certificados renovados o reemitidos, todas las Private Keys deben almacenarse en hardware certificado como FIPS 140 Nivel 2, Common Criteria EAL 4+ o equivalente. Para todos los OV Code Signing Certificates emitidos antes del 1 de junio de 2023, incluidos los certificados renovados o reemitidos, todas las Private Keys deben almacenarse en tokens de hardware.

28. **Restricciones adicionales para certificados TLS/SSL no públicos**. Los certificados TLS/SSL que se encadenan a un Root Certificate privado deben utilizarse solo con dominios de intranet y no pueden asignarse a dispositivos a los que se pueda acceder públicamente desde Internet. DigiCert se reserva el derecho de supervisar los servidores y/o dispositivos de Internet públicos para garantizar que los Certificados TLS/SSL privados cumplan con esta cláusula. Si DigiCert descubre cualquier uso de certificados TLS/SSL privados que no cumplan con esta cláusula, DigiCert notificará inmediatamente al Cliente el incumplimiento. El Cliente debe, en un plazo de veinticuatro (24) horas, (i) trasladar inmediatamente el Certificado TLS/SSL privado a un dominio de intranet; o (ii) eliminar y revocar el Certificado TLS/SSL privado de los servidores del Cliente. Si el Cliente no revoca o elimina el Certificado que no cumple con los requisitos, DigiCert podrá revocar el Certificado.

29. **Términos adicionales para certificados X9**. Por **"Certificado X9"** se entiende un Certificado emitido por DigiCert o sus filiales en el marco de la infraestructura de clave pública regida por el Accredited Standards Committee X9, Inc. Al adquirir y utilizar Certificados X9, el Cliente actuará de conformidad con los DigiCert X9 PKI Certificate Terms of Use (**"X9 Certificates Terms of Use "**), disponibles en https://www.digicert.com/legal-repository/, en su versión vigente en cada momento. Si existe un conflicto entre estos Certificate Terms of Use y los Certificate Terms of Use X9, prevalecerán los Certificate Terms of Use X9. El Cliente no utilizará Certificados X9 para TLS/SSL de confianza pública, S/MIME de confianza pública o cualquier otro fin fuera del marco de confianza X9, y DigiCert puede revocar cualquier Certificado X9 utilizado fuera de esas restricciones.

30. **Herramientas de comunicación/notificación electrónicas.** Al utilizar el correo electrónico u otras herramientas de comunicación o notificación electrónicas ("**Herramientas de notificación**") proporcionadas por DigiCert para enviar una comunicación o notificación ("**Comunicación**") usted acepta que (1) el contenido de dicha Comunicación se limitará estrictamente a la comunicación o notificación sobre los productos o servicios de DigiCert; (2) cumplirá con la legislación aplicable (incluida la ley de comunicaciones electrónicas aplicable y la ley de privacidad/protección de datos) en las jurisdicciones de los destinatarios de la Comunicación; (3) será el único responsable del contenido de cualquier Comunicación que envíe utilizando las Herramientas de notificación; y (4) indemnizará, defenderá y eximirá de responsabilidad a DigiCert frente a reclamaciones de terceros, acciones o multas reglamentarias gubernamentales, y todas las responsabilidades, daños y costes, incluidos los honorarios razonables de abogados que surjan de su uso de las Herramientas de notificación o el contenido de cualquier Comunicación que envíe utilizando las Herramientas de notificación.

31. **Supervivencia y finalización.** Los Certificate Terms of Use subsistirán a la rescisión del Acuerdo hasta que todos los Certificados emitidos caduquen o se revoquen.