Servicios de certificados y firma
Términos de uso

El Acuerdo correspondiente a los Servicios de Certificados de Entrust, cualesquiera Servicios de Firma Figital, Servicios de Sellado de Tiempo o CA especializadas se componen de estos términos de uso (en adelante, el "Anexo de ECSS"), la CPS y/o la TPS (que se define a continuación), los términos y condiciones generales de Entrust (en adelante, las "Condiciones Generales") expuestos en este Anexo de ECSS y también disponibles en https://www.entrust.com/entrust-certificate-services/repository-general-terms/es, y un Pedido de servicios de certificados, servicios de firma y/o CA especializadas. Los términos en mayúscula que no se definen en el presente documento tienen el significado que se les da en las Condiciones Generales.

A efectos aclaratorios, las partes reconocen y aceptan que el Acuerdo, tal y como se ha definido anteriormente, constituye el acuerdo de suscripción, según lo requerido y definido en los estándares del sector, para todos los certificados emitidos en virtud del presente documento.

Usted, como individuo que acepta el Acuerdo (tal y como se define en las Condiciones Generales), manifiesta y garantiza que está legalmente capacitado para formalizar contratos (por ejemplo, no es menor de edad). Si va a formalizar el Acuerdo en nombre de una entidad jurídica, por ejemplo, la empresa o la organización para la que trabaja, manifiesta que tiene la autoridad legal necesaria para vincular a dicha entidad jurídica. SI NO ACEPTA LOS TÉRMINOS Y CONDICIONES DEL ACUERDO (O NO TIENE LA AUTORIDAD LEGAL REQUERIDA PARA FORMALIZAR CONTRATOS O VINCULAR A LA ENTIDAD JURÍDICA EN CUYO NOMBRE DA DICHA ACEPTACIÓN), NO PODRÁ ACCEDER A LOS SERVICIOS ALOJADOS NI UTILIZARLOS. EL DERECHO CONTINUADO DE ACCESO Y USO DE LOS SERVICIOS ALOJADOS ESTÁ SUPEDITADO AL CUMPLIMIENTO ININTERRUMPIDO DE LOS TÉRMINOS Y CONDICIONES DEL ACUERDO POR PARTE DE USTED (O POR PARTE DE LA ENTIDAD JURÍDICA EN CUYO NOMBRE DA LA ACEPTACIÓN).

En vista de los compromisos establecidos a continuación, cuya idoneidad reconocen las partes, estas acuerdan lo siguiente.

1. Definiciones.

1.1. "**Proveedor de Software de Aplicación**" o "**ASV**" hace referencia a un desarrollador de software de navegador de Internet, software de correo electrónico u otro tipo de software que muestre o utilice certificados, incluidos, entre otros, Adobe, Apple, Google, Intel, Microsoft, Mozilla y Oracle.

1.2. "**Certificado**" hace referencia a un documento digital que, como mínimo: (a) identifica a la autoridad de certificación que lo emite; (b) nombra o identifica de otro modo a un sujeto; (c) contiene una clave pública de un par de claves; (d) identifica su periodo operativo; (e) incluye un número de serie; y (f) está firmado digitalmente por la autoridad de certificación. Hay varios tipos de Certificados que Entrust puede emitir a un suscriptor en función de los servicios de Certificados que se hayan adquirido, por ejemplo (y no de forma exhaustiva), Certificados SSL de OV, Certificados SSL de validación ampliada (en adelante, "**EV**"), Certificados de OV Code Signing, Certificados de EV Code Signing, Certificados de Document Signing, Certificados de Verified Mark (en adelante, "**VMC**"), Certificados de dispositivos móviles, Certificados de Private SSL, Certificados de S/MIME, Certificados de autenticación de sitios web cualificados por eIDAS (en adelante, "**eIDAS QWAC**"), Certificados de autenticación de sitios web cualificados por PSD2 (en adelante, "**PSD2 QWAC**"), Certificados de Qualified Seal de eIDAS (en adelante, "**eIDAS QSealC**"), Certificados de Qualified Seal de PSD2 (en adelante, "**PSD2 QSealC**") y Certificados de Qualified Signature de eIDAS (en adelante, "**eIDAS QSigC**").

1.3. "**Beneficiarios del Certificado**" hace referencia, conjuntamente, a todos los Proveedores de Software de Aplicación con los que Entrust ha formalizado un contrato para incluir los Certificados raíz de Entrust en dicho software de los ASV y todas las partes confiantes que realmente confían en dichos Certificados durante su periodo de validez.

1.4. "**Servicios de Certificados**" hace referencia a los servicios prestados por Entrust en relación con la emisión, administración y revocación de uno o varios Certificados, incluidos los derechos de Foreign Certificate Management, e incluye cualquier Certificado emitido a o para el Cliente de conformidad con el Acuerdo.

1.5. "**CPS**" hace referencia a la versión más reciente de la declaración de prácticas de certificación que se incorpora a modo de referencia en los Certificados emitidos por Entrust, puesto que se puede modificar

cada cierto tiempo de acuerdo con las condiciones de la CPS. Asimismo, se incluye aquí como referencia en el Acuerdo. La CPS aplicable a un Certificado específico depende del tipo de Certificado y puede encontrarse en Internet en http://www.entrust.net/cps o contactando con Entrust. Por ejemplo, los Certificados eIDAS QWAC y PSD2 QWAC se rigen por la versión más reciente del documento "Certification Practice Statement For Qualified Certificates" (Declaración de prácticas de certificación para certificados cualificados); los Certificados de Private SSL se rigen por la versión más reciente del documento "Certification Practice Statement For Private Trust Certificates" (Declaración de prácticas de certificación para certificados de confianza privada); y otros Certificados suelen regirse por la versión más reciente del documento "Certification Practice Statement" (Declaración de prácticas de certificación).

1.6. "**CA Especializada**" hace referencia a una autoridad de certificación emisora que se conecta a una de las CA raíz públicas de Entrust dedicadas a emitir Certificados para el Cliente.

1.7. "**Certificado Externo**" hace referencia a cualquier Certificado que no se emitió a o para el Cliente en virtud de este Anexo de ECSS. En aras de una mayor claridad, entre los Certificados Externos se pueden incluir los Certificados emitidos desde otras cuentas de servicios de administración, los Certificados comprados en el sitio web minorista de Entrust, los Certificados emitidos a partir de otras ofertas de servicios de Entrust (por ejemplo, PKI as a Service) y los Certificados emitidos por terceros.

1.8. "**Derechos de Foreign Certificate Management**" hace referencia a una licencia opcional que permite al Cliente utilizar su cuenta de administración para recibir determinados servicios de administración (como se establece en la Documentación) para un (1) Certificado Externo por cada Derecho de Administración de Certificados Externos adquirido por el Cliente. La cantidad de Derechos de Foreign Certificate Management disponibles para el Cliente se supervisará mediante su cuenta de administración, y el inventario del Cliente de Derechos de Administración de Certificados Externos disponibles se aumentará o disminuirá en una cantidad correspondiente al número de Certificados Externos añadidos a o publicados desde su cuenta de administración.

1.9. "**Servicios Alojados**" hace referencia, en este Anexo de ECSS, a los Servicios de Certificados específicos y cualquier Servicio de Sellado de Tiempo, Servicio de Firma y/o CA Especializada que el Cliente haya adquirido según lo especificado en el Pedido, e incluye una cuenta de administración.

1.10. "**Estándares del Sector**" hace referencia, conjuntamente, a las versiones más recientes de cada uno de los siguientes elementos, en cada caso, que sean aplicables a los distintos tipos de Certificados de confianza pública y Sellos de Tiempo emitidos por Entrust y a las que Entrust está sujeto y vinculado como emisor de dichos Certificados y Sellos de Tiempo:

1.10.1. Los requisitos de referencia del CA/Browser Forum para la emisión y la administración de Certificados de confianza pública.

1.10.2. Las directrices del CA/Browser Forum para la emisión y la administración de Certificados de validación ampliada (en adelante, las "Directrices de EV").

1.10.3. Los requisitos de referencia del CA/Browser Forum para la emisión y la administración de Certificados de Code Signing de confianza pública (en adelante, "BR de Code Signing").

1.10.4. Normas europeas elaboradas por el Comité Técnico del ETSI de Firmas e Infraestructuras Electrónicas.

1.10.5. Requisitos Mínimos de Seguridad para la Emisión de Certificados de Verified Mark aprobadas por AuthIndicators Working Group para VMC (en adelante, los "Requisitos de VMC").

1.10.6. Leyes y normativas.

1.11. "**Cuenta de Administración**" hace referencia a una herramienta de administración de autoservicio alojada por Entrust que identifica al Cliente por su nombre legal completo en el campo "Customer Name" (Nombre del Cliente), realiza un seguimiento de los derechos del Cliente con respecto a los Servicios Alojados y le permite, según corresponda de acuerdo con sus derechos, administrar la emisión, revocación y vencimiento de uno o varios Certificados, así como el acceso y uso de los servicios de firma.

1.12. "**Parte Confiante**" hace referencia a cualquier individuo o entidad que confía en un Certificado válido o en un Sello de Tiempo. Para evitar dudas, un ASV no es una "Parte Confiante" cuando el software distribuido por tal ASV simplemente muestra información sobre un Certificado.

1.13. **“Servicios de Firma**” hace referencia a los servicios prestados por Entrust en relación con la generación, administración y alojamiento de claves para firmar datos hash.

1.14. “**Sujeto**” hace referencia a la Persona o dispositivo identificado en el campo “Subject” (Sujeto) de un Certificado.

1.15. “**Suscriptor**” hace referencia a la Persona que solicita o recibe un Certificado.

1.16. “**Código Sospechoso**” hace referencia a cualquier código o conjunto de instrucciones que contenga funciones malintencionadas o vulnerabilidades graves, incluidos spyware, malware y otros códigos que se instalen sin el consentimiento del usuario y/u opongan resistencia a su propia eliminación, así como el código que pueda aprovecharse de formas no previstas por sus diseñadores para poner en peligro la fiabilidad del entorno informático en el que se ejecuta.

1.17. “**Sello de Tiempo**” significa datos en forma electrónica que vinculan otros datos electrónicos a un tiempo particular estableciendo evidencia de que estos datos existían en ese momento.

1.18. “**Servicios de sellado de tiempo**” se refiere a los servicios ofrecidos por Entrust relacionados con la emisión de uno o más Sellos de Tiempo, e incluye cualquier Sello de Tiempo emitido para el Cliente de conformidad con el Acuerdo.

1.19. "**TPS**" hace referencia a la versión más reciente de la declaración de prácticas de sellado de tiempo que describe las prácticas seguidas por Entrust al emitir el(los) Sello(s) de Tiempo, según se modifique cada cierto tiempo de acuerdo con los términos de la TPS, y que también se incluye en el presente. incorporado por referencia en el Acuerdo. La TPS aplicable a un sello de tiempo específico depende del tipo de sello de tiempo y se puede encontrar en Internet en http://www.entrust.net/cps o poniéndose en contacto con Entrust.

1.20. “**Usuarios**” tiene el significado establecido en las Condiciones Generales y, en este Anexo de ECSS, incluye los agentes del Cliente y todas las Personas que son Sujetos y Suscriptores de Certificados emitidos mediante la Cuenta de Administración del Cliente.

1.21. “**Válido**” hace referencia al hecho de que un Certificado no ha vencido ni se ha revocado.

2. <u>Funcionamiento de la PKI</u>. Cada CPS y cada TPS estableces las prácticas de Entrust para administrar la infraestructura de claves públicas para los Servicios Alojados y proporcionar los tipos de Certificados identificados en la CPS y los Sellos de Tiempo identificados en la TPS, incluido lo siguiente:

(a) Especificación de las políticas y Estándares del Sector aplicables.
(b) Información para las Partes Confiantes.
(c) Periodo de conservación del registro de eventos.
(d) Procedimientos para la resolución de quejas y disputas.
(e) Especificación de las auditorías de conformidad aplicables y otras evaluaciones.
(f) Información de contacto para las preguntas sobre los Certificados y Sellos de Tiempo.
(g) Forma en que se proporciona la información del estado de revocación y el periodo durante el que está disponible.

3. <u>Detalles de los Servicios Alojados.</u> Prestación de los Servicios Alojados. Entrust generará, proporcionará y operará los Servicios Alojados de acuerdo con la CPS, la TPS, la Documentación y los Pedidos del Cliente correspondientes a los Servicios Alojados. Sin perjuicio de lo anterior:

3.1. Servicios de Certificados: verificación, emisión y revocación de Certificados. Al recibir la solicitud de un Certificado, Entrust realizará la verificación limitada de la información incluida en la solicitud según lo descrito en la CPS en relación con el tipo de Certificado aplicable. Después de completar dicha verificación, Entrust emitirá los Certificados y hará que estén disponibles para su recuperación y administración si y como se establece en la CPS, la Documentación y los derechos del Cliente en virtud de su Pedido de Servicios de Certificados. Entrust puede rechazar las solicitudes de Certificados por los motivos establecidos en la CPS. Entrust tiene derecho a revocar un Certificado que haya emitido si el Cliente solicita su revocación, al vencimiento o resolución del Acuerdo, o por cualquier otra razón identificada para la revocación en el Acuerdo, la CPS o los Estándares del Sector.

3.2. Servicios de Firma. Al recibir una solicitud de generación de claves, Entrust generará y alojará un par de claves, y las pondrá a disposición del Cliente para su uso en relación con un Certificado para el que el

Cliente o una de sus Filiales sea el Suscriptor y/o el Sujeto, todo ello si y como se establece en la CPS, la Documentación y los derechos del Cliente en virtud de su Pedido de Servicios de Firma.

3.3. Servicios de Sellado de Tiempo. Al recibir una solicitud de Sello de Tiempo, Entrust emitirá un Sello de Tiempo, tal y como se establece en la TPS, la Documentación y los derechos del Cliente en virtud de su Pedido de Servicios de Sellado de Tiempo.

3.4. CA Especializada. Si un Pedido precisa que se proporcionen una o varias CA Especializadas al Cliente para su uso, Entrust alojará y operará cada CA Especializada de acuerdo con la CPS, la Documentación y los derechos del Cliente en virtud de su Pedido de CA Especializadas. Los detalles de la CA Especializada, como el Sujeto que se identificará en el Certificado de la CA Especializada, los tipos de Certificados que emitirá la CA Especializada y cualquier otra limitación o requisito se especificarán en un anexo por escrito formalizado mutuamente por las partes o en el Pedido de la CA Especializada. Cualquier anexo de CA Especializada se incluye en el "Acuerdo" para la CA Especializada. La CA Especializada y sus claves serán propiedad de Entrust y estarán bajo su control. El periodo de validez del Certificado de CA para una CA Especializada no será superior al de la CA raíz que lo emitió, pero Entrust puede revocarlo si el Cliente lo solicita, al vencimiento o resolución del Plazo de la Oferta, o por cualquier otra razón identificada para la revocación en el Acuerdo, la CPS o los Estándares del Sector.

3.5. Revisiones de los Servicios Alojados. Entrust puede modificar las características y funcionalidades de los Servicios Alojados en cualquier momento. Además, Entrust puede añadir, reducir, eliminar o revisar los niveles de servicio en cualquier momento cuando se haya modificado un acuerdo de nivel de servicio de un tercero aplicable a un Servicio Alojado. En caso de que cualquier modificación perjudique de manera sustancial al Cliente, Entrust realizará los esfuerzos comercialmente razonables para remitirle una notificación por escrito con sesenta (60) días de antelación (el correo electrónico o la publicación de un aviso en el sitio web de Entrust constituye una notificación por escrito).

4. Concesión de derechos.

4.1. Uso general. Con sujeción al cumplimiento del Acuerdo por parte del Cliente (y de los Usuarios), Entrust concede al Cliente, durante el Plazo de la Oferta, el derecho personal, de alcance mundial, no exclusivo, intransferible y no susceptible de sublicenciamiento a acceder a los Servicios Alojados y utilizarlos, a brindar a sus Usuarios la posibilidad de acceder a los Servicios Alojados y utilizarlos, y a distribuir Certificados emitidos por los Servicios de Certificados, en cada caso únicamente (a) de acuerdo con este Anexo de ECSS y la CPS y/o la TPS, como corresponda; (b) de acuerdo con la Documentación; (c) de acuerdo con cualesquiera especificaciones o limitaciones establecidas en el Pedido o impuestas por medios tecnológicos (como un código de licencia proporcionado por Entrust) de las capacidades de los Servicios Alojados que el Cliente pueda usar, como las limitaciones asociadas a los tipos o niveles de suscripción, y la cantidad o tipos de Certificados, Sellos de Tiempo, identidades, Usuarios, firmas o dispositivos adquiridos; y (d) con sujeción a las restricciones generales establecidas en la sección 3 de las Condiciones Generales (Restricciones).

4.2. Uso de evaluación. Entrust podrá, a su entera discreción, proporcionar al Cliente acceso a y derecho a utilizar cualquiera de los Servicios Alojados con fines de evaluación, en cuyo caso, independientemente de cualquier disposición contraria incluida en el Acuerdo, se aplicará esta sección 4.2 (Uso de evaluación) o un acuerdo de evaluación independiente formalizado por las partes. Con sujeción al cumplimiento por parte del Cliente de todas las restricciones, las condiciones y obligaciones recogidas en las Condiciones Generales, este Anexo de ECSS, la CPS y/o la TPS, como corresponda, y un Pedido aplicable (si corresponde), durante sesenta (60) días, el Cliente podrá, únicamente según sea necesario para la evaluación de un Servicio Alojado por parte del Cliente, acceder al Servicio Alojado y utilizarlo en exclusiva en, desde y/o en relación con un entorno de prueba (no de producción) del Cliente (y cuyo entorno solo contiene, a efectos aclaratorios, datos ficticios que no son de producción). En aras de una mayor claridad, los Certificados emitidos en lo que concierne a una evaluación de Servicios de Certificados (en adelante, los "Certificados de Prueba") tendrán un periodo operativo máximo de 60 días y no se podrán utilizar con fines de producción. Las pruebas de rendimiento y seguridad están expresamente excluidas de los fines de evaluación y estrictamente prohibidas. Entrust, a su entera discreción, puede ampliar el periodo de evaluación por escrito. Los fines de evaluación excluyen cualquier fin por el que el Cliente (o cualesquiera de sus Usuarios) genere ingresos. Las secciones 4.1 (Uso general), 8 (Servicios de Asistencia), 14.1 (Plazo de la Oferta) y 19 (Publicidad) no se aplican a ninguna evaluación del Servicio Alojado. Entrust puede, a su entera discreción, suspender o dar por terminados cualquier acceso de evaluación y otros derechos de evaluación del Servicio Alojado en cualquier momento, por cualquier motivo o sin él y sin previo aviso. El Cliente revocará todos y

cada uno de los Certificados de Prueba pendientes cuando haya completado la evaluación, pero, en cualquier caso, antes de la finalización del periodo de evaluación o cualquier cuenta de prueba creada para la evaluación. Por el presente, el Cliente autoriza a Entrust a revocar todos y cada uno de los Certificados de Prueba pendientes al finalizar el periodo de evaluación o cualquier cuenta de prueba creada para la evaluación.

5. Funciones, responsabilidades y manifestaciones y garantías del Cliente.

5.1. Agentes. Un Suscriptor puede ejercer sus derechos y obligaciones con respecto a los Servicios de Certificados a través del Cliente o de determinados Usuarios designados para cumplir con las funciones establecidas en el Anexo A, con sujeción a los requisitos de verificación o confirmación aplicables establecidos en la CPS, como la verificación de que una persona que solicita Certificados de EV es un "Solicitante de Certificados" verificado según las Directrices de EV (en adelante, los "**Agentes**"). Los Agentes designados pueden identificarse en el Anexo A, o bien se proporcionarán a Entrust durante la inscripción. Dicha designación podrá modificarse a través de los medios establecidos por Entrust cada cierto tiempo. El Suscriptor acepta que Entrust tiene derecho a contar con las instrucciones facilitadas por los Agentes con respecto a los Servicios Alojados como si las hubiera proporcionado el propio Suscriptor.

5.2. Usuarios de los Servicios de Firma. El Cliente puede ejercer sus derechos y obligaciones con respecto a los Servicios de Firma a través de determinados Usuarios designados por el Cliente a su entera discreción (en adelante, los "**Usuarios de los Servicios de Firma**"). Dicha designación podrá modificarse a través de los medios establecidos por Entrust cada cierto tiempo. El Cliente acepta que es responsable del cumplimiento del Acuerdo por parte de los Usuarios de los Servicios de Firma y del uso de las claves alojadas por los Servicios de Firma por parte de los Usuarios de los Servicios de Firma.

5.3. Manifestaciones y garantías. El Cliente cumplirá los requisitos establecidos en el Anexo B según corresponda cuando actúe en calidad de Suscriptor o Sujeto. El Cliente notificará a todos sus Usuarios, Filiales y cualquier otra Persona que actúe en calidad de Suscriptor, Sujeto, Agente o Usuario de los Servicios de Firma (por ejemplo, que solicite, reciba, gestione o se le emitan Certificados, o bien utilice los Servicios de Firma para generar claves y/o firmar datos hash) en virtud del presente Anexo de ECSS a través de la Cuenta de Administración del Cliente que deben cumplir los requisitos establecidos en este Acuerdo (incluidos los establecidos en el Anexo B) según corresponda a las actividades y funciones de los Suscriptores, Sujetos, Agentes y Usuarios de los Servicios de Firma en relación con los Servicios Alojados y los Certificados. Asimismo, el Cliente será responsable de garantizar dicho cumplimiento. El Cliente manifiesta y garantiza a Entrust y a todos los Beneficiarios del Certificado que el Cliente tiene la autoridad necesaria para vincular a todos los Suscriptores al Acuerdo si y en la medida en que dichos Suscriptores reciben algún Certificado en virtud de este Anexo de ECSS a través de la Cuenta de Administración del Cliente. El Cliente manifiesta y garantiza que cada uno de sus Usuarios de los Servicios de Firma ha o habrá obtenido los derechos y autorizaciones necesarios para el uso de las claves alojadas por los Servicios de Firma por parte de los Usuarios de los Servicios de Firma.

5.4. Sujetos independientes. En el caso de algunos Certificados, según lo permitido por la CPS aplicable, por ejemplo, Certificados de dispositivos móviles, Certificados de S/MIME y determinados Certificados de Document Signing (en adelante, los "Certificados de Cliente"), el Sujeto del Certificado puede ser un individuo diferente al Suscriptor. Si el Pedido del Cliente le da derecho a algún Certificado de Cliente, el Cliente acepta que dichos Certificados de Cliente solo se emitirán y distribuirán a tales Sujetos de conformidad con la versión más reciente del Acuerdo de Certificados de Cliente (que puede encontrarse en http://www.entrust.net/cps) y siempre que (i) el Suscriptor haya verificado que la información incluida en cada Certificado de Cliente es precisa; (ii) la persona a la que se emita dicho Certificado de Cliente haya dado su consentimiento para la inclusión de todos los datos que se incorporan en dichos Certificados de Cliente; (iii) el individuo al que se emita dicho Certificado de Cliente haya sido notificado acerca de sus obligaciones de acuerdo con la sección 5.3 (Manifestaciones y Garantías) anterior; y (iv) dicho Certificado de Cliente se utilice únicamente para actividades relacionadas con el Suscriptor.

5.5. Componentes alojados por el cliente. Si el Pedido del Cliente para un Servicio alojado incluye componentes de Software en las instalaciones, o si el Cliente utiliza productos o servicios de terceros en relación con el Servicio alojado (colectivamente, "Productos Alojados por el Cliente"), el Cliente será responsable de la gestión del ciclo de vida (parches, actualizaciones, etc.) de dichos Productos Alojados por el Cliente y la seguridad del entorno donde instala y utiliza dichos Productos Alojados por el Cliente. El Cliente implementará medidas de seguridad comercialmente razonables con respecto a los Productos Alojados

por el Cliente y el entorno donde están instalados. Sin perjuicio de lo anterior, el Cliente: (i) operará los Productos Alojados por el Cliente en un entorno con medidas de seguridad física, personal y electrónica apropiadas; y (ii) para cualquier Producto Alojado por el Cliente que sea o incluya software, utilizará siempre la versión actual de dicho software e instalará rápidamente los parches de seguridad y las actualizaciones requeridas para el correcto funcionamiento de todas las funciones del Servicio Alojado. El Cliente comprende que si no cumple con esta Sección, podría crear un riesgo de seguridad y/o afectar negativamente el funcionamiento del Servicio Alojado y Entrust puede tener derecho a suspender el Servicio Alojado de acuerdo con la Sección 15 (Suspensión). Además, es posible que el Cliente no pueda acceder a nuevas características o funciones del Servicio Alojado si no cumple con esta Sección.

5.6. Requisitos de Red. El Cliente es responsable de adquirir, mantener, monitorear y respaldar su infraestructura de comunicaciones, red (LAN o WAN) y todos los componentes que se conectan a los Servicios Alojados. Entrust no asume ninguna responsabilidad sobre la confiabilidad o el rendimiento de las conexiones descritas en este párrafo para dicha infraestructura externa, ni por la degradación del servicio o los fallaos causadas por la conectividad de red de dicha infraestructura externa.

5.7. Dispositivos. Para los Certificados emitidos a dispositivos, el Cliente es responsable de garantizar que los dispositivos relevantes admitan y sean interoperables con los Certificados.

5.8. Acceso no autorizado. El Cliente tomará todas las medidas razonables para evitar el acceso no autorizado a los Servicios Alojados, incluso asegurando, protegiendo y manteniendo la confidencialidad de sus credenciales de acceso. El Cliente es responsable de cualquier acceso y uso de los Servicios Alojados a través de la Cuenta de Administración del Cliente o mediante las credenciales de acceso del Cliente, así como de toda la actividad que tenga lugar en la Cuenta de Administración del Cliente. El Cliente notificará a Entrust de inmediato ante cualquier conocimiento o sospecha de uso no autorizado de los Servicios Alojados o vulneración de su seguridad en relación con los Servicios Alojados y hará todos los esfuerzos comercialmente razonables para detener dicha vulneración o uso no autorizado. Lo anterior no disminuirá la responsabilidad del Cliente con respecto a todos sus Usuarios.

6. <u>Manejo de información particular.</u> A efectos del presente Anexo de ECSS, la definición de “Información Confidencial” en las Condiciones Generales no incluye ninguna información que sea contenido en la nube (definido a continuación), que, en su lugar, está sujeta a esta sección (Manejo de información particular).

6.1. Información de administración. Entrust puede almacenar información relacionada con la Cuenta de Administración y el Pedido del Cliente, e información generada por la utilización del Servicio Alojado por parte del Cliente, como las credenciales de acceso del Cliente, la información de contacto de los Agentes y el uso de derechos (en adelante, la “Información de Administración”) en Estados Unidos y/o Canadá, y puede procesar la Información de Administración con fines de facturación, prestación de Asistencia e investigación de fraude, uso indebido o infracciones de este Acuerdo en Estados Unidos, Canadá y otros lugares en los que Entrust mantiene a su personal de asistencia e investigación.

6.2. Bases de datos de terceros. Al realizar una verificación limitada, Entrust puede determinar si la identidad de la organización, la dirección y el nombre de dominio proporcionados con una solicitud de Certificado son acordes a la información incluida en las bases de datos de terceros (en adelante, las “Bases de Datos”). Entrust puede realizar una investigación con la intención de confirmar determinados datos personales (según lo definido en la última versión del DPA de Entrust) y otra información, como el nombre comercial del Cliente, la dirección postal, el número de teléfono, la línea de negocio, el año de inicio, el número de empleados, el director ejecutivo y la existencia comercial del Cliente (conjuntamente, la “Información de Verificación”). El Cliente reconoce que parte de la Información de Verificación puede incluirse en las Bases de Datos.

6.3. Información del certificado. Entrust puede insertar en un Certificado cualquier información que se proporcione a Entrust en la solicitud asociada del Certificado, lo que puede incluir la Información de Verificación (en adelante, la “Información del Certificado”). Entrust también puede (a) utilizar la información que le facilita el Cliente para autenticar a los Suscriptores, (b) publicar los Certificados del Cliente en uno o varios registros de CT (Certificate Transparency) que pueden verse de manera pública y (c) usar dicha información para los fines establecidos en el Acuerdo y en la política de privacidad de Entrust.

6.4. Contenido en la nube. El término “Contenido en la Nube” hace referencia a la Información de Administración, la Información de Verificación y la Información del Certificado, así como a cualquier dato, texto u otro contenido que el Cliente o cualquier Usuario transfiera a Entrust para su procesamiento, almacenamiento o alojamiento por parte de los Servicios de Firma y cualquier resultado informático que el

Cliente o cualquier Usuario derive de lo anterior a través de su uso del Servicio de Firma. El Cliente sabe y consiente que Entrust procesará y/o transferirá el Contenido en la Nube en Norteamérica y en cualquier otra jurisdicción donde Entrust o cualesquiera de sus Filiales tenga presencia y pueda almacenar en la nube el Contenido en la Nube. Entrust puede acceder al Contenido en la Nube y utilizarlo para prestar los Servicios Alojados o, según sea necesario, para cumplir la legislación o un pedido vinculante de un organismo gubernamental.

6.5. Riesgos de la nube. Aunque el Contenido en la Nube puede cifrarse, el Cliente reconoce que existen riesgos inherentes al almacenar, transferir y procesar de cualquier otro modo datos en la nube, y que Entrust no tendrá ninguna responsabilidad ante el Cliente por la falta de disponibilidad del Contenido en la Nube o por cualquier daño, robo, acceso no autorizado, puesta en riesgo, alteración o pérdida que se produzca en el Contenido en la Nube o cualquier dato almacenado en, transferido a o de, o procesado de otra manera por los Servicios Alojados, incluso en tránsito.

6.6. Autorizaciones. El Cliente manifiesta y garantiza que él (y/o los Usuarios) ha o habrá obtenido los derechos y autorizaciones necesarios, y ha realizado las revelaciones precisas a los Usuarios correspondientes u otras terceras partes, de acuerdo con todas las legislaciones, reglas o normativas aplicables, para permitir al Cliente y sus Usuarios transferir el Contenido en la Nube a Entrust. Por el presente, el Cliente otorga a Entrust (incluidos cualesquiera de sus Filiales, subcontratistas o proveedores de servicios de alojamiento pertinentes) todos los derechos y autorizaciones necesarios para la recopilación, el uso y la revelación del Contenido en la Nube de conformidad con el Acuerdo. El Cliente será responsable de la precisión, la calidad y la legalidad del Contenido en la Nube, y de los medios por los que el Cliente lo adquirió.

6.7. Otras disposiciones sobre privacidad. Salvo que se indique lo contrario en esta sección (Manejo de información particular) o en el Acuerdo, Entrust no revelará a ningún tercero ningún Contenido en la Nube que Entrust obtenga durante su prestación de los Servicios Alojados en virtud del presente documento. Sin embargo, Entrust puede poner dicha información a disposición (i) de los tribunales, organismos encargados de velar por el cumplimiento de las leyes u otros terceros (incluida la divulgación en respuesta a una revelación civil) al recibir una orden judicial o citación, o siguiendo los consejos del asesor legal de Entrust; (ii) de los funcionarios encargados de velar por el cumplimiento de las leyes y otras personas con el fin de investigar sospechas de fraude, tergiversación, acceso no autorizado o posible actividad ilegal por parte del Cliente en opinión de Entrust; y (iii) de terceros según sea necesario para que Entrust pueda cumplir con sus responsabilidades en virtud del Acuerdo.

7. **Software**. Si Entrust proporciona algún Software en relación con los Servicios Alojados, por ejemplo, el Signing Automation Client en lo que concierne a un Servicio de Firma, se aplicará el Anexo ofrecido con el Software (en lugar de este Anexo de ECSS). Si no se facilita un Anexo más específico con el Software, el Anexo del Software es la licencia de usuario final que se encuentra disponible en https://www.entrust.com/-/media/documentation/licensingandagreements/certificate-solutions-software-schedule.pdf.

8. **Planes de servicio y servicios de asistencia**. Entrust prevé los compromisos de asistencia establecidos en el anexo de asistencia (disponible en https://www.entrust.com/-/media/documentation/licensingandagreements/entrust-certificate-solutions-hosted-support-schedule-lg.pdf) para los Servicios Alojados y cualquier Software proporcionado en relación con ellos. El “Plan de Servicio Silver”, como se describe en el anexo de asistencia, se incluye sin coste adicional durante el Plazo de la Oferta con una suscripción a uno o varios de los Servicios Alojados. Por una tarifa adicional, se pueden adquirir otros planes de servicio y niveles de asistencia.

9. **Interoperabilidad**. Puede haber complementos o API que permitan que los Servicios Alojados interoperen con productos o servicios de terceros (cada uno de ellos, una “Herramienta de Interoperación”). El Cliente reconoce y acepta que dichas Herramienta de Interoperación no forman parte de los Servicios Alojados, así como que Entrust no otorga derechos, garantías o asistencia para ninguna Herramienta de Interoperación o para la interoperabilidad de los Servicios Alojados con tales Herramientas de Interoperación en virtud del presente Anexo de ECSS. Si el Cliente utiliza cualquier Herramienta de Interoperación, tiene la responsabilidad exclusiva de asegurarse de que cuenta con todos y cada uno de los derechos necesarios para emplear la Herramienta de Interoperación, incluido su uso para transferir cualesquiera datos desde o hacia los Servicios Alojados, y para usar el producto o servicio con el que se conecta. El uso de una Herramienta de Interoperación no crea ninguna relación como subencargado del tratamiento de datos entre Entrust y ningún tercero.

10. <u>RENUNCIA DE GARANTÍA.</u> A efectos del presente Anexo de ECSS, se añade lo siguiente a la renuncia de garantía de las Condiciones Generales: **Entrust no manifiesta ni garantiza que cualquier tercero en particular o producto o servicio de terceros reconozca o considere de confianza cualquier Certificado, Sello de Tiempo o Digital Signature que se cree mediante los Servicios de Firma.**

11. <u>INDEMNIZACIÓN.</u>

11.1. Excepción adicional a la indemnización por IP. Además de las excepciones a la indemnización recogidas en la sección 10.1 (Reclamaciones de propiedad intelectual) de las Condiciones Generales, Entrust no se responsabilizará de ninguna Reclamación de IP con respecto a los Servicios de Certificados si la Reclamación de IP surge de la tecnología que emitió la solicitud de firma del Certificado (CSR) o cualquier información incluida en la CSR, a menos que la CSR la haya generado Entrust.

11.2. Datos adicionales del Cliente y reclamaciones de uso. Además de las obligaciones de indemnización del Cliente que figuran en la sección 10.2 (Datos del Cliente y reclamaciones de uso) de las Condiciones Generales, el Cliente defenderá, indemnizará y eximirá de responsabilidad a Entrust, sus Filiales y licenciantes, así como cada uno de sus respectivos empleados, responsables, directores y representantes frente a cualquier reclamación, demanda, juicio o proceso de terceros, sanción, coste, daño, pérdida, cargo por liquidación y gasto (incluidos los costes de investigación y los honorarios y gastos de abogados) que surja de o esté relacionado con lo siguiente: (a) el incumplimiento por parte del Cliente de las manifestaciones y garantías establecidas en la sección 6.6 (Autorizaciones) o los errores al proporcionarlas; (b) una infracción de la legislación aplicable por parte del Cliente, los Usuarios o el Contenido en la Nube; (c) una alegación de que el Contenido en la Nube infringe los derechos de propiedad intelectual de un tercero o se apropia indebidamente de ellos; y (d) una disputa entre el Cliente y cualquier Usuario (cada uno de los puntos, de la (a) a la (d), se considera incluido en la definición de "Reclamación Indemnizada por el Cliente" en las Condiciones Generales).

12. <u>RESPONSABILIDAD</u>. Además de, y sin limitar la generalidad de, las exclusiones y los límites de responsabilidad recogidos en las Condiciones Generales, las siguientes exclusiones específicas también se aplican a los Servicios Alojados (a efectos aclaratorios, en esta sección, "Entrust" tiene el significado de la sección 11 [Responsabilidad] de las Condiciones Generales):

12.1. **EXCLUSIONES ESPECÍFICAS. EN NINGÚN CASO ENTRUST SERÁ RESPONSABLE, Y EL CLIENTE RENUNCIA A CUALQUIER DERECHO QUE PUEDA TENER, DE CUALQUIER PÉRDIDA O DAÑO QUE NO SE PUEDA ATRIBUIR DIRECTAMENTE AL USO O A LA CONFIANZA DE UN CERTIFICADO, UN SELLO DE TIEMPO O DE LOS SERVICIOS DE CERTIFICADOS O SERVICIOS DE SELLADO DE TIEMPO PROPORCIONADOS EN VIRTUD DEL ACUERDO, LO QUE INCLUYE CUALQUIER PÉRDIDA O DAÑO DERIVADO DE LA COMBINACIÓN O INTEGRACIÓN DEL CERTIFICADO, SELLO DE TIEMPO O DE LOS SERVICIOS DE CERTIFICADOS O DE LOS SERVICIOS DE SELLADO DE TIEMPO CON CUALQUIER SOFTWARE O HARDWARE NO PROPORCIONADO POR ENTRUST SI LA PÉRDIDA O EL DAÑO NO SE HUBIERA PRODUCIDO COMO RESULTADO DEL USO DEL CERTIFICADO O DE LOS SERVICIOS DE CERTIFICADOS ÚNICAMENTE. ADEMÁS, ENTRUST NO SE RESPONSABILIZARÁ EN NINGÚN CASO DE NINGÚN DAÑO A LOS SUSCRIPTORES, PARTES CONFIANTES O CUALQUIER OTRA PERSONA QUE SURJA DE O ESTÉ RELACIONADO CON EL USO O USO INDEBIDO DE, O LA CONFIANZA EN CUALQUIER CERTIFICADO EMITIDO EN VIRTUD DEL ACUERDO O LA CPS QUE: (I) HAYA VENCIDO O SE HAYA REVOCADO; (II) SE HAYA UTILIZADO PARA CUALQUIER FIN DISTINTO AL ESTABLECIDO EN EL ACUERDO; (III) SE HAYA MANIPULADO; (IV) CON RESPECTO AL CUAL EL PAR DE CLAVES SUBYACENTE A DICHO CERTIFICADO O EL ALGORITMO CRIPTOGRÁFICO EMPLEADO PARA GENERAR EL PAR DE CLAVES DE DICHO CERTIFICADO SE HAYA VISTO COMPROMETIDO POR LA ACCIÓN DE CUALQUIER PARTE QUE NO SEA ENTRUST (INCLUIDOS, ENTRE OTROS, EL SUSCRIPTOR O LA PARTE CONFIANTE); O (V) SEA OBJETO DE TERGIVERSACIONES U OTROS ACTOS U OMISIONES ENGAÑOSOS DE CUALQUIER OTRA PARTE, INCLUIDOS LOS SUSCRIPTORES Y LAS PARTES CONFIANTES. SALVO EN LA MEDIDA EN QUE SE ESTIPULE EXPRESAMENTE EN EL ACUERDO, ENTRUST NO SE RESPONSABILIZARÁ EN NINGÚN CASO ANTE EL SUSCRIPTOR, LA PARTE CONFIANTE O CUALQUIER OTRA PARTE POR LOS PERJUICIOS QUE SURJAN DE CUALQUIER RECLAMACIÓN DE QUE EL CONTENIDO DE UN CERTIFICADO (INCLUIDA CUALQUIER MARCA VERIFICADA DE UN VMC) INFRINGE CUALQUIER PATENTE, MARCA COMERCIAL, DERECHO DE AUTOR, SECRETO COMERCIAL U OTRO DERECHO DE PROPIEDAD INTELECTUAL DE CUALQUIER PARTE.**

13. Impago de Tarifas. Si no se recibe el pago en el plazo de los diez (10) días hábiles siguientes a la notificación por escrito de que hay un pago vencido, Entrust podrá, además de los derechos establecidos en las Condiciones Generales, revocar todos los Certificados.

14. Plazo de la Oferta y rescisión.

14.1. Plazo de la Oferta. Los Servicios de Certificados se venden por unidades (por Certificado) o por suscripción. Los Servicios de Firma y las CA Especializadas se venden por suscripción. El Plazo de la Oferta comenzará en la primera de las fechas en que Entrust habilite la Cuenta de Administración para que el Cliente la utilice o en la fecha en que el Cliente reciba uno o varios Certificados. A menos que se especifique lo contrario en el Pedido, el Plazo de la Oferta continuará en vigor (i) en el caso de cada Certificado adquirido por unidades, durante 365 días si el Certificado permanece sin emitir o durante el periodo de validez del Certificado si este se emite; o (ii) en el caso de los Servicios Alojados adquiridos por suscripción, durante el periodo indicado en el Pedido. Con respecto a los Servicios de Sellado de Tiempo disponibles en relación con los Servicios de Certificados, el Plazo de Oferta será el mismo que el Plazo de Oferta para los Servicios de Certificados relacionados. En cualquier caso, el Plazo de la Oferta puede finalizar antes, tras la rescisión del Acuerdo de conformidad con sus condiciones.

14.2. Rescisión. Además de los derechos de rescisión contemplados en las Condiciones Generales, el Acuerdo de los Servicios Alojados se rescindirá anticipadamente si el Cliente o sus Usuarios no cumplen con cualquiera de los términos o condiciones materiales de este Anexo de ECSS, la CPS o la TPS o bien tras la revocación por parte de Entrust de todos los Certificados emitidos en virtud del presente documento si dicha revocación tiene lugar antes del final del Plazo de la Oferta. Entrust también puede rescindir el Acuerdo a su entera discreción avisando al Cliente con el fin de cumplir con cualquier licencia de terceros u otra obligación contractual o legal (incluido cualquier Estándar del Sector) a la que Entrust esté sujeto.

14.3. Efectos de la rescisión o el vencimiento. Tras el vencimiento del Plazo de la Oferta (a menos que lo suceda inmediatamente un Plazo de Oferta de renovación) o la rescisión del Acuerdo de un Servicio Alojado: (i) el Cliente deberá cesar al instante todo tipo de uso del Servicio Alojado; y (ii) Entrust podrá revocar todos los Certificados emitidos en virtud del Acuerdo y dar de baja cualquier CA Especializada.

15. Suspensión. En caso de que Entrust sospeche que el Cliente y/o los Usuarios han incumplido el Acuerdo o la CPS, Entrust podrá suspender el acceso y uso de los Servicios Alojados por parte del Cliente y/o dichos Usuarios sin previo aviso, además del resto de los recursos que Entrust pueda tener de conformidad con el Acuerdo. Nada en el Acuerdo requiere que Entrust emprenda ninguna acción contra cualquier Cliente, Usuario u otro tercero por infringir el Acuerdo, pero Entrust es libre de tomar cualquier medida a su entera discreción.

16. Uso del sello de sitio protegido de Entrust. Con sujeción a los términos y condiciones del Acuerdo, el Cliente puede utilizar los Servicios de Certificados con el sello de sitio protegido de Entrust siempre y cuando (i) Entrust proporcione al Cliente el sello de sitio protegido de Entrust junto con los Servicios de Certificados y (ii) **AL HACER CLIC EN EL ICONO "ACCEPT" (ACEPTAR) QUE APARECE A CONTINUACIÓN Y AL UTILIZAR EL SELLO DE SITIO PROTEGIDO DE ENTRUST, EL CLIENTE ACEPTE QUEDAR OBLIGADO A CUMPLIR LOS TÉRMINOS Y CONDICIONES DEL ACUERDO DE LICENCIA DEL SELLO DE SITIO PROTEGIDO DE ENTRUST ESTABLECIDO EN** http://www.entrust.net/cps**.**

17. Software de Código Abierto y Productos de terceros.

17.1. Código Abierto. Las versiones de determinados programas de software de código abierto de terceros (incluidas las bibliotecas y los archivos redistribuibles) pueden integrarse, ofrecerse o descargarse automáticamente como parte de cualquier Oferta (en adelante, el "Software Auxiliar"). Si se incluye o proporciona un acuerdo de licencia independiente perteneciente al Software Auxiliar con las Ofertas, el Software Auxiliar estará sujeto al acuerdo de licencia independiente aplicable al Software Auxiliar. Si lo solicita, Entrust facilitará al Cliente una lista completa del Software Auxiliar y las licencias correspondientes, y dicha lista se considerará Información Confidencial de Entrust.

17.2. Productos y servicios de Proveedores Externos. Entrust puede revender, distribuir, proporcionar u ofrecer de otro modo algunos componentes de hardware, software y servicios de terceros (en adelante, los "**Productos del Proveedor Externo**"). Salvo que se indique expresamente en este Anexo de ECSS, Entrust no tiene ninguna obligación y excluye toda responsabilidad con respecto a los Productos del Proveedor Externo, cuyo uso solo estará sujeto a los términos, condiciones y documentos normativos del

Proveedor Externo (en adelante, las "**Condiciones del Proveedor**") acompañando, incorporados o proporcionados de otro modo con los Productos del Proveedor Externo o puestos a disposición por el proveedor externo. En particular:

17.2.1. Si el Cliente adquiere cualquier producto de Sixscape (por ejemplo, SixMail, SixEscrow) a través de Entrust o en relación con los Servicios de Certificados, el uso de los productos de Sixscape estará sujeto a las Condiciones del Proveedor Sixscape incluidas o proporcionadas con los productos y disponibles en www.sixscape.com/product-and-warranty/. Entrust proporcionará asistencia en relación con los productos de Sixscape de conformidad con el anexo de asistencia disponible en https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf.

17.2.2. Si el Cliente utiliza cualquier producto de WebID, que ofrece verificación cara a cara, el uso de los productos de WebID estará sujeto a las Condiciones del Proveedor WebID que deben aceptarse antes de acceder a dichos Productos del Proveedor. El Cliente reconoce y acepta que podrá enviar Información de Verificación, incluidos datos personales, a WebID a través de la Cuenta de Administración y que WebID proporcionará un paquete de registro de datos a Entrust para informar de los resultados de la verificación. En aras de una mayor claridad, todo el tratamiento de la Información de Verificación y los datos personales por parte de Entrust se realizará de conformidad con el Acuerdo, y el tratamiento por parte de WebID se efectuará de acuerdo con las Condiciones del Proveedor WebID.

17.2.3. Entrust puede ofrecer, con determinados Certificados, servicios opcionales de análisis diario de malware alojados por un Proveedor en nombre de Entrust, como se describe con más detalle en la Documentación (en adelante, los "Servicios de Análisis de Malware"). Dichos Servicios de Análisis de Malware están sujetos a que el Cliente proporcione la información necesaria al Proveedor para la prestación de tales servicios y acepte las Condiciones del Proveedor para recibir los resultados. Entrust se reserva el derecho a modificar las características y la funcionalidad de los Servicios de Análisis de Malware o a interrumpir dichos servicios durante el Plazo de la Oferta y no garantiza que tales servicios detecten o sean capaces de detectar malware, amenazas de seguridad o vulnerabilidades.

17.3. Ausencia de uso independiente. Cualquier Producto de Proveedores Externos o Software Auxiliar incluido o integrado en la Oferta solo puede utilizarse con la Oferta aplicable, a menos que se permita lo contrario en el acuerdo aplicable que acompañe a dicho Producto de Proveedores Externos o Software Auxiliar.

18. **Terceros beneficiarios**. Se notifica al Cliente que hay terceros beneficiarios del Acuerdo. Se acuerda expresamente que los Beneficiarios del Certificado serán terceros beneficiarios en virtud del Acuerdo de Servicios de Certificados. Además, con respecto a las disposiciones del Acuerdo que se relacionan con (i) el uso de ciertos componentes de una Oferta en los que dichos terceros tienen un interés, (ii) productos y servicios proporcionados por terceros subcontratistas, proveedores y licenciantes de Entrust , o (iii) Productos de Proveedores Externos proporcionados por proveedores externos; dichas disposiciones se hacen expresamente para el beneficio de dichos terceros beneficiarios y son exigibles por dichos terceros beneficiarios además de ser exigibles por Entrust.

19. **Publicidad.** Durante el plazo y los treinta (30) días posteriores, el Cliente concede a Entrust el derecho, gratuitamente, de utilizar el nombre y/o el logotipo del Cliente, en todo el mundo, para identificar al Cliente como tal en el sitio web de Entrust u otros materiales de marketing o publicidad.

Anexo A

Con autorización para solicitar un Certificado de Suscriptor:	
Con autorización para aprobar la solicitud de un Certificado de Suscriptor y autorizar a otros a solicitar Certificados de Suscriptor:	
Con autorización para aceptar el acuerdo de suscriptor en nombre del Suscriptor:	

Anexo B

Manifestaciones, garantías y obligaciones de los Suscriptores y Sujetos

Parte 1: Suscriptores

Como condición para emitir cualquier Certificado a o para un Suscriptor, cada Suscriptor hace, en su propio nombre y, si corresponde, en nombre de su superior o Agente en virtud de una relación de subcontratista o servicio de alojamiento, los siguientes compromisos, manifestaciones, afirmaciones y garantías en beneficio de los Beneficiarios del Certificado, Entrust y cualesquiera de las Filiales de Entrust que emitirán Certificados a o para el Suscriptor:

Para todos los Certificados.

1. Si el Suscriptor solicita la emisión de un Certificado a o para otra Persona, esta ha autorizado al Suscriptor para que actúe en su nombre, incluida la solicitud de Certificados en nombre de dicha Persona, y para que haga los compromisos, manifestaciones, afirmaciones y garantías recogidos en el presente anexo en nombre de dicha Persona, así como en el propio nombre del Suscriptor.
2. Toda la información proporcionada y todas las manifestaciones realizadas, en todo momento, por parte del Suscriptor en relación con cualesquiera Servicios de Certificados, incluso en la solicitud de Certificados y en lo que respecta a la emisión de Certificados, son y serán íntegras, correctas y exactas (y dicha información y manifestaciones se actualizarán de manera oportuna cada cierto tiempo según sea necesario para mantener dicha integridad, corrección y exactitud), y no infringen, se apropian indebidamente, diluyen, compiten injustamente o vulneran de otro modo la propiedad intelectual u otros derechos de cualquier persona, entidad u organización en cualquier jurisdicción. A efectos aclaratorios, al enviar cualquier solicitud de un Certificado utilizando información preseleccionada, se considera que el Suscriptor está volviendo a hacer los compromisos, manifestaciones, afirmaciones y garantías establecidos en este Anexo B. Asimismo, Entrust no tendrá la obligación de emitir ningún Certificado que contenga información preseleccionada si posteriormente se descubre que dicha información ha cambiado o es de algún modo inexacta, incorrecta o errónea.
3. La clave privada correspondiente a la clave pública enviada a Entrust con la solicitud de Certificado se creó mediante sólidas técnicas criptográficas y se han tomado todas las medidas razonables para, en todo momento, garantizar el control (y, en el caso de los Certificados de OV Code Signing y EV Code Signing, el control exclusivo), mantener la confidencialidad y prohibir el uso no autorizado de la clave privada (y cualquier acceso asociado o dato o dispositivo de activación, por ejemplo, contraseña o token), así como protegerla adecuadamente, incluido, en el caso de los Certificados de OV Code Signing y EV Code Signing, de acuerdo con las disposiciones del apartado “Data Security and Private Key Protection” (Seguridad de los datos y protección de las claves privadas) de los BR de Code Signing.
4. Cualquier dispositivo que almacene claves privadas se operará y mantendrá de forma segura.
5. No se instalará ni utilizará ningún Certificado hasta que el Suscriptor (o, en el caso de los Certificados de Code Signing, el Agente del Suscriptor) haya revisado y verificado que el contenido del Certificado es exacto y correcto.
6. En el caso de todos los Certificados SSL, Certificados SSL de EV y Certificados de Private SSL de Entrust, el Certificado se instalará únicamente en los servidores a los que se pueda acceder en el nombre de dominio (subjectAltName(s)) que figure en el Certificado.
7. Los Certificados y la clave privada correspondiente a la clave pública que se incluye en dichos Certificados solo se utilizarán de acuerdo con todas las leyes aplicables y exclusivamente de conformidad con el Acuerdo, y solo se emplearán en nombre de la organización que aparezca como Sujeto en dichos Certificados.
8. El contenido de los Certificados no se modificará indebidamente.
9. El Suscriptor notificará a Entrust, dejará de utilizar el Certificado y la clave privada correspondiente a la clave pública del Certificado, y solicitará la revocación del Certificado:
    9.1. inmediatamente si cualquier información incluida en el Certificado o la solicitud de un Certificado cambia, si es o se vuelve incorrecta o inexacta, o si cualquier cambio en las circunstancias pudiera hacer que la información del Certificado fuera errónea.
    9.2. inmediatamente si hay algún conocimiento o sospecha de pérdida, robo, uso indebido o puesta en riesgo de la clave privada (o los datos de activación de la clave) correspondiente a la clave pública del Certificado, incluso si el valor de la clave privada se ha revelado a una persona no autorizada o esta ha tenido acceso a él (en adelante, la “**Puesta en Riesgo de la Clave**”), o si se ha perdido el control de la clave privada por otros motivos.

9.3. en el caso de un Certificado de OV Code Signing o EV Code Signing inmediatamente si hay pruebas de que el Certificado se ha utilizado para firmar Código Sospechoso.

10. El Suscriptor dejará de utilizar de inmediato el Certificado y la clave privada correspondiente a la clave pública de dicho Certificado tras su vencimiento o revocación.
11. El Suscriptor responderá al instante a las instrucciones de Entrust con respecto a cualquier Puesta en Riesgo de la Clave o uso indebido o sospecha de uso indebido de un Certificado.
12. El Suscriptor reconoce y acepta que Entrust tiene derecho a revocar un Certificado inmediatamente si:
    12.1. El Cliente incumple el presente Acuerdo.
    12.2. Entrust descubre que se ha producido una Puesta en Riesgo de la Clave privada del Certificado.
    12.3. Se requiere la revocación en virtud de la CPS o los Estándares del Sector.
    12.4. Entrust descubre que el Certificado se ha puesto en riesgo o se está utilizando para Código Sospechoso o que la clave privada correspondiente a la clave pública del Certificado se ha usado para firmar digitalmente Código Sospechoso.
13. Si el Sujeto designado en el o los Certificados es una entidad independiente del Suscriptor, el Sujeto ha autorizado la inclusión de su información en el Certificado.
14. El Suscriptor es propietario del nombre de dominio o la dirección de correo electrónico que figuran en el Certificado, además de controlarlo o tener el derecho exclusivo de utilizarlo.
15. El Suscriptor reconoce y acepta que Entrust tiene derecho a modificar el Acuerdo cuando sea necesario para cumplir con cualquier cambio en los Estándares del Sector.
16. El Suscriptor discernirá con buen juicio si es apropiado, dado el nivel de seguridad y confianza ofrecido por el Certificado, utilizar el Certificado en cualquier circunstancia dada.

Certificados de Code Signing.

17. Asimismo, en el caso de los Certificados de OV Code Signing y EV Code Signing:
    17.1. El Suscriptor hará todos los esfuerzos comercialmente razonables para aplicar las prácticas de Code Signing establecidas en el documento de mejores prácticas de Code Signing (disponible en https://www.entrust.com/-/media/documentation/whitepapers/code-signing-best-practices-v2.pdf) o poniéndose en contacto con Entrust (en adelante, las "**Mejores Prácticas de Code Signing**").
    17.2. El Suscriptor generará y utilizará de forma segura cualquier dispositivo que almacene claves privadas, como se describe en las Mejores Prácticas de Code Signing, y usará contraseñas que se generen aleatoriamente con al menos 16 caracteres que incluyan letras mayúsculas, minúsculas, números y símbolos para transportar las claves privadas.
    17.3. El Suscriptor no solicitará ningún Certificado de Code Signing o de EV Code Signing que contenga una clave pública que se utilice o se utilizará con cualquier otro tipo de Certificado.
    17.4. El Certificado y la clave privada correspondiente a la clave pública de dicho Certificado solo se emplearán para fines legales y autorizados, y no se usarán para firmar digitalmente Código Sospechoso.
    17.5. Se proporcionarán una red adecuada y otros controles de seguridad para ofrecer protección frente al uso indebido de la clave privada correspondiente a la clave pública del Certificado.
    17.6. El Suscriptor reconoce y acepta que Entrust tiene autorización para compartir información sobre el Suscriptor, la aplicación firmada, el Certificado y las circunstancias circundantes con otras autoridades de certificación o grupos del sector, incluido el CA/Browser Forum, si:
        17.6.1. el Certificado o el Suscriptor se ha identificado como fuente de Código Sospechoso,
        17.6.2. no se puede verificar la autoridad para solicitar el Certificado, o
        17.6.3. el Certificado se revoca por motivos distintos a los de la solicitud del Suscriptor (por ejemplo, como resultado de la puesta en riesgo de la clave privada, la detección de malware, etc.).
    17.7. El Suscriptor reconoce que los ASV pueden determinar de forma independiente que un Certificado es malintencionado o se ha visto comprometido y que los ASV y sus productos pueden modificar las experiencias de los clientes o restringir un Certificado de OV Code Signing o EV Code Signing sin previo aviso al Cliente o Entrust y sin importar el estado de revocación del Certificado de Code Signing.

Certificados Cualificados.

18. Además, en el caso de los Certificados eIDAS QWAC, PSD2 QWAC, eIDAS QSealC, PSD2 QSealC y eIDAS QSigC:
    18.1. El Suscriptor cumplirá todos los requisitos de la CPS para utilizar un tipo específico de dispositivo criptográfico (incluyendo un dispositivo criptográfico seguro o un dispositivo de creación de firma/sello cualificado, QSCD) y, si es necesario:

18.1.1. la o las claves privadas del Sujeto solo se utilizarán para funciones criptográficas dentro del dispositivo criptográfico especificado.
18.1.2. si las claves del Sujeto se generan bajo el control del Suscriptor o del Sujeto, las claves del Sujeto se generarán dentro del dispositivo criptográfico especificado.
18.2. El Suscriptor da su consentimiento para que Entrust mantenga un seguimiento de la información utilizada en el registro, el suministro del dispositivo del Sujeto, ya sea al Suscriptor o al Sujeto cuando sean distintos, y cualquier revocación posterior, la identidad y cualquier atributo específico incluido en el Certificado, y transmita esta información a terceros en las mismas condiciones que exigen los Estándares del Sector en caso de que Entrust dé por terminados sus servicios.
18.3. El Suscriptor exige la publicación del Certificado en la forma y condiciones establecidas en la CPS y obtendrá, en su caso, la autorización del Sujeto para dicha publicación.
18.4. La clave privada y la correspondiente clave pública asociadas al Certificado solo se utilizarán de acuerdo con las limitaciones notificadas al Suscriptor, incluso en la CPS.
18.5. Si el Suscriptor o el Sujeto genera las claves del Sujeto:
18.5.1. las claves del Sujeto se generarán mediante un algoritmo según lo especificado en los Estándares del Sector para los usos de la clave certificada tal y como se identifica en la CPS.
18.5.2. la longitud y el algoritmo de la clave serán los especificados en los Estándares del Sector para los usos de la clave certificada tal y como se identifica en la CPS durante el periodo de validez del Certificado.
18.5.3. la clave privada del Sujeto se mantendrá bajo control del Sujeto, y si el Sujeto es un individuo, bajo el control exclusivo del Sujeto.
18.6. La clave privada del Sujeto se utilizará bajo el control del Sujeto, y si el Sujeto es un individuo, bajo el control exclusivo del Sujeto.
18.7. Al ser informado de que el Certificado del Sujeto se ha revocado o de que la Issuing CA se ha visto comprometida, el Suscriptor se asegurará de que el Sujeto deje de utilizar la clave privada correspondiente a la clave pública del Certificado.
18.8. Con respecto a eIDAS QSigC, los pares de clave solo se utilizarán para firmas electrónicas.
18.9. Con respecto a eIDAS QSealC y PSD2 QSealC, los pares de clave solo se utilizarán para sellos electrónicos.

Certificados de Verified Mark.

19. Además, en el caso de los VMC:
19.1. El Suscriptor solicitará y utilizará los VMC de acuerdo con los Requisitos de VMC y estará sujeto a ellas.
19.2. Las marcas comerciales enviadas en una solicitud de VMC representan marcas comerciales registradas que son propiedad del Suscriptor o para las que ha obtenido la licencia adecuada para poder otorgar la licencia limitada en los términos de uso adjuntos a los Requisitos de VMC. Asimismo, revocará inmediatamente el VMC si ya no posee o tiene una licencia adecuada para las marcas comerciales aplicables.

Parte 2: Sujetos individuales, cuando son diferentes del Suscriptor

Si el Sujeto y el Suscriptor son entidades independientes y el Sujeto es una Persona (es decir, no un dispositivo), como condición para emitirle cualquier Certificado eIDAS QWAC, PSD2 QWAC, eIDAS QSealC, PSD2 QSealC y eIDAS QSigC, el Sujeto debe aceptar las siguientes obligaciones:

1. El Sujeto cumplirá todos los requisitos de la CPS para utilizar un tipo específico de dispositivo criptográfico (incluyendo un dispositivo criptográfico seguro o QSCD) y, si así se precisa, la o las claves privadas del Sujeto solo se usarán para funciones criptográficas con el dispositivo criptográfico especificado.
2. El Sujeto da su consentimiento para que Entrust mantenga un seguimiento de la información utilizada en el registro, el suministro del dispositivo del Sujeto, ya sea al Suscriptor o al Sujeto cuando sean distintos, y cualquier revocación posterior, la identidad y cualquier atributo específico incluido en el Certificado, y transmita esta información a terceros en las mismas condiciones que exige la norma ETSI EN 319 411-1 en caso de que Entrust dé por terminados sus servicios.
3. La clave privada y la correspondiente clave pública asociadas al Certificado solo se utilizarán de acuerdo con las limitaciones notificadas al Sujeto, incluso en la CPS.
4. El Sujeto prohibirá el uso no autorizado de su clave privada.

5. Si el Sujeto genera sus claves, la clave privada del Sujeto se mantendrá el control del Sujeto, y si el Sujeto es un individuo, bajo el control exclusivo del Sujeto.
6. La clave privada del Sujeto se utilizará bajo el control del Sujeto, y si el Sujeto es un individuo, bajo el control exclusivo del Sujeto.
7. El Sujeto notificará a Entrust de inmediato:
   7.1. si cualquier información incluida en el Certificado cambia, si es o se vuelve incorrecta o inexacta, o si cualquier cambio en las circunstancias pudiera hacer que la información del Certificado fuera errónea.
   7.2. y dejará de utilizar de forma inmediata y permanente la clave correspondiente si hay algún conocimiento o sospecha de pérdida, robo, uso indebido o puesta en riesgo de la clave privada (o los datos de activación de la clave) correspondiente a la clave pública del Certificado, incluso si el valor de la clave privada se ha revelado a una persona no autorizada o esta ha tenido acceso a él, o si se ha perdido el control de la clave privada por otros motivos.
8. Al ser informado de que el Certificado del Sujeto se ha revocado o de que la Issuing CA se ha visto comprometida, el Sujeto dejará de utilizar la clave privada.