**REGLAMENTO TÉCNICO SALVADOREÑO** **RTS 35.01.01:20**

# TECNOLOGÍA DE LA INFORMACIÓN. FIRMA ELECTRÓNICA. REQUISITOS TÉCNICOS PARA ACREDITACIÓN DE PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA.

Correspondencia: Este Reglamento Técnico Salvadoreño no tiene correspondencia con normativa internacional.

ICS 35.020 RTS 35.01.01:20

Editada por el Organismo Salvadoreño de Reglamentación Técnica, ubicado en Boulevard San Bartolo y Calle Lempa, costado Norte del INSAFORP, Edificio CNC, Ilopango, San Salvador, El Salvador. Teléfono (503) 2590-5335 y (503) 2590-5338. Sitio web: www.osartec.gob.sv

# INFORME

Los Comités Nacionales de Reglamentación Técnica conformados en el Organismo Salvadoreño de Reglamentación Técnica, son las instancias encargadas de la elaboración de Reglamentos Técnicos Salvadoreños. Están integrados por representantes de la Empresa Privada, Gobierno, Defensoría del Consumidor y sector Académico Universitario.

Con el fin de garantizar un proceso consultivo con los diferentes sectores, este proyecto de Reglamento Técnico Salvadoreño fue sometido a consulta nacional a través de los medios electrónicos y digitales disponibles durante el período de emergencia ocasionada por la pandemia del COVID-19.

El estudio elaborado fue aprobado como RTS 35.01.01:20 TECNOLOGÍA DE LA INFORMACIÓN. FIRMA ELECTRÓNICA. REQUISITOS TÉCNICOS PARA ACREDITACIÓN DE PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA, por el Comité Nacional de Reglamentación Técnica. La oficialización del Reglamento conlleva el Acuerdo Ejecutivo del Ministerio correspondiente de su vigilancia y aplicación.

Este Reglamento Técnico Salvadoreño está sujeto a permanente revisión con el objeto de que responda en todo momento a las necesidades y exigencias de la técnica moderna.

**CONTENIDO** **PÁG.**

## 1. OBJETO

Establecer los requisitos técnicos para la prestación de servicios de emisión de certificados electrónicos que deberán cumplir los prestadores de servicios de certificación en virtud de la Ley de Firma Electrónica.

## 2. ÁMBITO DE APLICACIÓN

Aplica a toda persona jurídica registrada en el territorio nacional, público o privado, nacional o extranjera, que solicite acreditarse como Proveedor de Servicio de Certificación Electrónica.

## 3. DEFINICIONES

Para los efectos de este Reglamento Técnico Salvadoreño serán aplicables las siguientes definiciones:

**3.1. Acreditación:** autorización que otorga la autoridad competente establecida en la Ley de Firma Electrónica, a los proveedores de servicios de certificación, para operar y proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en la referida Ley, su Reglamento y demás normativa relacionada.

**3.2. Certificado Electrónico:** documento proporcionado por un proveedor de servicios de certificación que otorga certeza a la firma electrónica certificada, garantizando la asociación de la persona con dicha firma.

**3.3. Proveedor de Servicios de Certificación:** persona jurídica autorizada por la autoridad competente, dedicada a emitir certificados electrónicos y demás actividades previstas en la Ley de Firma Electrónica.

## 4. ABREVIATURAS

- **ETSI:** European Telecommunications Standards Institute, por sus siglas en inglés (Instituto Europeo de Normas de Telecomunicaciones).
- **IT:** Information Technology, por sus siglas en inglés (Tecnología de la Información)
- **MINEC:** Ministerio de Economía
- **RTS:** Reglamento Técnico Salvadoreño

## 5. ESPECIFICACIONES TÉCNICAS

### 5.1. Requisitos tecnológicos de calidad y seguridad

Para la prestación de servicios de certificación electrónica se debe cumplir lo establecido en la Tabla 1:

**Tabla. 1: Requisitos tecnológicos de calidad y seguridad**

| No | Parámetro a cumplir | Requerimiento de cumplimiento |
|---|---|---|
| 1 | Requisitos generales y de seguridad para la emisión de certificados electrónicos para proveedores de servicios de certificación | ETSI EN 319 411-1 V1.2.2 (2018-04). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. |

| No | Parámetro a cumplir | Requerimiento de cumplimiento |
|---|---|---|
| | | *(Firmas Electrónicas e Infraestructuras (ESI); Política y requisitos de seguridad para Proveedores de Servicios de Confianza que emiten certificados; Parte 1: Requisitos Generales).* |
| 2 | Perfiles de Certificados Electrónicos, especificando estructuras de datos comunes para su uso utilización en el contexto internacional. | ETSI EN 319 412-1 V1.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. *(Firmas Electrónicas e Infraestructuras (ESI); Perfiles de certificados; Parte 1: Descripción General y estructuras de datos comunes).* |
| 3 | Requisitos de contenido para la emisión de certificados electrónicos expedidos a personas naturales. | ETSI EN 319 412-2 V2.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons. *(Firmas Electrónicas e Infraestructuras (ESI); Perfiles de certificados; Parte 2: Perfil de certificado de certificados emitidos a personas naturales.)* |
| 4 | Requisitos de contenido para la emisión de certificados electrónicos expedidos a personas jurídicas. | ETSI EN 319 412-3 V1.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons. *(Firmas Electrónicas e Infraestructuras (ESI); Perfiles de certificados; Parte 3: Perfil de certificado para certificados emitidos a personas jurídicas.)* |
| 5 | Campos QCStatement para los Certificados Electrónicos, siguiendo los lineamientos de las normas europeas para identificar que se trata de certificados calificados. | ETSI EN 319 412-5 V2.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements. *(Firmas Electrónicas e Infraestructuras (ESI); Perfiles de certificados; Parte 5: QCStatements.)* |
| 6 | Perfil para el protocolo de sellado de tiempo y los requisitos del token de sellado de tiempo. | ETSI EN 319 422 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles. *(Firmas Electrónicas e Infraestructuras (ESI); Protocolo de sellado de tiempo y perfiles de token de sellos de tiempo.)* |
| 7 | Requisitos de seguridad que se deben establecer en el sistema de gestión de la seguridad de la información destinado a los sistemas de conservación de firmas y/o datos. | ETSI TS 101 533-1 V1.3.1 (2012-04). Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management. *(Firmas Electrónicas e Infraestructuras (ESI); Sistemas de Seguridad para Preservación de Datos; Parte 1: Requisitos para la Implementación y Administración.)* |

Fuente: Basada en European Telecommunications Standards Institute (ETSI), por sus siglas en inglés (Instituto Europeo de Normas de Telecomunicaciones).

### 5.2. Requisitos de política y seguridad

Para la prestación de servicios de certificación electrónica se debe cumplir lo establecido en la Tabla 2:

**Tabla. 2: Requisitos de política y seguridad**

| No | Descripción | Estándar |
|---|---|---|
| 1 | Requisitos para Proveedores de Servicios de Certificación en la prestación de cualquier servicio de certificación, las cuales deberán de ser aplicables a todos sus procedimientos, procesos y medidas de seguridad. | ETSI EN 319 401 V2.2.1 (2018-04). Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. *(Firmas Electrónicas e Infraestructuras (ESI); Política General de Requisitos para Proveedores de Servicios de Confianza.)* |
| 2 | Medidas de seguridad que deben seguir los Proveedores de Servicios de Certificación para la emisión, mantenimiento y gestión del ciclo de vida los certificados digitales, en el que se incluyen los requisitos generales exigidos por la Parte 1 (ETSI EN 319 411-1 V1.2.2 (2018-04)). | ETSI EN 319 411-2 V2.2.2 (2018-04). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. *(Firmas Electrónicas e Infraestructuras (ESI); Política y requisitos de seguridad para Proveedores de Servicios de Confianza que emiten certificados; Parte 2: Requisitos para proveedores de servicios de confianza que emitan certificados cualificados de la UE.)* |
| 3 | Medidas de seguridad para la operación y gestión de los Proveedores de Servicios de Certificación que emiten sellos de tiempo. | ETSI EN 319 421 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. *(Firmas Electrónicas e Infraestructuras (ESI); Política y Requisitos de Seguridad para Proveedores de Servicios de confianza que emitan sellos de tiempo.)* |
| 4 | Requisitos a los Proveedores de Servicios de Certificación que firmen y/o almacenen objetos de datos en nombre de sus clientes. | ETSI TS 102 573 V2.1.1 (2012-04). Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects. *(Firmas Electrónicas e Infraestructuras (ESI); Requisitos de política para proveedores de servicios de confianza que firmen y/o almacenen objetos de datos.)* |

Fuente: Basada en European Telecommunications Standards Institute (ETSI), por sus siglas en inglés (Instituto Europeo de Normas de Telecomunicaciones).

### 5.3. Procedimiento de acreditación

**5.3.1.** Las personas jurídicas interesadas deben proveer información, documentación y evidencias que soporten la conformidad de los servicios cuya acreditación solicita, con las previsiones de carácter legal y técnico en el país, que se detalla a continuación:

a) Datos generales de la persona jurídica solicitante, así como de representante legal o apoderado, incluyendo copias certificadas por Notario de los documentos que acrediten la existencia legal de ésta y que comprueben la calidad con que actúa el Representante Legal o apoderado, según el caso; asimismo, deberá acompañarse de copias certificadas por Notario, del documento de identidad y Número de Identificación Tributaria del representante legal o apoderado;
b) Certificaciones obtenidas para el desarrollo de su actividad o servicio y certificaciones de los dispositivos que demuestren conformidad con estándares internacionales reconocidos;
c) Los datos que permitan establecer comunicación con el solicitante, incluidos el nombre de dominio de internet y los datos de atención al público;
d) Indicación del servicio a prestar, acompañada de la descripción de la actividad que desarrollará;
e) Medios de notificación, debiendo señalar una notificación de correo electrónico;
f) Comprobante de pago de las tasas de la acreditación, la cual se divide en: la tasa por inscripción, que es equivalente a cuatro salarios mínimos mensuales del sector comercio y servicio, y la tasa por renovación anual, que corresponderá a dos salarios mínimos mensuales del sector comercio y servicio;
g) Solvencias tributarias, municipales y previsionales. En caso de no poseer las solvencias previsionales, deberá presentar una constancia de no inscripción como empleador;
h) Documentación que permita verificar el compromiso de adquirir los equipos especializados necesarios y los servicios de personal técnico adecuado en el plazo máximo de 90 días hábiles contados a partir de la notificación de la acreditación otorgada;
i) Rendir fianza cuyo monto ascenderá al cinco por ciento del activo de los solicitantes; en caso de renovación de fianza, el monto será del veinte por ciento del valor total de los contratos suscritos con sus usuarios, no obstante, no podrá ser menor de la fianza inicial. En ningún caso, esta podrá ser menor a quinientos salarios mínimos ni mayor a dos mil salarios mínimos, ambos del sector, comercio y servicios. En caso de renovación de fianza, el monto será del veinte por ciento del valor total de los contratos suscritos con sus usuarios, no obstante, no podrá ser menor de la fianza inicial.

   La fianza debe ser expedida por una sociedad domiciliada en El Salvador autorizada por la Superintendencia del Sistema Financiero. Esta fianza será utilizada para indemnizar los daños y perjuicios que se ocasionasen a los usuarios de los servicios de certificación. La fianza será revisada y renovada anualmente antes de su vencimiento, tomando en cuenta los cambios en el nivel de riesgo asumido por el proveedor de servicios de certificación;
j) Documentación que permita verificar que cuenta con capacidad técnica para garantizar la seguridad, la calidad y la fiabilidad de los certificados emitidos, de conformidad a los requerimientos contenidos en las normas técnicas, salvo en el caso del art. 44 inciso segundo de la Ley de Firma Electrónica;
k) Documentación que permita verificar que cuenta con el personal técnico adecuado con conocimiento especializado comprobable en la materia y experiencia en el servicio a prestar, salvo en el caso del art. 44 inciso segundo de la Ley de Firma Electrónica;

l) Documentación que permita verificar que posee la capacidad económica y financiera suficiente para prestar los servicios autorizados como proveedor de servicios de certificación;
m) Documentación que permita verificar que cuenta con un sistema de información de alta disponibilidad actualizado y eficiente, en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como los certificados electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a estos, salvo en el caso del art. 44 inciso segundo de la Ley de Firma Electrónica.

**5.3.2.** El interesado deberá cumplir con los requisitos establecidos en el numeral 5.1 y 5.2 de este Reglamento, lo cual será verificado a través del procedimiento de evaluación de la conformidad detallado en el numeral 6 del presente RTS.

**5.3.3.** El área correspondiente del MINEC dispondrá de una guía o instructivo que detallará el procedimiento para la tramitación, evaluación y aprobación de una solicitud de acreditación o renovación de ésta como Proveedor de Servicios de Certificación Electrónica de acuerdo con la Ley de Firma Electrónica, su Reglamento y demás normativa relacionada.

**5.3.4.** La acreditación que emita el área correspondiente del MINEC deberá ser renovada anualmente, en virtud de lo dispuesto en la Ley de Firma Electrónica. Los Proveedores de Servicios de Certificación Electrónica deberán solicitar la renovación de su acreditación con al menos un mes de anticipación al requerimiento de la renovación anual.

## 6. PROCEDIMIENTO DE EVALUACION DE LA CONFORMIDAD

### 6.1. Evaluación de la conformidad

El área correspondiente del MINEC, o quien esta designe para tal fin, evaluará la conformidad en el cumplimiento de los requisitos y obligaciones de los Proveedores de Servicios de Certificación. Cada requisito será evaluado individualmente, de conformidad a un procedimiento y una escala predefinida que se desarrolla en el correspondiente instructivo.

### 6.2. Cumplimiento de requisitos

El Proveedor de Servicios de Certificación debe demostrar el cumplimiento de los requisitos de acreditación mediante los siguientes medios:
a) Aportando los antecedentes que exige la Ley de Firma Electrónica, su Reglamento y la normativa legalmente aplicable;
b) Presentando la documentación e información solicitada por el área correspondiente del MINEC, o quien esta designe, dentro de los plazos establecidos en el procedimiento de acreditación y evaluación;
c) Permitiendo el libre acceso al área correspondiente del MINEC, o quien ésta designe, para realizar la auditoria;
d) Entregando cualquier información adicional pertinente solicitada por el área correspondiente del MINEC, o quien ésta designe, durante el proceso de acreditación.

### 6.3. Condiciones para su aplicación

**6.3.1.** El área correspondiente del MINEC tiene la decisión final para que el proceso de evaluación que realizará (por ejemplo, una solicitud de acreditación o una ampliación del alcance acreditado, entre otros) pueda ser abordado mediante el uso de técnicas de evaluación presenciales o remotas según corresponda. Dicha decisión será tomada tras considerar las correspondientes indicaciones reflejadas en la guía de evaluación o el análisis de riesgos particular si fuese el caso, el cual en todo caso tendrá en cuenta la naturaleza de las actividades a evaluar y su complejidad. De igual forma, la decisión vendrá condicionada por los medios y herramientas de comunicación suficientes para acometer la evaluación de la conformidad necesaria.

**6.3.2.** Para la ejecución de los correspondientes controles, debe estar disponible el personal técnico, legal, de organización, de calidad o dirección que se requiera dependiendo de la naturaleza de la evaluación. Esto deberá ser acordado antes de la evaluación entre el área correspondiente del MINEC, o quien ésta designe, para realizar la auditoria a fin de llevar a cabo la revisión y el solicitante de la acreditación o Proveedor de Servicios de Certificación en caso de que fuese necesario. Es recomendable que el solicitante tenga acceso a su responsable de IT para solucionar problemas que pudieran surgir.

**6.3.3.** La duración de una evaluación de la conformidad remota puede diferir de la correspondiente *in situ*, dependiendo de qué aspectos se cubran en dicha evaluación. Además, también es probable que la evaluación se fragmente en actividades individuales que se lleven a cabo en el transcurso de un período más largo.

**6.3.4.** El uso de estas técnicas de evaluación lleva aparejadas una serie de incertidumbres, tanto en la calidad de la información que pueda obtenerse en cada caso como a los imponderables que pueden surgir durante su aplicación, por lo que el área correspondiente del MINEC advertirá al inicio del proceso de evaluación que en caso que se pusiese de manifiesto que la información obtenida por el área correspondiente del MINEC, por sí misma o por intermedio de una tercera organización designada para la ejecución de ciertos controles, no fuese concluyente o suficiente para tomar una decisión favorable, se resolverá en sentido negativo.

**6.3.5.** Aún en caso de que el proceso de evaluación de conformidad termine con éxito (con la concesión o mantenimiento de la acreditación), si la naturaleza de actividad solicitada o el resultado de la evaluación así lo aconsejase, la evaluación podría tener que ser complementada con actividades de evaluación extraordinarias (tales como otras evaluaciones, aplicación de ciertos controles o visitas de acompañamiento extraordinarias, auditorías de seguimiento a corto plazo, entre otros).

### 6.4. Técnicas de evaluación

**6.4.1.** Entrevistas. Para confirmar la información previamente evaluada de manera documental y apoyada, si fuera preciso, con la presentación de nuevos documentos/registros que se muestran y evalúan a través de su presentación física, o demostración en pantallas que se identifican y se envían por otros medios idóneos.

**6.4.2.** Utilización de herramientas de videoconferencia. Las cuales permitirán el uso compartido de audio y datos con las personas encargadas de realizar la evaluación de la conformidad, de forma que puedan mantener una conversación mientras ambos ven la pantalla del auditado. En ciertas circunstancias, también es posible que los auditores soliciten que comparta documentación en el propio chat de la auditoría. Grabaciones de esas videoconferencias podrán ser realizadas siempre que se dé un acuerdo entre las partes.

**6.4.3.** Evaluación presencial. A través de ella se confirmará, mediante observación presencial, el cumplimiento de los requisitos, realizando revisiones y aplicación de controles a instalaciones, equipos o documentación relativa a la prestación del servicio de certificación cuya conformidad se estuviese evaluando.

**6.4.4.** Requerimiento de certificaciones. Estas certificaciones deberán ser emitidas por terceras organizaciones mediante las cuales se pueda verificar el cumplimiento de algunos de los requisitos y obligaciones relativas a la seguridad, métodos, organización de la infraestructura o cualquier otro que resultase idóneo. El requerimiento de dichos certificados podrá ser requerido por el área correspondiente del MINEC o quien ésta designe, especialmente cuando existan restricciones geográficas, de movilidad, organizativas, de capacidad técnica o de cualquier otro tipo que impidan la evaluación de tales requisitos a través de personal del área correspondiente del MINEC o quien ésta designe.

**6.4.5.** Observación de actividades técnicas en remoto. La utilización de este método se realizará con restricción, solo en caso de no poder realizar dichas verificaciones a través de cualquier método previsto en este numeral. Las actividades incluyen transmisiones en vivo, grabaciones, revisiones post auditoría y entrevistas técnicas de acuerdo a los métodos descritos a continuación.

a) Para la transmisión en vivo, se debe comprobar que puede transmitir en vivo video y audio bidireccional en la ubicación en la que se realiza la actividad. Esto a menudo requiere el uso de redes móviles o wifi, así que debe comprobar la conectividad en la ubicación;
b) Cuando se haga uso de grabaciones, éstas deberán ser acordadas con el equipo auditor y deben ser realizadas en una sola toma, sin edición posterior y con registro de fecha y hora. El solicitante debe asegurarse de que la grabación es de la claridad adecuada tanto para el video como para el audio. Además, el personal que lleva a cabo la actividad debe narrar lo que está haciendo y por qué.

**6.4.6.** Otras técnicas recomendadas por la autoridad competente.

**6.4.7** Para realizar el procedimiento de evaluación, se deberá utilizar una matriz para la evaluación de conformidad en el cumplimiento de los requisitos y obligaciones de los Proveedores de Servicios de Certificación, la cual servirá de base para obtener los resultados de la evaluación.

### 6.5. Frecuencia de la evaluación

**6.5.1.** La evaluación de la conformidad inicial: se llevará a cabo dentro del proceso de acreditación como Proveedor de Servicios de Certificación conforme a las disposiciones de la Ley de Firma Electrónica y su Reglamento.

**6.5.2.** Primera auditoría de vigilancia: deberá llevarse a cabo dentro de los 12 meses posteriores a la fecha de acreditación, de conformidad con las previsiones legales sobre la materia.

**6.5.3.** Auditorías de vigilancia para la evaluación de conformidad posteriores: en casos de recibir, denuncias, quejas, reclamos o ante la sospecha de incumplimientos establecidos en el procedimiento, el área correspondiente del MINEC podrá realizar auditorías de vigilancia posterior sin que se encuentre programada.

**6.5.4.** Todas las desviaciones en la evaluación de la conformidad de los Proveedores de Servicios de Certificación deben estar justificadas y documentadas.

### 6.6. Resultados de la evaluación

**6.6.1.** El proceso de evaluación de la conformidad del Proveedor de Servicios de Certificación acarreará un resultado de conformidad con lo previsto en la normativa legalmente aplicable.

**6.6.2.** En el caso de que el resultado de la evaluación de conformidad arrojase que el solicitante de la acreditación o el Proveedor de Servicios de Certificación ya acreditado no cumpliese con requisitos formales; o se detectasen no conformidades que por su nivel de gravedad no pongan en riesgo de manera flagrante la provisión del servicio, las mismas serán calificadas como subsanables. Para ello, el evaluado presentará un plan de medidas preventivas que debe ser aprobado por el área correspondiente del MINEC, quien dará el respectivo seguimiento para la verificación del cumplimiento del mismo, posteriormente el área correspondiente del MINEC o quien está designe, deberá dictaminar su conformidad para la prestación de los servicios de certificación cuya acreditación hubiese solicitado o estuviese prestando.

**6.6.3.** De no cumplir con las medidas correctivas descritas en el numeral anterior y de ser identificadas como no subsanables, no se otorgará la conformidad al Solicitante/Proveedor de Servicios de Certificación. En este caso, el solicitante o Proveedor deberá presentar un Plan de Acciones Correctivas detallando todas las actividades para la subsanación que debe ser aprobado por el área correspondiente del MINEC quien dará el respectivo seguimiento para la verificación del cumplimiento del mismo, cuya verificación ocurrirá en cualquier caso previo al otorgamiento de la conformidad.

## 7. DOCUMENTO DE REFERENCIA

**7.1.** ETSI EN 319 401 V2.2.1 (2018-04). Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

**7.2.** ETSI EN 319 411-1 V1.2.2 (2018-04). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates.

**7.3.** ETSI EN 319 411-2 V2.2.2 (2018-04). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates.

**7.4.** ETSI EN 319 412-1 V1.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles.

**7.5.** ETSI EN 319 412-2 V2.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles.

**7.6.** ETSI EN 319 412-3 V1.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles.

**7.7.** ETSI EN 319 412-5 V2.1.1 (2016-02). Electronic Signatures and Infrastructures (ESI); Certificate Profiles.

**7.8.** ETSI EN 319 421 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

**7.9.** ETSI EN 319 422 V1.1.1 (2016-03). Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

**7.10.** ETSI TS 101 533-1 V1.3.1 (2012-04). Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security.

**7.11.** ETSI TS 102 573 V2.1.1 (2012-04). Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects.

**7.12.** FIPS PUB 140-2 (2001): "Requisitos de Seguridad para Módulos Criptográficos".

**7.13.** IETF RFC 3161 (2001): "Internet X.509 Infraestructura de Clave Pública: Protocolo de sellado de tiempo (Time-Stamping Protocol)".

**7.14.** IETF RFC 3647: "Internet X.509 Infraestructura de Clave Pública – Política de Certificación y Marco de Prácticas de Certificación".

**7.15.** IETF RFC 5280: "Internet X.509 Certificado de Infraestructura de Clave Pública y Perfil de Lista de Certificados Revocados (CRL)".

**7.16.** ISO/IEC 15408 (partes 1-3): "Tecnología de la información – Técnicas de seguridad – Criterios de evaluación para seguridad IT".

**7.17.** ISO/IEC 27002 (2013): "Tecnología de la información – Técnicas de seguridad – Código de prácticas para la gestión de seguridad de la información".

**7.18.** ISO/IEC 9594-8/ Recommendation ITU-T X.509: "Tecnología de la Información – Interconexión de Sistemas Abiertos – El Directorio: Marcos de certificados de atributos y clave pública".

**7.19.** Ley de Firma Electrónica, Ministerio de Economía. Decreto Legislativo No 133, Diario Oficial No 196, Tomo No 409 del 26 de octubre de 2015. El Salvador.

**7.20.** Reglamento de la Ley de Firma Electrónica. Ministerio de Economía. Decreto Legislativo No 60, Diario Oficial No 201, Tomo No 413 del 28 de octubre de 2016. El Salvador.

## 8. BIBLIOGRAFÍA

**8.1.** Consejo Nacional de Calidad. Organismo Salvadoreño de Reglamentación Técnica. Guía de Buenas Prácticas de Reglamentación Técnica [en línea], editada en noviembre de 2016, [consulta: 27 de noviembre de 2019]. Disponible en: http://www.osartec.gob.sv/images/jdownloads/Reglamentoss/GBPRT/GBPRT-%20OSARTEC%2001-11-2016_vf.pdf

## 9. VIGILANCIA Y VERIFICACIÓN

**9.1.** La vigilancia y verificación del cumplimiento de este Reglamento Técnico Salvadoreño le corresponde al área correspondiente del Ministerio de Economía de conformidad con la legislación vigente.

**9.2.** El incumplimiento a las disposiciones de este Reglamento Técnico, se sujetará a las sanciones de la legislación vigente.

## 10. VIGENCIA

**10.1.** El presente Reglamento Técnico Salvadoreño entrará en vigencia a partir de la fecha de su publicación en el Diario Oficial.

**10.2.** El Presente Reglamento Técnico Salvadoreño de urgencia tendrá una validez de un año a partir de su entrada en vigencia.

**-FIN DEL REGLAMENTO TÉCNICO SALVADOREÑO-**