

GACETA OFICIAL



DE LA REPÚBLICA DE CUBA

MINISTERIO DE JUSTICIA

EXTRAORDINARIA LA HABANA, JUEVES 1 DE SEPTIEMBRE DE 2016 AÑO CXIV

Sitio Web: <http://www.gacetaoficial.cu/>—Calle Zanja No. 352 esquina a Escobar, Centro Habana

Teléfonos: 7878-3849, 7878-4435 y 7873-7962

Número 24

Página 351

MINISTERIO

GOC-2016-772-EX24

INTERIOR

RESOLUCIÓN No. 2/2016

POR CUANTO: El Decreto-Ley No. 199 “Sobre la Seguridad y Protección de la Información Oficial”, de 25 de noviembre de 1999, establece y regula el Sistema para la Seguridad y Protección de la Información Oficial, y en su Disposición Final Segunda faculta al Ministerio del Interior para dictar cuantas otras disposiciones resulten necesarias para su mejor cumplimiento.

POR CUANTO: La Resolución No. 2, del Ministro del Interior, General de Cuerpo de Ejército Abelardo Colomé Ibarra, que pone en vigor los “Reglamentos para la Criptografía y el Servicio Cifrado en el Territorio Nacional y para el Servicio Central Cifrado en el Exterior”, de fecha 2 de julio de 2002, establece las normas, procedimientos y responsabilidades que deben aplicarse y cumplirse en los órganos, organismos, entidades y sus dependencias o por cualquier otra persona jurídica radicada en el territorio nacional y las personas naturales residentes en el país, para el empleo de la Criptografía y el Servicio Cifrado en el territorio nacional, así como las aplicables al Servicio Central Cifrado en el exterior.

POR CUANTO: La utilización de las técnicas criptográficas basadas en certificados digitales de llave pública, proporcionados por una infraestructura de prestadores de servicios comerciales o no de certificación, facilita brindar seguridad y validez a la información y sistemas de informática y comunicaciones en el marco de la informatización de la sociedad.

POR CUANTO: Es necesario establecer un ordenamiento que garantice la confianza en el empleo y validez de los certificados digitales y técnicas asociadas, mediante la puesta en vigor del Reglamento para el funcionamiento de la infraestructura de llave pública en interés de la protección criptográfica de la información oficial de la República de Cuba.

POR TANTO: En el ejercicio de la atribución que me está conferida en el artículo 33, del Decreto-Ley No. 67 “De Organización de la Administración Central del Estado”, de fecha 19 de abril de 1983,

Resuelvo:

PRIMERO: Establecer la Infraestructura de Llave Pública en interés de la protección criptográfica de la información oficial de la República de Cuba (en lo adelante la Infraestructura).

SEGUNDO: Aprobar el Reglamento sobre el funcionamiento de la Infraestructura de Llave Pública en interés de la protección criptográfica de la Información Oficial en la República de Cuba (en lo adelante el Reglamento), que como Anexo Único se adjunta a la presente Resolución.

TERCERO: Designar al Servicio Central Cifrado del Ministerio del Interior como la Autoridad Raíz de la Infraestructura, con las funciones que se establecen en el precitado Reglamento.

CUARTO: El Reglamento, no establece equivalencia jurídica entre la firma digital de documentos electrónicos realizada con los métodos criptográficos asociados a los certificados digitales de llave pública, y la firma manuscrita tradicional.

QUINTO: Los precios para la comercialización de los certificados digitales de llave pública y los tributos a rendir por los servicios criptográficos de certificación, se ajustan conforme a las disposiciones establecidas por el Ministerio de Finanzas y Precios, y en correspondencia con la legislación tributaria.

SEXTO: Facultar al Jefe de la Dirección de Criptografía del Ministerio del Interior, con la emisión de las instrucciones complementarias que resulten necesarias en virtud del mejor cumplimiento del Reglamento, y para gestionar el proceso de aprobación de la creación de servicios criptográficos que brinda la Infraestructura.

SÉPTIMO: Crear la Comisión Consultiva para la Gobernanza Tecnológica de la Infraestructura de Llave Pública (en lo adelante Comisión Consultiva), con el objetivo de colegiar y compatibilizar las normas técnicas a establecer para la prestación de los servicios criptográficos en la precitada Infraestructura, con las relativas al desarrollo técnico de equipamientos y dispositivos criptográficos nacionales; la gestión y seguridad de la documentación e información electrónica, las telecomunicaciones y el Ciberespacio.

DISPOSICIONES FINALES

PRIMERA: Las actuaciones y acciones no autorizadas por parte de los funcionarios, de los prestadores de servicios criptográficos de certificación y/o de los suscriptores, violatorias del régimen de seguridad, de los roles específicos para la operación de estas entidades y de los métodos que se establecen para el empleo de los certificados digitales son calificadas de hechos que pueden ser sancionables administrativa o penalmente, en virtud de la legislación vigente, de acuerdo con la magnitud, fines y daños ocasionados por la violación.

SEGUNDA: El empleo del certificado digital y de los medios de creación de la firma digital, que se incluyan en el documento oficial de identidad del ciudadano en el país, está sujeto a regulaciones específicas relacionadas con el Sistema de Identidad Nacional.

TERCERA: Los terceros de buena fe, solo pueden depositar su confianza en aquellos usos criptográficos definidos en el presente Reglamento y sus instrucciones complementarias, en la Declaración de Prácticas de Certificación de los prestadores de estos servicios y de los usos que cada certificado digital tiene identificados, y son responsables de la verificación del estado de su vigencia en el proceso de consulta para las transacciones con los suscriptores.

CUARTA: El Ministerio de las Fuerzas Armadas Revolucionarias para su funcionamiento adecua en lo que resulte necesario, la aplicación de las disposiciones establecidas en esta Resolución.

QUINTA: La presente Resolución entra en vigor a los noventa (90) días contados a partir de su publicación en la Gaceta Oficial de la República de Cuba.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio del Interior.

DADO en La Habana, a los 9 días del mes de agosto de 2016.

Viceministro Primero del Interior
Vicealmirante

Julio César Gandarilla Bermejo

ANEXO ÚNICO REGLAMENTO

SOBRE EL FUNCIONAMIENTO DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA EN INTERÉS DE LA PROTECCIÓN CRIPTOGRÁFICA DE LA INFORMACIÓN OFICIAL EN LA REPÚBLICA DE CUBA

CAPÍTULO I GENERALIDADES

ARTÍCULO 1.- El presente Reglamento establece las normas y procedimientos generales para el funcionamiento en el país de la Infraestructura de Llave Pública, los prestadores de servicios criptográficos de certificación que la componen; el empleo de los certificados digitales de llave pública (en lo adelante certificados digitales), los criptomateriales y técnicas criptográficas asociadas a ellos, y se aplica, a la información oficial que se procesa, transmite y almacena en forma de datos informáticos, electrónicos y de mensajes de Infocomunicaciones, salvo en las obligaciones contraídas por el Estado cubano en virtud de convenios o tratados internacionales que requieran un tratamiento particular.

ARTÍCULO 2.- La Dirección de Criptografía del Ministerio del Interior examina y aprueba el empleo del certificado digital en interés de asegurar la protección criptográfica de la confidencialidad de la información oficial clasificada, en los casos en que por cuestiones técnicas y funcionales se requiera.

ARTÍCULO 3.- A los efectos del presente Reglamento, los términos de Órgano, Organismo de la Administración Central del Estado, entidad e información oficial son los definidos en el Decreto-Ley No. 199 “Sobre la Seguridad y Protección de la Información Oficial”, de 25 de noviembre de 1999.

ARTÍCULO 4.- A los efectos de lo dispuesto en el presente Reglamento, se entiende por:

- 1) **Algoritmo criptográfico:** Conjunto ordenado de operaciones matemáticas específicas, que implementadas en software o en medios electrónicos realizan secuencialmente y a partir de una lógica, la transformación de una información en texto legible, en texto cifrado ilegible por personas no autorizadas.
- 2) **Autenticación:** Atributo de seguridad de la información que permite la comprobación de la identidad de un actuante (persona, software o equipo, según corresponda) en una transacción electrónica o telemática que se ejecuta mediante operaciones criptográficas, que pueden ser combinadas con otras medidas de protección técnica.
- 3) **Autoridad de Certificación:** Entidad de confianza probada, responsable de emitir y revocar los certificados digitales utilizados por terceros en funciones criptográficas de protección de la información oficial, como por ejemplo, en la firma digital para autenticar la autoría de documentos electrónicos y software; cifrado, acceso seguro a servidores web, etc.
- 4) **Autoridad Raíz:** Autoridad máxima de confianza probada, situada en la cúspide de la cadena de autoridades, responsable de emitir y revocar certificados digitales utilizados por los prestadores de servicios criptográficos de certificación y suscriptores individuales para su operación en la Infraestructura de Llave Pública.
- 5) **Autoridad de Registro:** Entidad de confianza probada, la cual puede operar de forma autónoma, o formar parte de una autoridad de certificación, y cuyas funciones específicas consisten en registrar las peticiones que hagan las personas naturales y jurídicas para obtener la posesión de un certificado digital. Esta autoridad comprueba la veracidad y corrección de los datos que aportan los solicitantes en las peticiones, y envía las peticiones a una autoridad de certificación para que sean procesadas.
- 6) **Autoridad de Sellado o Estampado de Tiempo:** Prestador de Servicio de Certificación de confianza probada, en línea o fuera de ella, que testifica la existencia de un dato electrónico en una fecha y hora concreta para crear un sello electrónico invariable que entrega al solicitante, el cual se construye mediante la ejecución de operaciones criptográficas de firma digital combinadas con el propio dato a testificar y parámetros de tiempo real astronómico que lo obtiene de una fuente de alta fiabilidad técnica.
- 7) **Autoridad de Validación:** Es el componente dentro de la Infraestructura, que tiene como tarea suministrar información sobre la vigencia de validez de los certificados digitales que, a su vez, hayan sido registrados por una autoridad de registro y emitidos por una autoridad de certificación.
- 8) **Certificado Digital de Llave Pública:** Es un archivo o documento electrónico mediante el cual, una autoridad de certificación (tercero confiable) garantiza la vinculación entre la identidad de un sujeto o entidad (nombre, dirección, número de identidad o pasaporte, y otros elementos de identificación) y una llave criptográfica pública, y es una pieza imprescindible en los protocolos que se usan para autenticar a las partes de una comunicación digital.
- 9) **Certificado Digital de Llave Pública Reconocido:** Es aquel que se expide y firma digitalmente por una autoridad de certificación, aprobada para operar en la Infraestructura, cuyo certificado digital (el de la autoridad) está firmado por la Autoridad Raíz.
- 10) **Certificado Digital Comodín:** Certificado digital que puede ser utilizado con varios subdominios de un dominio (sistema de identificación de dispositivos y/o equipos conectados a una red de infocomunicaciones).
- 11) **Clave personal de acceso (PIN):** Secuencia de caracteres que permite el acceso a la llave privada.
- 12) **Criptomaterial:** Se refiere a la llave o conjunto de llaves de cifrado que se emplea en las operaciones de transformación criptográfica de la información.

- 13) **Declaración de Prácticas de Certificación:** Documento público donde la entidad prestadora de servicios criptográficos de certificación, manifiesta sus políticas y procedimientos particulares para el ejercicio de su autoridad, el uso de los certificados digitales bajo su jurisdicción y trámites asociados, basados en los preceptos generales del presente Reglamento y las referencias internacionales al respecto.
- 14) **Firma digital:** Es un valor numérico que se adhiere a un mensaje o documento y que se obtiene mediante un procedimiento matemático conocido, vinculado a la llave privada del suscriptor iniciador de una comunicación y al texto del mensaje para permitir determinar que este valor se ha obtenido exclusivamente con esa llave privada (secreta) del iniciador, y que el mensaje inicial no ha sido modificado después de efectuada la transformación.
- 15) **GMT:** Tiempo medio de Greenwich (por sus siglas en inglés, *Greenwich Mean Time*) es una norma internacional para ajustar el tiempo en relojes y demás dispositivos de medición de los horarios, tomando como base el horario del meridiano cero, que pasa por esa ciudad cercana a Londres en el Reino Unido.
- 16) **Hash (Resumen):** Se obtiene de la aplicación de una función matemática unidireccional que opera sobre un documento digital, secuencia digital numérica, etc., todos de gran tamaño medido en bits, y brinda como resultado un valor más pequeño y de tamaño fijo, cualquiera sea su entrada, que se utiliza en aplicaciones criptográficas que protegen la integridad de la información.
- 17) **Infraestructura de Llave Pública:** Conjunto de entidades componentes del sistema jerárquico de prestadores de servicios criptográficos de certificación, que funcionan con tecnologías de seguridad, criptografía, políticas, y normas técnico-organizativas aprobadas por el Ministerio del Interior, en aras de brindar la confianza necesaria a sus suscriptores y a terceros de buena fe en el uso de los certificados digitales y criptomateriales asociados para la protección de la información oficial que se tramita por los medios de infocomunicaciones. Una autoridad de certificación de nivel superior garantiza la confiabilidad de una o varias de nivel inferior a ella subordinada.
- 18) **Lista de Revocación de Certificados:** Documento digital público, que expide una autoridad de validación o de certificación, donde figura exclusivamente la relación de los certificados digitales revocados o suspendidos.
- 19) **Llave Pública:** Es uno de dos valores numéricos, obtenidos por métodos matemáticos complejos y criptográficamente seguros, que se le asigna a una persona de manera pública en directorios u otro sitio accesible por terceros, para que los remitentes puedan cifrar mensajes electrónicos a enviar a ella. Se utiliza también en la verificación por los destinatarios de un documento electrónico que tiene una firma digital hecha por la persona que actúa como remitente y es poseedora de la llave pública.
- 20) **Llave Privada:** Es uno de dos valores numéricos, obtenidos por métodos matemáticos complejos y criptográficamente seguros, que se asigna a una persona para su empleo en descifrar datos y la creación de la firma digital de documentos electrónicos. Este valor numérico es secreto y está asociado matemáticamente a la llave pública de la precitada persona.
- 21) **Métodos de defensa criptológica:** Medidas técnicas, organizativas y educativas que se adoptan en locales, equipos de procesamiento criptográfico de la información y sobre los suscriptores que los operan para neutralizar, mitigar o eliminar los posibles ataques de ingeniería social, cibernéticos, informáticos y/o electrónicos, a realizar por intrusos que intentan obtener datos, tecnologías de criptografía y criptomateriales de interés con fines no legítimos.
- 22) **Módulo Criptográfico de Alta Seguridad (MCAS):** Equipo o dispositivo electrónico que se destina en específico para la ejecución de operaciones criptográficas tales como, cifrado de contenidos, generación y almacenamiento de llaves criptográficas, entre otras; el cual dispone con carácter obligatorio de medidas de defensa criptológica. Se conoce internacionalmente como HSM (siglas en inglés de High Security Module).
- 23) **Notación ASN.1:** Notación Sintáctica Abstracta que en la literatura tecnológica se describe por sus siglas en inglés como *Abstract Syntax Notation One*, y es una norma técnica internacional para representar datos que se almacenan con independencia de la computadora en uso y sus formas de representación internas.

- 24) **Política de Certificación:** Conjunto de reglas que especifican las características de emisión, gestión, aplicabilidad y/o uso de los distintos tipos de certificados digitales en una comunidad de suscriptores y usuarios, sistemas o clase particular de aplicaciones que tengan requerimientos de seguridad comunes.
- 25) **Prestador de Servicios Criptográficos de Certificación:** Persona jurídica que presta servicios criptográficos y expide certificados digitales para su utilización en la creación y verificación de la firma digital y el establecimiento de canales de comunicaciones seguros, como por ejemplo las autoridades de certificación, registro, sellado de tiempo, validación, tercero de confianza, custodia de documentos electrónicos, consulta de atributos, entre otros.
- 26) **Protocolo Criptográfico:** Conjunto de reglas que se establecen e implementan en software o en medios electrónicos para ordenar el funcionamiento de las técnicas criptográficas en el intercambio seguro de datos entre entidades a través de canales de comunicaciones, y definen la sintaxis, semántica y sincronización aplicada a estas técnicas.
- 27) **Protocolo OCSP:** Por sus siglas en inglés *Online Certificate Status Protocol*, es una norma técnica internacional para ejecutar con rapidez y en línea con servidores web dedicados a esta función, la verificación automática del estado de revocación de un certificado digital X.509.
- 28) **Protocolo SSL:** Protocolo criptográfico, que se denomina internacionalmente por sus siglas en inglés como Secure Sockets Layer, y significa capa de conexión segura, cuya función es proporcionar autenticación y privacidad a la información entre extremos de una comunicación sobre Internet mediante el empleo de la criptografía basada en certificados digitales, que se utiliza comúnmente para garantizar la seguridad en el acceso a sitios web.
- 29) **Repositorio:** Sistema de información que se emplea para almacenar y recuperar certificados digitales, y otras informaciones relativas a estos.
- 30) **Responsable del certificado digital:** Persona natural, que se identifica en los campos del certificado digital y que el suscriptor determina como el responsable de la custodia y activación del mismo. Esta figura se emplea como regla, en la protección de servidores, canales y servicios seguros de comunicaciones.
- 31) **Suscriptor:** Persona natural o jurídica a cuyo nombre se expide un certificado digital por la autoridad de certificación correspondiente y por tanto, actúa como titular del mismo, conoce y acepta los derechos y deberes para su empleo, que se establece en el presente Reglamento y en la Declaración de Prácticas de Certificación de la autoridad emisora de dicho certificado digital.
- 32) **X.509:** Estándar universal de la Unión Internacional de Telecomunicaciones (UIT) que establece el formato general para la confección y estructura de los certificados digitales.

ARTÍCULO 5.- Los jefes de órganos, organismos de la Administración Central del Estado y entidades proponen la creación o cierre de autoridades y/o prestadores de servicios criptográficos de certificación de su ámbito de competencia a la Dirección de Criptografía, quien se encarga, en un plazo no superior a los cuarenta y cinco (45) días, de realizar el proceso de comprobación y presentar, de corresponder, la solicitud a la aprobación del Ministro del Interior, así como de notificar al solicitante los resultados.

ARTÍCULO 6.- Los prestadores de servicios criptográficos de certificación y los órganos, organismos de la Administración Central del Estado o entidades que disfrutan del servicio, garantizan el aseguramiento financiero y material de los recursos técnicos, humanos y logísticos, tanto para el ejercicio de las funciones de los prestadores de servicios criptográficos de certificación como de los suscriptores, incluidos los medios portadores de la llave privada y los mecanismos para la creación y verificación de la firma digital, así como para las demás acciones de protección de la información con el uso de certificados digitales que establece el presente Reglamento.

ARTÍCULO 7.- A los efectos de los servicios en línea, se presume que un prestador de servicios criptográficos de certificación radica en Cuba, cuando dicho prestador se encuentre registrado en los controles de los organismos de la Administración Central del Estado o entidades reguladoras de las actividades socio-económicas cubanas que tenga relación y disponga de licencia para el uso de las telecomunicaciones del país para tales fines.

ARTÍCULO 8.- Los certificados digitales que emiten las autoridades de certificación de la Infraestructura para la firma digital de documentos electrónicos tienen valor, tanto para las transacciones nacionales como internacionales.

ARTÍCULO 9.- Todas las entidades prestadoras de servicios criptográficos de certificación aprobadas por el Ministerio del Interior, disponen de medios técnicos seguros para el sellado de tiempo de los trámites a realizar con los certificados digitales.

CAPÍTULO II
DEL CERTIFICADO DIGITAL DE LLAVE PÚBLICA
SECCIÓN PRIMERA

Generalidades

ARTÍCULO 10.- Se establece el estándar X.509 como el formato oficial de los certificados digitales a emplear en los servicios de protección criptográfica de la información oficial en el país.

ARTÍCULO 11.- Los certificados digitales se clasifican en las siguientes categorías:

- a) Categoría 1: Certificados Digitales de Llave Pública de carácter personal para firma digital de mensajería y ficheros electrónicos (CD-Pfirma).
- b) Categoría 2: Certificados Digitales de Llave Pública de carácter técnico para la protección de canales y servicios de comunicaciones (CD-SSL).

ARTÍCULO 12.- Los certificados digitales X.509 contienen obligatoriamente los siguientes campos:

- a) Relacionados con el Sujeto: Los datos que identifican al sujeto titular del certificado digital, siendo estos: el nombre y los apellidos, su número de identidad permanente o de pasaporte; o identificación de equipo según corresponda, el Órgano, Organismo de la Administración Central del Estado o entidad a la que pertenezca y el país de procedencia.
- b) Relacionados con los Datos del Certificado: Versión del certificado digital y su identificador o número de serie, el cual es único; la denominación de la autoridad de certificación que lo emite y firma, así como el tiempo de validez del certificado digital, donde se especifica el plazo de inicio y fin de su vida útil, en fecha y hora exacta nacional y del GMT.
- c) Relacionados con las Llaves Criptográficas: Se fijan los usos permitidos para las llaves criptográficas adquiridas para los servicios de protección de la información oficial, así como se publica la llave pública del suscriptor en notación ASN.1 y el algoritmo criptográfico a emplear con dicha llave.
- d) Relacionados con la Autenticidad de la Autoridad de Certificación: Se especifica la secuencia de campos que llena la Autoridad de Certificación y que identifican la firma electrónica digital de los campos previos. Dicha secuencia contiene tres atributos: el algoritmo de firma utilizado, el resumen (hash) de la firma, y la propia firma digital.

ARTÍCULO 13.- Los representantes de los suscriptores, señalan a la Dirección de Criptografía otros campos para el llenado de datos de los certificados digitales, en interés de servicios específicos o por requerimientos establecidos para las relaciones comerciales internacionales y de otra índole, con el objetivo de compatibilizar y estandarizar el formato de los certificados digitales con los prestadores de servicios criptográficos de certificación.

ARTÍCULO 14.- La Dirección de Criptografía comunica anualmente a los órganos, organismos de la Administración Central del Estado, entidades y a los prestadores de la Infraestructura de Llave Pública, los ajustes a realizar a las versiones de los certificados digitales, las extensiones a utilizar en sus archivos, los formatos electrónicos para las solicitudes y repositorios de los mismos y de sus correspondientes llaves de cifrado y firma; los campos opcionales a agregar a su formato, así como lo relacionado con la notación técnica para su llenado, y demás elementos técnicos y criptográficos que garanticen la seguridad e interoperabilidad en su empleo.

ARTÍCULO 15.- En los campos del certificado digital destinados a nombre, razón social y/o denominación de su solicitante, se admiten solo los datos de identidad verdaderos del titular.

ARTÍCULO 16.- Los certificados digitales son únicos y universales, se emiten y entregan a los representantes de los suscriptores, previa aprobación de la autoridad de registro correspondiente, por la Autoridad Raíz o una autoridad de certificación aprobada por el Ministerio del Interior, mediante la firma de un contrato de servicio.

SECCIÓN SEGUNDA

De la solicitud y otorgamiento de los certificados digitales de llave pública

ARTÍCULO 17.- La solicitud y otorgamiento de certificados digitales procede de la siguiente forma:

- a) El jefe del Órgano, Organismo de la Administración Central del Estado o entidad, mediante la persona designada por él como representante de los suscriptores de su ámbito, envía a la autoridad de registro correspondiente, de forma escrita, acuñada, y en el formato electrónico establecido por la Dirección de Criptografía al efecto, la relación de los datos necesarios de los candidatos a titulares de certificados digitales para el llenado de los campos obligatorios establecidos en el presente Reglamento para su emisión. En los casos de autogeneración de llaves criptográficas para la creación de la firma digital, la solicitud en formato electrónico se acompaña de la llave pública producida.

- b) La autoridad de registro, en un plazo no superior a los quince (15) días, realiza la comprobación de la identidad de cada candidato a suscriptor y de la posesión de las licencias correspondientes para la operación en el ámbito de las telecomunicaciones, a través de los sistemas estatales establecidos al efecto.
- c) De existir contradicciones con los datos identificativos presentados de los futuros titulares de certificados digitales, la autoridad de registro devuelve la solicitud al representante de los candidatos a suscriptores para que se rectifiquen.
- d) El jefe de la autoridad de registro, en un término de siete (7) días posterior a la conclusión del proceso de comprobación de identidad, envía a la autoridad de certificación correspondiente la solicitud de emisión de certificados digitales y la constancia de la verificación sobre la validez de los datos identificativos de los futuros suscriptores, en formato electrónico, con su firma digital y la del funcionario que procesa la información al respecto, en la garantía de la integridad y la autenticación de origen de la misma.
- e) La autoridad de certificación, en plazo no mayor a los treinta (30) días, posterior a la recepción de la solicitud de la autoridad de registro, produce, publica y entrega el certificado digital al suscriptor en los formatos convenidos con el mismo y de acuerdo con lo establecido en el presente Reglamento y en la Declaración de Prácticas de Certificación de la autoridad; realiza el cobro por su adquisición, de proceder y firma a tales efectos el contrato correspondiente según la legislación vigente en la materia.

ARTÍCULO 18.- El representante del suscriptor del Órgano, Organismo de la Administración Central del Estado o entidad interesada realiza la solicitud de CD-SSL de forma presencial en las oficinas de la autoridad de registro correspondiente, acompañado de los documentos originales de identificación del responsable del certificado digital y la titularidad del dominio a proteger para suscribir el contrato.

ARTÍCULO 19.- La autoridad de registro, en el caso de las solicitudes de CD-SSL, comprueba con la entidad reguladora competente, la veracidad de la titularidad de los nombres de dominios, datos de conectividad y servicios de infocomunicaciones, que el solicitante requiere proteger.

ARTÍCULO 20.- La autoridad de registro recibe del representante del suscriptor, en el caso de las solicitudes para la obtención de CD-SSL, además de los datos generales identificativos de los candidatos a responsables de su custodia y activación, la información sobre las características del equipamiento técnico de destino de dicho certificado digital.

ARTÍCULO 21.- Las autoridades de certificación realizan el proceso de generación, emisión y entrega de CD-SSL a partir de las normas de calidad y seguridad que establece la Dirección de Criptografía para la protección criptográfica de los servicios de comunicaciones.

ARTÍCULO 22.- La Dirección de Criptografía aprueba la necesidad de utilizar certificados digitales que funcionan en forma de comodines en los servidores de redes de infocomunicaciones, con el objetivo de evitar que un suscriptor pueda emplearlo para establecer un sitio web malicioso con protección criptográfica e imitar sitios legítimos.

ARTÍCULO 23.- Los suscriptores de certificados digitales son únicos. Un suscriptor puede poseer bajo su titularidad varios certificados digitales para diferentes funciones.

ARTÍCULO 24.- Establecer en el caso de los CD-Pfirma, las siguientes reglas:

- a) La llave criptográfica privada única la genera y custodia el suscriptor, a partir de los procedimientos de las tecnologías que se aprueben para la creación de la firma digital.
- b) Cuando la llave criptográfica privada, a solicitud del titular del certificado digital o por razones técnicas o de seguridad se genere en la autoridad de certificación, su producción se realiza obligatoriamente de forma compartida por tres funcionarios de esta entidad, y se entrega al suscriptor en un dispositivo informático o electrónico protegido con medidas de cifrado y control de acceso a ella por medio de una contraseña o código PIN.
- c) El traslado de la llave criptográfica privada, instalada en el dispositivo protegido, desde la autoridad de certificación hasta el puesto de trabajo del suscriptor, viaja con el PIN entregado por la autoridad.

La información confidencial sobre el código PIN para el acceso inicial a la llave criptográfica privada se envía al Órgano, Organismo de la Administración Central del Estado o entidad a la que pertenece su titular, en sobre sellado y lacrado a través de correo postal seguro y se entrega en la Oficina de Control de la Información Clasificada o similar, quien la hace llegar al suscriptor correspondiente.

- d) El titular de la llave criptográfica privada, puede cambiar el código PIN del dispositivo protegido, por otro código por él solamente conocido.
- e) La autoridad de certificación no guarda copia de la llave criptográfica privada del suscriptor, con el objetivo de asegurar la posesión exclusiva de su titular, en la garantía de la no existencia de dudas en la unicidad total del ejercicio de firma digital de documento, y el no repudio en esta acción personal e intransferible, de forma tal que no se pueda involucrar a la autoridad en hechos de falsificación o suplantación de la firma digital de un documento electrónico.
- f) Existencia de una seguridad criptográfica efectiva para que los datos utilizados en la generación de la firma digital, no puedan derivarse a partir de la llave pública empleada para la verificación de la misma por un tercero, o de la propia firma. De igual forma, la firma digital se protege contra su falsificación con la tecnología existente en cada momento.

ARTÍCULO 25.- Los certificados digitales y llaves criptográficas asociadas, solo se utilizan para el empleo determinado en la categoría establecida en el presente Reglamento y en las especificaciones para la emisión del propio certificado digital.

SECCIÓN TERCERA

De la suspensión, revocación y extinción de la vigencia de los certificados digitales de llave pública

ARTÍCULO 26.- La autoridad que emite los certificados digitales puede suspenderlos o revocarlos a solicitud del representante del suscriptor o por decisión propia, cuando las circunstancias de seguridad de la Infraestructura, o de la información y funciones del suscriptor así lo requieran, quien informa en este caso en un término no mayor a las veinticuatro (24) horas a la autoridad de registro que lo aprueba y al Órgano, Organismo de la Administración Central del Estado o entidad que ampara al suscriptor afectado.

ARTÍCULO 27.- La suspensión de un certificado digital tiene un carácter temporal, lo que implica la pérdida de su validez, similar a la de un certificado digital revocado durante el período de suspensión, que no excede a los treinta (30) días a partir de su anuncio y registro como tal, pasados los cuales dicho certificado digital se revoca automática y definitivamente.

El certificado digital dentro del tiempo de suspensión, se reactiva por el representante del suscriptor, quien realiza los trámites presenciales en la autoridad de registro correspondiente, cuando las causas de dicha suspensión hayan desaparecido.

ARTÍCULO 28.- La suspensión o la revocación del certificado digital de prestador de servicios criptográficos de certificación se realiza por solicitud del jefe de Órgano, Organismo de la Administración Central del Estado o entidad que lo ampara, al Ministerio del Interior a través de la Dirección de Criptografía, quien efectúa las investigaciones pertinentes, y somete a la aprobación del Ministro del Interior la decisión de suspensión o revocación mencionadas.

ARTÍCULO 29.- La solicitud de revocación tiene como mínimo la siguiente información:

- a) Fecha de solicitud de la revocación.
- b) Identidad del suscriptor.
- c) Razón detallada para la petición de revocación.
- d) Identidad y cargo funcional de la persona que pide la revocación.

ARTÍCULO 30.- El representante del suscriptor informa sobre la solicitud de revocación de un certificado digital a la autoridad de registro correspondiente, la que formula de proceder, la orden de revocación a la autoridad de certificación que lo emite, en un plazo no mayor a los tres (3) días hábiles, concluida la validación de dicha solicitud.

ARTÍCULO 31.- Una vez aprobada la revocación de un certificado digital, la autoridad de certificación genera y publica, en un plazo no mayor a las veinticuatro (24) horas una nueva lista de revocación de certificados (CRL).

ARTÍCULO 32.- Son causas de extinción de la vigencia de un certificado digital:

- a) Expiración del período de validez que figura en el certificado digital.
- b) Revocación formulada por el poseedor del certificado digital, a través de su representante, a la autoridad de certificación correspondiente que lo emite.
- c) Violación o puesta en peligro del secreto de los datos de creación de firma del suscriptor (poseedor del certificado digital) o del prestador de servicios criptográficos de certificación, o la utilización indebida de dichos datos por un tercero.

- d) Resolución judicial o administrativa que lo disponga.
- e) Fallecimiento del suscriptor, acreditada legalmente la defunción por su representante ante la autoridad de registro correspondiente.
- f) Extinción de alguno de los atributos legales del suscriptor para hacer uso del certificado digital, notificado por su representante, o como resultado de investigaciones, auditorías y controles establecidos por la legislación vigente.
- g) Fallecimiento de la persona que ejerce como representante del suscriptor o extinción del estatus establecido por el Órgano, Organismo de la Administración Central del Estado o entidad.
- h) Incapacidad sobrevenida, total o parcial, del suscriptor del certificado digital o de su representante.
- i) Terminación o extinción de la representación.
- j) Extinción o disolución de la persona jurídica bajo la cual el suscriptor posee y emplea el certificado digital.
- k) Alteración de las condiciones de custodia o del uso de los datos de creación de la firma digital, que estén reflejadas en los certificados digitales expedidos.
- l) Cese en la actividad del prestador de servicios criptográficos de certificación salvo que, previo consentimiento expreso del suscriptor, a través de su representante, la gestión de los certificados digitales expedidos por aquel se transfiera a otro prestador de servicios de la Infraestructura.
- m) Alteración de los datos aportados para la obtención del certificado digital o modificación de las circunstancias verificadas para la expedición del mismo, como las relativas al cargo o a las facultades de representación, de manera que este ya no es conforme a la realidad.
- n) Incumplimiento en el pago de los servicios criptográficos de certificación contratados con sus prestadores.
- o) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

ARTÍCULO 33.- La autoridad de certificación suspende la vigencia de los certificados digitales expedidos a sus suscriptores, si concurre alguna de las siguientes causas:

- a) Solicitud del suscriptor, a través de su representante y con la conformidad escrita del jefe del Órgano, Organismo de la Administración Central del Estado o entidad. Se incluye también a solicitud expresa de dicho jefe.
- b) Resolución judicial o administrativa que lo disponga.
- c) La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados digitales.
- d) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

ARTÍCULO 34.- La suspensión de la vigencia de un certificado digital, surte efecto a partir de su inclusión en el repositorio del prestador de servicios de certificación para la consulta pública por terceros.

ARTÍCULO 35.- La extinción y suspensión de la vigencia de un certificado digital no tiene efectos retroactivos.

ARTÍCULO 36.- El tiempo máximo de vigencia del certificado digital y las llaves criptográficas asociadas para su funcionamiento es el siguiente:

- a) Certificado Digital de la Autoridad Raíz: Quince (15) años.
- b) Certificado Digital de Prestadores de Servicios Criptográficos de Certificación: Diez (10) años.
- c) Certificados Digitales de suscriptores: Dos (2) años.

ARTÍCULO 37.- Para solicitar la renovación del certificado digital es necesaria en todos los casos, la presencia física del representante del suscriptor en las oficinas de la autoridad de registro correspondiente. Una vez aprobada la renovación, la autoridad de certificación determinada, realiza la emisión de un nuevo certificado digital.

CAPÍTULO III

DE LOS PRESTADORES DE SERVICIOS CRIPTOGRÁFICOS DE CERTIFICACIÓN DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA

SECCIÓN PRIMERA

De la organización de la Infraestructura de Llave Pública

ARTÍCULO 38.- La Infraestructura de Llave Pública se organiza jerárquicamente mediante un conjunto de entidades prestadoras de servicios criptográficos de certificación de la siguiente forma:

- a) El Servicio Central Cifrado del Ministerio del Interior que funge como Autoridad Raíz.
- b) Prestadores corporativos, que realizan las actividades de esta índole para el empleo de los certificados digitales por los suscriptores en el marco interno de un Órgano, Organismo de la Administración Central del Estado o entidad.
- c) Prestadores comerciales, básicamente empresas o entidades especializadas que en el marco de su objeto social, están en capacidad de realizar a favor de terceros las actividades de esta índole, mediante la venta de certificados digitales y cobros por dichos servicios a suscriptores.

SECCIÓN SEGUNDA

De la Autoridad Raíz

ARTÍCULO 39.- El Servicio Central Cifrado tiene las siguientes funciones:

- a) Generar y firmar digitalmente su propio certificado digital, así como producir las llaves criptográficas propias (pública y privada) para el ejercicio de sus funciones, en un acto especial de testificación y documentación.
- b) Producir y suministrar los criptomateriales específicos que requieran para la prestación de los servicios las autoridades de certificación aprobadas.
- c) Firmar digitalmente, los certificados digitales de los prestadores de servicios criptográficos de certificación aprobados para operar en la Infraestructura, así como de los funcionarios que laboran en la propia Autoridad Raíz.
- d) Asesorar técnica y organizativamente a los prestadores de servicios criptográficos de certificación incorporados a la Infraestructura.
- e) Informar a los prestadores de servicios criptográficos de certificación y suscriptores según corresponda, los parámetros técnicos, de seguridad y plazos de vigencia para el empleo de los criptomateriales y sus dispositivos portadores en los procesos de creación y verificación de la firma digital, así como los criterios complementarios necesarios para la elaboración de la Declaración de Prácticas de Certificación de dichos prestadores de servicios en el país.
- f) Participar según corresponda en las auditorías, inspecciones y controles estatales sobre la técnica criptográfica y demás funciones relativas a la Criptografía que se les practiquen a los prestadores de servicios criptográficos de certificación y suscriptores componentes de la Infraestructura.
- g) Realizar inspecciones técnicas con aviso previo, o sorpresivas a los prestadores de servicios criptográficos de certificación directamente subordinados y emitir el dictamen correspondiente.
- h) Participar en el análisis y aportar los elementos correspondientes sobre el cierre de la operación de prestadores de servicios criptográficos de certificación directamente subordinados.
- i) Organizar y realizar según corresponda la preparación especializada de los funcionarios de los prestadores de servicios criptográficos de certificación, así como el proceso de evaluación y acreditación de los niveles de profesionalidad alcanzados por cada uno, como condición necesaria de idoneidad para ejercer la actividad.
- j) Participar en las investigaciones de incidentes que atenten contra la seguridad y fiabilidad de la Infraestructura.
- k) Fungir como Autoridad de enlace técnico con autoridades raíces de otros países y de organizaciones internacionales, para asegurar la interoperabilidad de los certificados digitales cubanos y de la Infraestructura con sistemas similares del resto del mundo en las transacciones electrónicas de Cuba con el extranjero que estén aprobadas por los órganos y organismos de la Administración Central del Estado competentes.

ARTÍCULO 40.- El personal del Servicio Central Cifrado que ejerce la Autoridad Raíz, es acreditado como auditor criptográfico internacional por la entidad del país competente.

SECCIÓN TERCERA

De los Prestadores de Servicios Criptográficos de Certificación, Autoridades de Registro y de Certificación

ARTÍCULO 41.- Los prestadores de servicios criptográficos de certificación para el ejercicio de sus funciones, están obligados a cumplir los requisitos organizativos, tecnológicos y de seguridad siguientes:

- a) Tener definidos e implementados con evidencias, los roles compartidos de los administradores técnicos, los funcionarios de certificación especializados y los custodios del material criptográfico aprobado, así como las medidas de seguridad que se establecen en el presente Reglamento.

- b) Tener habilitado el Código de Ética de los funcionarios de la entidad prestadora de servicios criptográficos de certificación, los que están en el deber de guardar el secreto profesional respecto a los datos confidenciales de carácter personal de los suscriptores y de las tecnologías de procesamiento y gestión de los certificados digitales.
- c) Disponer de una página web oficial y publicar su certificado digital en el repositorio especificado, que incluye la huella digital del mismo para su comprobación por terceros; su Declaración de Prácticas de Certificación actualizada, aprobada y protegida su propiedad intelectual; los mecanismos de acceso publicitario del servicio, los precios de comercialización cuando corresponda, así como los datos suficientes del suscriptor para que pueda realizar el ejercicio de los procesos de firma digital de documentos y su verificación por terceros.
- d) Realizar cada dos (2) años la revisión de la Declaración de Prácticas de Certificación y someterla a la aprobación de la Dirección de Criptografía.
- e) Mantener accesible el servicio de consulta sobre la vigencia de los certificados digitales y hacer constar, de manera clara e inmediata, la extinción o suspensión de la vigencia de los mismos en el plazo previsto en el presente Reglamento. Este servicio debe tener la doble opción para consultar en línea de forma activa, mediante el uso del protocolo OCSP y la descarga de la lista de revocación por métodos clásicos, así como de correo electrónico protegido y otras variables que faciliten dicha consulta.
- f) Informar al suscriptor o a su representante de manera previa o simultánea a la extinción o suspensión de la vigencia de su certificado digital sobre este hecho, especificar los motivos, así como la fecha y hora en que el certificado digital queda sin efecto. En los casos de suspensión, informa además, su duración máxima. Se extingue la vigencia del certificado digital si, al final de dicho plazo, no se levanta la suspensión.
- g) Conservar toda la información relevante sobre las operaciones hechas con los certificados digitales, listas de revocación y estampados de tiempo por un período no menor a los quince (15) años; mantener la actualización del registro de eventos, en correspondencia con los requerimientos informativos y de señalización que al efecto establece la Dirección de Criptografía.
- h) Tener en funcionamiento permanente todas las medidas de seguridad física y lógicas, así como las trazas auditables de los eventos para el aseguramiento del dispositivo de confidencialidad de su llave criptográfica privada, y otros datos y medios requeridos por los suscriptores.
- i) Disponer de sistemas técnicos y/u organizativos de control, bloqueo, aviso y seguimiento de acceso y proximidad a los medios de trabajo especializados, y la aplicación racional de métodos de defensa criptológica frente a interceptaciones de sus comunicaciones e intromisiones informáticas o eléctricas en los equipos de prestación del servicio.
- j) Tener implementadas medidas para evitar y/o extinguir incendios, inundaciones, excesos de humedad y otros desastres tecnológicos, así como para la salva y restauración segura de la información de interés.
- k) Obtener, en los casos de prestadores comerciales de estos servicios, respaldo financiero mediante pólizas de seguro del tipo que corresponda, relacionados con los daños que un incidente de esta categoría cause a la actividad de los mismos.
Tener organizado el sistema de análisis y esclarecimiento de hechos contrarios al buen empleo de los certificados digitales bajo su jurisdicción, así como para la tramitación de las informaciones requeridas por los órganos administrativos, de control, fiscales y judiciales, según corresponda.
- l) Asumir toda la responsabilidad frente a los suscriptores y terceros de buena fe, en cuanto a la calidad del servicio que presta, con independencia de que parte de los procesos técnicos que lo aseguran se acuerden o contraten a una entidad externa al servicio criptográfico de certificación.
- m) Actualizar la información y estado de los parámetros de fiabilidad de todos los activos técnicos de la autoridad y demás prestadores de servicios criptográficos de certificación subordinados, así como realizar una clasificación de los mismos de acuerdo con sus necesidades de protección, en correspondencia con la evaluación de riesgos.

- n) Garantizar la seguridad de la parte de la Infraestructura bajo su jurisdicción de forma permanente para identificar posibles debilidades y establecer las acciones correctoras pertinentes, así como tener habilitados los medios para la revisión de todos los materiales desechables donde se almacena información para la eliminación segura de residuos informativos comprometedores de la seguridad de los suscriptores, la Infraestructura y los servicios de certificación.
- o) Disponer del equipamiento aprobado por la Dirección de Criptografía para la generación y gestión de los certificados digitales y los criptomateriales asociados, incluidos los medios de redundancia de los componentes técnicos más críticos, propios o contratados a una tercera entidad confiable y también aprobada; del plan de medidas para mantener los servicios de copia de respaldo y el Módulo Criptográfico de Alta Seguridad (MCAS) para la custodia y conservación de la llave privada de la autoridad o prestador de servicios criptográficos de certificación según corresponda.
- p) Realizar la activación de la llave privada bajo el principio de control con varias personas, que garantice que ningún funcionario en particular, tenga el dominio exclusivo de las actuaciones críticas.
- q) Atender y dar respuestas a las peticiones, quejas y reclamos hechos por los suscriptores y terceros de buena fe, de conformidad con lo que se establezca en la Declaración de Prácticas de Certificación.
- r) Tener actualizados y validados los resultados de auditorías, inspecciones y otros procedimientos de control interno, que demuestren la existencia de un ambiente confiable en el entorno de funcionamiento del prestador de servicios criptográfico de certificación, en correspondencia con lo establecido en la legislación vigente, teniendo en orden y acreditado por los órganos competentes, los mecanismos de solvencia económica para asegurar la prestación del servicio en general.
- s) Realizar obligatoriamente, una vez al año, una auditoría a todos los procesos de gestión de certificados digitales, en al menos una muestra del dos por ciento (2 %) de los certificados digitales gestionados, de acuerdo a la práctica internacional.

ARTÍCULO 42.- Los funcionarios que laboran en las entidades prestadoras de servicios criptográficos de certificación, son previamente aprobados, de acuerdo con los procedimientos estatales vigentes, por los jefes del Órgano, Organismo de la Administración Central del Estado o entidad de su jurisdicción, teniendo que haber recibido la preparación especializada y aprobar la evaluación que le realiza la Autoridad Raíz, la cual los acredita con el instrumento de titulación y el certificado digital correspondientes.

ARTÍCULO 43.- La solicitud para la creación de un prestador de servicios criptográficos de certificación, se acompaña de la fundamentación sobre la necesidad y el alcance del mismo en el territorio nacional y/o internacional que avala el jefe de Órgano, Organismo de la Administración Central del Estado o entidad solicitante, así como del estudio de factibilidad para su puesta en explotación y sostenibilidad en base a la evaluación de la existencia de condiciones tangibles para cumplir por el prestador de servicio propuesto con las obligaciones y facultades que establece el presente Reglamento.

ARTÍCULO 44.- La Dirección de Criptografía realiza las investigaciones y consultas previas necesarias con el Órgano, Organismo de la Administración Central del Estado o entidad interesada, y terceros pertinentes; elabora el dictamen correspondiente a presentar al Ministro del Interior para la aprobación o no del servicio solicitado, así como notifica con posterioridad al solicitante los resultados del proceso.

ARTÍCULO 45.- Las autoridades de certificación están facultadas para:

- a) Firmar digitalmente el certificado digital de la persona jurídica de los prestadores de servicios criptográficos de certificación subordinados; la lista de revocación de los certificados digitales de los prestadores de servicios criptográficos de certificación subordinados suspendidos temporal o definitivamente para operar en la Infraestructura, así como el de suscriptores asociados directamente a la autoridad.
- b) Realizar la preparación previa de los funcionarios aprobados de los prestadores de servicios criptográficos de certificación que se le subordinen para su evaluación y acreditación por la Autoridad Raíz, acción última que los autoriza a operar en la Infraestructura.

- c) Realizar inspecciones a los prestadores de servicios criptográficos de certificación bajo su jurisdicción para comprobar el mantenimiento de las condiciones de seguridad y confiabilidad del servicio.
- d) Realizar y/o participar, en el ámbito de su competencia, en las investigaciones criptológicas, cuando existan sospechas o se hayan cometido actos de vulneración de seguridad de la Infraestructura bajo su jurisdicción; en la comisión de delitos y otras acciones dañinas relacionadas con el mal empleo de los certificados digitales y los servicios asociados, actividad que se coordina previamente con la Autoridad Raíz.
- e) Asesorar y avalar los proyectos de Declaración de Prácticas de Certificación, así como los destinados para la instalación de las tecnologías de los prestadores de servicios criptográficos de certificación subordinados para ejercer sus actividades.
- f) Organizar comités de evaluación de seguridad, encargados de analizar los proyectos de Declaración de Prácticas de Certificación, antes de ser aprobada y publicada, siendo responsables de asegurar su integridad y disponibilidad para el acceso al público en la página web de la Autoridad de Certificación.
- g) Firmar los contratos de servicios de certificación con los suscriptores asociados, a través de sus representantes.
- h) Suministrar dispositivos criptográficos de alta seguridad para la creación de la firma digital y el resguardo de llaves criptográficas, previa validación por la Dirección de Criptografía.
- i) No expedir un certificado digital, cuando se ponga en riesgo la credibilidad, valor comercial y/o idoneidad moral o legal de parte o de toda la Infraestructura e informar en el marco de las setenta y dos (72) horas después del acto, a su autoridad jerárquica superior.
- j) Solicitar documentos adicionales a los exigidos en el formulario de solicitud de un certificado digital, en original o copia, como parte del proceso de registro, con el objetivo de verificar fehacientemente la identidad del solicitante; también puede eximir la presentación de cualquier otro documento secundario, cuando la identidad del solicitante haya sido suficientemente verificada, a través de los medios disponibles por la autoridad.

ARTÍCULO 46.- Los roles fundamentales a cumplimentar por los funcionarios de una autoridad de certificación son los siguientes:

- a) Jefe de Autoridad, que puede ser el mismo para la autoridad de registro, si están integrados en un solo órgano.
- b) Custodios de la Llave Privada de la Autoridad (2 funcionarios). Si la autoridad está integrada con la de registro, se emplea una sola llave para la autoridad.
- c) Receptor de datos de permisos de emisión. Puede ser el mismo de expedición de permiso, de estar integradas las autoridades.
- d) Generación de los certificados digitales.
- e) Publicación de los certificados digitales.
- f) Inspección y Auditoría.

ARTÍCULO 47.- El examen evaluativo para la acreditación de los funcionarios que ejercen los diversos roles en las autoridades de certificación, contiene como mínimo los siguientes elementos de comprobación de conocimientos sobre:

- a) La Declaración de Prácticas de Certificación.
- b) Las normativas vigentes en materia de Seguridad de la Información Oficial, Criptografía, las relacionadas con la Infraestructura y empleo de los certificados digitales.
- c) Las Políticas de Seguridad y la aceptación del Código de Ética, así como lo que se establece para la confidencialidad de la información que maneja en virtud de su rol.
- d) La operación de los medios computacionales y/o electrónicos, así como de las aplicaciones informáticas para cada puesto de trabajo específico.
- e) Los procedimientos de seguridad criptográfica en general y en particular para cada rol específico en la autoridad.
- f) Los procedimientos de operación y administración de cada rol específico para la segregación de funciones de certificación y los relacionados con el enfrentamiento a las contingencias.

ARTÍCULO 48.- No constituye información clasificada a los efectos de las operaciones de las autoridades de certificación, y por lo tanto es accesible a terceros, la contenida en la Declaración de Prácticas y en la Política de Certificación, así como el estado de los certificados digitales con los datos que establece el presente Reglamento para su publicación.

ARTÍCULO 49.- La información y documentación relativa a la gestión de los certificados digitales, se conserva durante un período mínimo de quince (15) años en archivos protegidos con técnicas de cifrado y autenticación, que aseguren el acceso solo a funcionarios autorizados para llevar a cabo verificaciones de integridad u otras, mediante el empleo de aplicaciones específicas y aprobadas de visualización y gestión de eventos.

ARTÍCULO 50.- La depuración de los archivos de conservación de la información relativa a los certificados digitales, se realiza, con la aprobación de la Autoridad Raíz y previa coordinación con los órganos, organismos de la Administración Central del Estado y entidades usuarias involucradas con los datos, en un acto donde participan los funcionarios designados de la autoridad.

ARTÍCULO 51.- Si los recursos técnicos, medios criptográficos y/o los datos de una autoridad de certificación u otro prestador de servicios criptográficos de certificación en la Infraestructura se alteran o se sospecha que han sido alterados, se detiene su funcionamiento hasta que se restablezca la seguridad del entorno, mediante instrucciones expresas de la Autoridad Raíz. La restitución del servicio se decreta por dicha autoridad, posterior al conocimiento de los resultados de la auditoría obligatoria a efectuar para identificar las causas de la alteración y asegurar su eliminación.

ARTÍCULO 52.- Las actividades críticas del proceso de certificación, requieren del control, seguimiento y registro sistemático de eventos que se producen durante su operación, las que se catalogan como mínimo en:

- a) Informativa: Significa que una acción se realizó de forma exitosa.
- b) Marca: Inicio y finalización de una sesión.
- c) Advertencia: Presencia de un hecho anormal pero no de una falla.
- d) Error: Una operación genera una falla predecible.
- e) Error fatal: Una operación genera una falla impredecible.

ARTÍCULO 53.- Los órganos, organismos de la Administración Central del Estado y entidades rectoras de procesos y sistemas de trabajo estatales, o ejecutores de servicios básicos para la economía y la sociedad que requieran del empleo de los certificados digitales pueden establecer autoridades de registro, que posibiliten un efectivo aseguramiento de la fiabilidad y viabilidad en la identificación y datos profesionales de los candidatos a suscriptores.

ARTÍCULO 54.- La autoridad de registro de un Órgano, Organismo de la Administración Central del Estado o entidad puede concertar contrato o convenio de trabajo con una autoridad de certificación de carácter comercial aprobada por el Ministerio del Interior, con el objetivo de encargarle la emisión de certificados digitales de suscriptores de su interés.

ARTÍCULO 55.- Los roles fundamentales que cumplen los funcionarios de una autoridad de registro son los siguientes:

- a) Jefe de Autoridad.
- b) Atención al público.
- c) Verificación de datos identificativos de solicitantes de certificados digitales, incluidos datos técnicos para CD-SSL.
- d) Custodio de la Llave Privada de la Autoridad (2 funcionarios).
- e) Expedición de permiso de emisión.

CAPÍTULO IV

DE LOS SUSCRIPTORES DE CERTIFICADOS DIGITALES DE LLAVE PÚBLICA

ARTÍCULO 56.- Los suscriptores poseedores de certificados digitales tienen las obligaciones siguientes:

- a) Suministrar a la autoridad de registro o a la autoridad de certificación según corresponda, la información exacta, completa y veraz en relación a los datos que esta solicite para la realización del proceso de registro.
- b) Conocer y aceptar, las condiciones de empleo del certificado digital, los criptomateriales y lo que establece el presente Reglamento, así como la Declaración de Prácticas de Certificación de la autoridad de certificación en la cual está inscripto.
- c) Cumplir las medidas de seguridad que establece la Declaración de Prácticas y en las Políticas de Certificación, que publica la autoridad de certificación a la cual está suscripto.
- d) Resguardar en lugar seguro, los dispositivos y llave privada para las operaciones criptográficas autorizadas a realizar con el certificado digital.
- e) No transferir a otra persona, los dispositivos para las operaciones criptográficas aprobadas a realizar, la llave privada y la clave personal de acceso al dispositivo de creación de firma (PIN).

- f) Asumir la responsabilidad y riesgos derivados de la fiabilidad y seguridad del puesto de trabajo, equipo y/o dispositivo informático o medio desde el cual emplee su certificado digital.
- g) Responsabilizarse con los riesgos derivados de la aceptación de una conexión de infocomunicaciones segura sin haber realizado previamente la perceptiva verificación de la validez del certificado digital exhibido por el prestador de servicios telemáticos. Los procedimientos para contrastar la seguridad de conexión de infocomunicaciones se aseguran por dicho servicio al poseedor.
- h) Renovar el certificado digital cuando por razones excepcionales se le haya modificado el número de identidad permanente.
- i) Emplear el certificado digital y sus medios criptográficos para los usos que se establecen en su emisión y para las funciones administrativas y de servicios que fundamentan su suscripción a la Infraestructura.
- j) Notificar, en un plazo de veinticuatro (24) horas, a su dirección superior inmediata, a los funcionarios de seguridad y protección de su Órgano, Organismo de la Administración Central del Estado o entidad, así como a la autoridad de certificación que emitió su certificado digital, a través de las vías contractuales establecidas con el prestador de servicios, cualquier hecho o situación anómala relativa al certificado digital y que tipifica como causa de revocación del mismo, e informar cuando considere que la seguridad de la protección criptográfica está en riesgo.
- k) Solicitar inmediatamente, a la autoridad de certificación que emite su certificado digital, la revocación o suspensión del mismo, a través de su representante legal, en caso de tener conocimiento o sospecha del comprometimiento de la seguridad de la llave criptográfica privada, entre otras causas por: pérdida, robo, compromiso potencial, conocimiento por terceros de la clave personal de acceso al dispositivo de resguardo de la llave criptográfica privada y detección de inexactitudes en la información.
- l) No realizar acciones o intentos de acciones de monitoreo, manipulación o de ingeniería inversa sobre la implementación técnica – hardware y software– de los servicios de certificación.
- m) Abonar los pagos que se establecen por la emisión del certificado digital y la prestación de los servicios criptográficos de certificación.

ARTÍCULO 57.- Los suscriptores poseedores de certificados digitales tienen los siguientes derechos:

- a) Recibir de la autoridad de certificación correspondiente, los datos de consulta para emplear los servicios de seguridad de la información que posibilita el uso del certificado digital.
- b) Solicitar la revocación y/o renovación de su certificado digital, a través de su representante legal, ante la autoridad de certificación correspondiente.
- c) Realizar las acciones de firma digital y autenticación de documento y origen de comunicaciones, asistido por el certificado digital y los métodos criptográficos aprobados.
- d) Autorizar la publicación del certificado digital de su posesión en los repositorios públicos de los prestadores de servicios de la Infraestructura.
- e) Devolver el certificado digital y los medios para su empleo al prestador de servicios criptográficos de certificación suministrador, en el término de garantía contratado con esa entidad, cuando compruebe su mal funcionamiento.
- f) Solicitar y recibir información de la autoridad de registro correspondiente sobre las causas de la suspensión o revocación de su certificado digital.
- g) Reclamar al prestador de servicio criptográfico de certificación que corresponda, el resarcimiento por los daños que ocasione a su actividad el mal funcionamiento de su certificado digital.

CAPÍTULO V

DE LAS FUNCIONES DE LA COMISIÓN CONSULTIVA PARA LA GOBERNANZA TECNOLÓGICA DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA

ARTÍCULO 58.- La Comisión Consultiva la integran especialistas designados de los ministerios de Comunicaciones, Fuerzas Armadas Revolucionarias, del Interior, Ciencia, Tecnología y Medio Ambiente (CITMA), Finanzas y Precios, Industrias y de Justicia; de las oficinas Nacional de Estadísticas e Información y Nacional de Normalización del CITMA, así como del Instituto de Criptografía de la Universidad de La Habana.

ARTÍCULO 59.- La Dirección de Criptografía organiza y coordina el funcionamiento de la Comisión Consultiva, la cual sesiona regularmente una vez cada seis (6) meses, y de forma extraordinaria cuando las circunstancias lo requieran, previa coordinación con los organismos de la Administración Central del Estado o entidad de pertenencia de sus miembros a través del sistema de planificación del Estado.

ARTÍCULO 60.- El Presidente de la Comisión Consultiva puede invitar a especialistas designados de otros órganos, organismos de la Administración Central del Estado o entidades, según los asuntos a tratar, previa solicitud a los jefes correspondientes del Ministerio del Interior.

ARTÍCULO 61.- La Comisión Consultiva emite recomendaciones y dictámenes sobre los siguientes elementos:

- a) Planes y rendición de informes estratégicos a los niveles superiores de dirección del Gobierno sobre el funcionamiento y la evolución técnico-organizativa de la Infraestructura.
- b) Proyectos de normativas técnicas y organizativas para la prestación de los servicios criptográficos de seguridad de la información y las comunicaciones ofrecidos por la Infraestructura.
- c) Creación de plataformas tecnológicas y dispositivos de operaciones criptográficas para el funcionamiento de los prestadores de servicios criptográficos de certificación de la Infraestructura.
- d) Proyectos de Declaración de Prácticas de Certificación de los prestadores de servicios criptográficos de certificación de la Infraestructura.
- e) Consideraciones técnicas de acuerdo con la práctica internacional y costos de la producción y servicios de Criptografía, para el establecimiento de los precios de comercialización de certificados digitales y de los tributos a los prestadores de servicios criptográficos de certificación y suscriptores, en correspondencia con la legislación vigente al efecto y las disposiciones del Ministerio de Finanzas y Precios.