DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

AUTORIDAD DE CERTIFICACIÓN DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA ETECSA (AC ETECSA)

(Versión 1.0)

11 de julio de 2024
"AÑO 64 DE LA REVOLUCIÓN"

1. INTRODUCCIÓN

ETECSA, fundada en 1994 con la misión de prestar servicios públicos de telecomunicaciones en Cuba y desarrollar el país socioeconómicamente, ha detectado la necesidad de contribuir en el uso de los certificados digitales como medio de autenticación segura, firma y verificación de documentos digitales, aseguramiento de confidencialidad y habilitación de canales de infocomunicaciones y sitios web seguros, entre otras aplicaciones, dentro de la propia empresa. También tiene como objetivo extender este servicio a terceros, que pueden ser otras empresas e instituciones o personas naturales, para que tengan la oportunidad de resguardar mucho mejor sus datos sensibles y los canales habituales de comunicación que emplean.

Con la Informatización de la Sociedad, la digitalización de la información, de los trámites personales y de los procesos internos de las empresas, se requiere mantener la integridad de los datos e identificar eficientemente al “propietario” o “responsable” de los mismos. El aporte a la economía nacional está en minimizar las importaciones de insumos de oficina y de equipos de impresión, y por consiguiente en recursos para el mantenimiento en el tiempo de estos. La sustitución de los documentos impresos por documentos digitales firmados a través de certificados digitales, fortalece la capacidad para compartir la información, comprobar su validez, autoría; agiliza la tramitación y procesamiento de grandes volúmenes de datos y optimiza los tiempos de respuesta.

También se acerca la cultura tecnológica a la población más analógica y le muestra la importancia de adicionar seguridad a los datos digitales que maneja, a la par que se cumplen con las regulaciones de protección de la información vigentes en Cuba y en el mundo, cada vez más globalizado y que exige en muchos escenarios que se protejan trámites y datos usando este servicio de Llave Pública.

Tomando como referencia lo planteado con anterioridad, se propone el texto dep presente documento con las principales pautas que regulan el funcionamiento de la Infraestructura de Llave Pública ETECSA.

1.1. Presentación

Esta Declaración de Prácticas de Certificación describe las prácticas y procedimientos implementados por la Autoridad de Certificación ETECSA (en lo adelante AC ETECSA) para brindar Servicios de Llave Pública dentro de la empresa y a terceros (*personas naturales o jurídicas)*, con los que comercializa los diferentes certificados digitales emitidos a través de la Plataforma de Gestión de Certificados Digitales (PGCD)- de desarrollo propio -, que respalda dicho proceso fundamental.

Cumpliendo con el artículo 4.13 de la Res. 2/16 del MININT, este documento se publicará en el sitio web oficial de la Empresa y también en la anteriormente mencionada plataforma *PGCD* (*https://certificados.etecsa.cu*).

Para la redacción del documento se tomó como guía la Declaración de Prácticas de Certificación (versión 1) de la Autoridad de Certificación Servicio Central Cifrado, emitida en marzo de 2016.

1.2. Nombre e identificación del documento

Este documento se titula “Declaración de Prácticas de Certificación” AUTORIDAD DE CERTIFICACIÓN DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA ETECSA (AC ETECSA) (versión 1).

1.3. Participantes de la Infraestructura de Llave Pública (PKI)

1.. Estructura general de la Infraestructura de Llave Pública

La Infraestructura de Llave Pública de la AC ETECSA, se subordina a la Autoridad Raíz representada por la Autoridad de Certificación Servicio Central Cifrado (ACSCC). La ACSCC es el máximo *Representante* en Cuba de los Servicios Criptográficos, definido por la Res. 2/16 del MININT, y del conjunto de Autoridades de Certificación permitidas en el territorio nacional. La AC ETECSA forma parte subordinada y confiable de esta cadena de autoridades de confianza.

La AC ETECSA implementa lo pautado en esta Declaración de Prácticas de Certificación hacia sus Divisiones Organizativas internas. *La comercialización y*

extensión de los Servicios de Llave Pública a personas naturales y jurídicas forman parte de los objetivos de la Empresa en una segunda etapa.

A través de esta infraestructura se puede establecer y mantener un entorno seguro de gestión de certificados digitales, para los usuarios con roles de *funcionario* de la Autoridad de Registro y de Certificación y también para los propios Titulares de certificados, a través del uso de la *PGCD*.

Con esta plataforma se automatizan los procesos asociados al *registro*, *aprobación*, *emisión*, *revocación y renovación* de certificados digitales (CD). Posee un sistema de trazas en las que quedan reflejados los procesos de gestión por los que transita una solicitud hasta convertirse en CD y conserva las acciones de los funcionarios que interactúan con ellos. Se incluyen además los servicios de la Autoridad de Validación (VA) que posibilitan la verificación de la validez de cada uno de los CD emitidos, permitiendo el uso de las funciones de: Firma Digital, Autenticación de usuarios a servicios y aplicaciones, y la protección de canales de comunicación.

2.. Entidad de Certificación (EC)

La Entidad de Certificación de la AC ETECSA tiene como principal activista dentro de la *PGCD* al *Funcionario EC*[1], el cual tiene la máxima responsabilidad de efectuar la *emisión*, *la revocación o la renovación* de un CD, cualesquiera sea su tipología –*firma digital*, *SSL*, *VPN*-. Además, cuenta con interfaces gráficas que resumen la actividad de todas las Unidades Organizativas (UO) subordinas. Se recomienda que este funcionario forme parte de los *cuadros* o *directivos* de la Empresa.

La AC ETECSA emite sus CD-Pfirma y los CD-SSL destinados a *Candidatos* de la Empresa o clientes externos a esta, a partir de la *PGCD*. Estos son firmados y emitidos tomando como base el certificado de Autoridad de Certificación que firmó y reconoce la ACSCC. En el caso de la emisión de los CD-SSL se generan a partir de criptomateriales (PEM) entregados también por la ACSCC y ha establecido el "*Procedimiento de Operación para distribuir CD-SSL*" que garantiza el flujo de trabajo correcto para dicha generación.

[1] Rol asociado a una persona cuyos datos son verificados previo a la asignación de tal responsabilidad.

La AC ETECSA desempeñará las funciones de Autoridad de Certificación y Autoridad de Registro, al unísono, cuando se el solicitante del servicio PKI proceda de la Empresa; y como Autoridad de Certificación cuando se solicite por terceros.

Los tiempos de respuesta a solicitudes de *emisión*, *revocación o renovación* de CD no excederán los (3) días hábiles a partir de su recepción.

3.. Entidad de Registro (ER).

La Entidad de Registro de la AC ETECSA es la encargada de verificar que coinciden las solicitudes de *Candidatos* aprobados por la máxima dirección de la UO solicitante y los registros efectuados por el *Representante* en la *PGCD*. Tiene como principal activista dentro de la *PGCD* al *Funcionario ER*, el cual solo podrá disponer de la información de actividad de las Autoridades de Registro bajo su control.

Como parte de otras de las acciones que los *Funcionarios ER* realizan se encuentra el envío de las solicitudes de *emisión*, *revocación o renovación* a la *EC*, para la gestión correspondiente. Y también, el intercambio con el o los *Representantes* que se le subordinen para informar errores o solicitar datos requeridos para el correcto funcionamiento del servicio.

Los tiempos de respuesta a solicitudes de aprobación de *emisión*, *revocación* o *renovación* de CD no excederán los (3) días hábiles a partir de su recepción.

4.. *Representante.*

El *Representante* de una UO es el máximo responsable de insertar los datos de las personas o servicios que requieren CD en la *PGCD* y que estos sean veraces. Deben tomar en cuenta solo los *Candidatos* aprobados por la máxima autoridad de la UO y bajo ese mismo criterio realizar la solicitud del CD, con los datos que se le pidan a través de la *PGCD*.

Se encarga de hacerle llegar al respectivo funcionario de la ER que lo atiende, el predicho listado de *Candidatos*, con las actualizaciones que vayan surgiendo durante el transcurso de la prestación del servicio.

5.. Titular.

Son aquellos Usuarios Finales que usarán los CD y los Servicios Criptográficos asociados a la PKI de la AC ETECSA: pueden ser personas, dispositivos electrónicos, aplicaciones informáticas, u otros. Son los máximos responsables de la custodia del CD puesto a su disposición y responden administrativa y/o legalmente según sea el caso, por el incorrecto uso o manipulación del mismo.

6.. Terceros de buena fe.

Son las personas o entidades (diferentes al Titular del certificado), que pueden o no tener a su cargo un CD, sin embargo, deciden *aceptar* y *confiar* en un certificado digital emitido por la AC ETECSA.

1.4. Usos de los certificados digitales

Los CD que emite la AC ETECSA tienen un uso determinado y bien específicos, de acuerdo a la autorización otorgada por la Autoridad Raíz. Pueden emplearse para: firma de documentos digitales, firma de certificados, firma de CRL, No Repudio, firma de cógido fuente y de correos electrónicos; reconocimiento de Llave y cifrado de Llave. Por otro lado, para protección de canales de comunicación (Autenticación Servidor Web TLS, Autenticación Cliente Web TLS) y para Estampado de Tiempo. No está permitido el cifrado de cualquier tipo de información usando los certificados que emite la AC ETECSA.

Se incluyen las firmas digitales para trámites, correspondencias y servicios a la población. También se tienen en cuenta para garantizar la interacción de las empresas cubanas con entidades homólogas extranjeras y el comercio electrónico internacional, siempre y cuando estás últimas acepten como *confiables* los CD emitidos por la AC ETECSA.

Estos certificados constituyen la garantía de la protección de la información que se firma, se procesa, se transmite o se almacena con la utilización de las tecnologías de la información y otros medios electrónicos. Se emitirán de acuerdo a lo normado en los “Requerimientos técnicos, organizativos y de seguridad provisionales para el Servicio Criptográfico basado en la Infraestructura de Llave Pública”.

1.. Uso apropiado de los certificados digitales

Atendiendo a su uso permitido, los CD se clasifican en las siguientes categorías:

a) Categoría 1: Certificados digitales de Llave Pública para la Firma Digital de mensajería y ficheros electrónicos. Se les denomina como CD – Pfirma.
b) Categoría 2: Certificados Digitales de Llave Pública de carácter técnico para la protección de canales y servicios de comunicaciones. Se les denomina como CD-SSL.

2.. Prohibición en el uso de los certificados digitales

Los certificados digitales sólo podrán emplearse de acuerdo a lo establecido en el numeral 1.1.4.1 de esta Declaración.

1.5. Detalles del Contacto

1.. Organización de la Administración de la Declaración de Prácticas de Certificación

Esta Declaración de Prácticas de Certificación fue redactada por Especialistas en el Grupo de Prevención de Fuga de Información (*GPFI*) de la DOPS, con el objetivo de la implantación de la Infraestructura de Llave Pública para la empresa ETECSA y otras empresas, instituciones, entidades o personas naturales; bajo la supervisión de la dirección general de la empresa y el personal técnico especializado de la ACSCC.

2.. Colectivo técnico de contacto

Todo comentario o sugerencia relativa a esta Declaración de Prácticas de Certificación, puede ser dirigido al *GPFI*, teléfonos *(537)876-7876*, o a la dirección de correo soportepki@etecsa.cu.

1. **Colectivo técnico que determina la coherencia entre la Declaración de Prácticas de Certificación y la política**

En caso de ajustes o cambios en esta Declaración de Prácticas de Certificación, que pueda interferir lo que está regulado en las diferentes políticas, debe contactarse en la siguiente dirección con el colectivo técnico, responsable de mantener actualizadas y en buen estado esta Declaración de Prácticas de Certificación y sus políticas.

Dirección de Seguridad Tecnológica, teléfono: *(537)876-7812* o a la dirección de correo soportepki@etecsa.cu.

3.. Procedimiento de aprobación de las Declaraciones de Prácticas de Certificación

El procedimiento de aprobación de la Declaración de Prácticas de Certificación de la AC ETECSA se elaboró según lo establecido en el acápite 1.1.5.3 de la Declaración de Prácticas de Certificación de la Autoridad de Certificación Raíz de la República de Cuba.

1.6. Definiciones y acrónimos

1.. Definiciones

Son las establecidas en los "Requerimientos técnicos, organizativos y de seguridad provisionales para el Servicio Criptográfico basado en la Infraestructura de Llave Pública"

2.. Acrónimos

CA	Autoridad de Certificación
AC ETECSA	Autoridad de Certificación Intermedia ETECSA
AC ETECSA-ER	Entidad Registradora de la Autoridad de Certificación ETECSA
AC ETECSA-EC	Entidad Certificadora de la Autoridad de Certificación ETECSA
ACSCC	Autoridad de Certificación Servicio Central Cifrado
ACSCC-EC	Entidad Certificadora de la Autoridad de Certificación Servicio Central Cifrado
ACSCC-ER	Entidad Registradora de la Autoridad de Certificación Servicio Central Cifrado
RA	Autoridad de Registro
VA	Autoridad de Validación
CD o CID	Certificado digital o certificado de identidad digital
CRL	Lista de Certificados Revocados
DC	Dirección de Criptografía del Ministerio del Interior

DPC	Declaración de Prácticas de Certificación
PKI	Infraestructura de Llave Pública
MININT	Ministerio del Interior
OCSP	Protocolo de verificación en línea del estado de los certificados
OU	Unidades Organizativas
PIN	Clave personal de acceso
PSCC	Prestador de Servicios Criptográficos de Certificación

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIOS

1.1. Repositorios

La AC ETECSA dispone de repositorios donde se publican: su certificado firmado por la ACSCC, los certificados emitidos por la propia AC, las CRL, la DPC y sus actualizaciones y otras informaciones relativas a la AC ETECSA y su servicio PKI.

Dado el creciente número de entidades de diferentes sectores económicos que encuentran en la Firma Digital una salida a las limitaciones materiales para el almacenamiento y vigencia de su información institucional impresa, la Dirección de ETECSA, de conjunto con asesores técnicos, comerciales y la aprobación de la ACSCC, propone implementar Servicios de Llave Pública e integrarse al Sistema de Autoridades Certificadoras nacionales.

Además, se sugiere crear Autoridades de Registro subordinadas a la AC ETECSA, en correspondencia con cada uno de los contratos comerciales que se firmen entre las partes. De esta manera se garantiza mejor manejo de las solicitudes, mejor control y seguridad de la información de los Titulares y mayor gestión de certificados por las diferentes entidades.

Toda la información contenida en los repositorios es pública y está disponible las 24 horas del día y los 7 días de la semana. Cuando se produzca una interrupción por causa de Fuerza Mayor, la AC ETECSA cuenta con el equipo de soporte que de antemano tiene la responsabilidad de restablecer el servicio en el menor tiempo posible.

1.2. Publicación de información sobre certificación

Es responsabilidad de la AC ETECSA publicar su certificado digital firmado por la ACSCC, el cual puede ser descargado desde la dirección https://www.etecsa.cu/es/certificados-digitales

La AC ETECSA está en la obligación de:

a) Publicar y mantener actualizado el repositorio de los certificados emitidos,
b) Publicar y mantener actualizadas las Listas de Certificados Revocados (CRL), las cuales pueden ser descargadas desde la siguiente direccione URL: http://certificados.etecsa.cu/ocsp/crl-download/
c) La dirección señalada en b) está insertada en los certificados digitales emitidos, como argumento del campo "*Punto de distribución CRL*".
d) Publicar y mantener actualizada la DPC, la llave pública de ACSCC y la llave pública de AC ETECSA en el sitio https://www.etecsa.cu/es/certificados-digitales

1.3. Frecuencia de publicación de la CRL

1.. Certificado digital de la AC ETECSA

El actual certificado firmado por la ACSCC tiene un período de validez de cinco (5) años, es decir, estará vigente hasta 2026. Como estrategia para evitar detenciones innecesarias en el servicio, un año antes del vencimiento se notificará a la ACSCC y a terceros subordinados; y tres(s) meses antes se solicitará a la ACSCC la generación del nuevo certificado de autoridad.

2.. Certificados digitales emitidos por la AC ETECSA

Los certificados digitales emitidos por la AC ETECSA se publicarán inmediatamente posterior a su emisión, con la correspondiente actualización del repositorio de certificados.

3.. Lista de Certificados Revocados (CRL)

Las CRL correspondientes a la AC ETECSA tendrán un periodo de validez de 15 días y se publicarán en:

http://certificados.etecsa.cu/ocsp/crl-download/

La realización de un cambio de estado en alguno de los certificados emitidos trae consigo la generación de una nueva CRL, y esta se actualizará en un término no mayor a las veinticuatro (24) horas de realizado el cambio de estado del certificado digital.

En caso de no existir un cambio en los estados de los certificados emitidos, se actualizará esta CRL antes de su fecha de caducidad.

4.. Declaración de Prácticas de Certificación

La AC ETECSA realizará cada dos (2) años una revisión de esta DPC y las nuevas versiones se publicarán por los canales aquí definidos, de forma inmediata, luego de su aprobación por la ACSCC.

1.4. Controles de acceso a los repositorios

El acceso a la información que publica la AC ETECSA en su web oficial para la Autoridad https://www.etecsa.cu/es/certificados-digitales, sólo permitirá funciones de consulta a la información pública del repositorio de los certificados digitales emitidos. La modificación o actualización de la información, queda restringida a los funcionarios de la AC ETECSA que están a cargo de tales responsabilidades.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

1.1. Nombres

1.. Tipos de nombres

La AC ETECSA genera y firma certificados con tipos de nombres acordes al estándar X.509 v3.

Para el certificado AC ETECSA, el Nombre Distinguido (DN) tanto del Titular (subject) como del Emisor (issuer), está formado por los siguientes atributos:

- CN = ETECSA
- OU = ETECSA
- O = MINCOM
- L = Playa
- ST = La Habana
- C = CU

2.. Necesidad de que los nombres sean significativos

La AC ETECSA garantiza que los Nombres Distinguidos (DN) de los certificados emitidos por ella sean significativos, lo que permite establecer la identificación unívoca del Titular del certificado y vincular su identidad con la clave pública. Esta garantía se concreta con el apoyo de sistemas de Bases de Datos que permiten la comparación nombres de usuarios, Nombre(s) y Apellidos, de forma tal de que cada certificado sea único e irrepetible.

3.. Reglas para la interpretación de los diferentes formatos de nombres

Para la interpretación de los Nombres Distinguidos en los certificados emitidos por la AC ETECSA, se utilizan las reglas descritas en la ITU-T X.500 Distinguished Name (DN). Para todos los atributos se utiliza la codificación UTF-8.

4.. Unicidad de los nombres

Los nombres de los Titulares son únicos para poder identificarlos plenamente. En el DN se utiliza una combinación de valores que permite garantizar la unicidad, basada en los especificado en el numeral 3.1.1.2.

5.. Solución de conflictos relativos a nombres

La AC ETECSA utilizará algoritmos automáticos para generación de nombres de usuario de certificados que sean únicos e irrepetibles, tomando como punto de partir

1.2. Validación inicial de identidad

1.. Autenticación de la identidad de una persona

Como paso previo a la realización de solicitudes, la AC ETECSA exigirá que cada UO que requiera los servicios de Llave Pública, expecíficamente el uso de la *PGCD* que declare quién actuará como *Representante* de sus Titulares, resguardando dicha información hasta que se produzca algún cambio de *Representante*, por los motivos que fuere.

La solicitud de un CD la realiza el *Representante* del Titular, que se encarga de *registrar* los datos del C.I del *Candidato*, completando los campos de la interfaz correspondiente en la *PGCD*.

Los datos en la solicitud serán contrastados por el *Funcionario ER* a cargo de la UO solicitante. De no corresponder alguna información, este notificará al *Representante* sobre los detalles de la negación de continuidad del trámite, Hasta este punto se realiza una primera fase de validación de la identidad de solicitante contra los sistemas instaurados en ETECSA para tales efectos, si se tratase de uno de sus trabajadores; o contra *la Ficha Única del Ciudadano*, *cuando se trate de terceros*. En el caso de la ER la solicitud es validada en un término de tres (3) días hábiles posteriores a la fecha de solicitud.

Para el caso de un tercero con una Autoridad de Registro constituida mediante contrato y subordinada a la AC ETECSA, sus funcionarios a cargo de la administración de dicha autoridad definen los periodos en que validan la solicitud realizada por sus Titulares.

2.. Información no verificada del Titular

No se aceptará por parte de la AC ETECSA información de un Titular que no pueda ser verificada por los canales establecidos en el numeral 3.1.2.1 de esta DPC.

3.. Validación de Autoridad

El *Candidato* que requiera acreditar en su certificado digital el cargo que desempeña en la entidad donde trabaja, deberá presentar además de sus datos personales, la documentación pertinente que acredite el *nombramiento* dicho cargo. En este caso la AC ETECSA aplica con lo establecido en la Res. 23, del MININT, de noviembre de 2022.

El mismo tratamiento se tendrá en cuenta cuando la AC ETECSA tramite una solicitud de un *Sello Electrónico*.

4.. Criterios para la Interoperación

La AC ETECSA establece un nivel de dependencia e interoperabilidad con la ACSCC, y esta a su vez con Autoridades de Certificación nacionales, con otras Autoridades Raíz y organizaciones de otros países. De esta forma se asegura el reconocimiento y las cadenas de confianza de los certificados digitales cubanos y de la Infraestructura de Llave Pública nacional 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.

1.3. Identificación y Autenticación de solicitudes de renovación de claves

La *renovación* de claves para la AC ETECSA consiste en la creación de una nueva llave privada y su correspondiente certificado; a partir de los datos del Titular guardados en la *PGCD*, tras haber sido revocado por cualquiera de las causas descritas en el numeral 4.1.8 de esta DPC. Los procedimientos para la *renovación* de un certificado que se describen en el numeral 4.1.5 de esta DPC.

1.4. Identificación y Autenticación de solicitudes de revocación

El *Funcionario ER* al recibir del *Representante* el "Modelo de solicitud de Revocación de CD", aplica lo descrito en el numeral 4.1.8.2 y reenvía la solicitud a la EC, a través del interfaz correspondiente en la *PGCD*. Para que el proceso cumpla con las regulaciones vigentes, se debe especificar como justificación de la revocación del certificado, la causa que la provocó. De esta manera se asegura la trazabilidad de los motivos de revocación ante posibles reclamaciones o auditorías al servicio.

La EC al aceptar la revocación del CD, este pasa a un nuevo estado: "Revocado". Con esta acción la EC debe garantizar la actualización de la nueva CRL y publicarla inmediatamente por los canales de información de los que disponga el servicio.

4. Requerimientos operacionales del ciclo de vida de los certificados

1.1. Solicitud de certificados digitales

1.. Habilitados para solicitar certificados digitales

Están habilitados para solicitar certificados digitales a la AC ETECSA, directamente usando la *PGCD*, los *Representantes* de las OU interesadas en el servicio de Llave Pública. Sus permisos son recibidos y verificados por su homólogo en la AC, teniendo en cuanta el "Modelo de nombramiento de *Representante*" firmado por la máxima autoridad en dicha OU. Sus datos son contrastados en Bases de Datos generales (LDAP, Ficha Única del Ciudadano, u otras) enlazadas al *PGCD*.

2.. Proceso de solicitud y responsabilidades

La solicitud de un CD la realiza el *Representante* de una OU, a través de la interfaz de la *PGCD*. También el propio *Candidato* puede hacerla presencialmente ente un *Funcionario ER*. En ambos casos, es responsabilidad del *Funcionario ER* comprobar la validez de la identidad del solicitante aplicando el proceso descrito en el numeral 3.1.2.

La protección a la información de los todos los usuarios en la *PGCD* está dada por:

- Uso de un canal seguro HTTPS para el acceso y gestión de la plataforma.
- Los permisos sobre la Infraestructura se asignan de acuerdo a los roles de confianza definidos en el numeral 5.1.2.1 de la presente DPC.
- La solicitud de certificados solo es visible para el *Representante* de una OU y para un funcionario ER.
- La información de los certificados emitidos puede listarse por el Titular del CD, su *Representante* (si procede) y los *Funcionarios ER* y *EC*.

1.2. Procesamiento de la solicitud del certificado

1.. Realización de las funciones de identificación y autenticación

Las funciones de identificación y autenticación se realizan por parte *Representante* de la UO; el cual ha sido verificado contra el modelo de nombramiento para su cargo y ha recibido los permisos correspondientes para efectar estas tareas.

Una vez recibida la solicitud en la ER, firmada por el *Representante* (si procede), se realiza la comprobación de la identidad del *Candidato* según la descripción del numeral 3.1.2.

De existir contradicciones con los datos identificativos del *Candidato* la ER rechaza la solicitud, notificando al *Representante* sobre el error.

Si todos los datos son correctos, el *Funcionario ER* procede a *Aprobar* la solicitud. Posterior a la aprobación, la solicitud *desaparece* de la lista, enviándose al listado de “Pendientes de emisión”, visible para el *Funcionario EC*. Tras la emisión por la EC, el Titular podrá descargar su llave privada del enlace que recibe en el e-mail ingresado en su solicitud.

Igualmente reciben la notificación de entrega el *Funcionario ER* y el *Representante* del Titular.

2.. Aprobación o denegación de la solicitud

Cada *Funcionario ER* tiene dentro de sus tareas las de aprobar o denegar las solicitudes de certificados digitales.

A partir de la recepción de la solicitud de un certificado digital, el *Funcionario ER* tiene un período de hasta tres (3) días hábiles para la ejecución de todo el proceso de aprobación o denegación de la solicitud. En el caso de una ER subordinada, esta puede establecer periodos de aprobación o denegación diferentes, nunca superiores a los que define la AC ETECSA-ER.

Las solicitudes de certificación serán rechazadas cuando no cumplan con los requerimientos de información solicitados, cuando no sea posible la verificación de la información brindada por el *Candidato*, o cuando se compruebe falsedad en la información proporcionada.

En todos los casos, se notificará al *Representante* la denegación de la solicitud y sus causas, vía e-mail.

En el caso de aceptación de la solicitud por parte de la ER correspondiente, a través de la *PGCD*, se *Aprueba* la solicitud y esta se envía al(los) funcionario(s) de la AC ETECSA-EC. Este proceso es notificado a los involucrados mediante mensajes de e-mail, informándose en cada caso en qué estado se encuentra la solicitud y qué rol la está realizando.

3.. Plazo para el procesamiento de la solicitud de un certificado

A partir de la recepción de la solicitud de certificado digital, la AC ETECSA-ER tiene un período de tres (3) días hábiles para la ejecución de todo el proceso de la solicitud de un certificado., este puede establecer periodos de aprobación o denegación diferentes, nunca superiores a los que define la AC ETECSA-ER.

1.3. Emisión del certificado

1.. Acciones de la Autoridad de Certificación durante la emisión del certificado

El proceso automático de emisión de certificados digitales utilizado por la AC ETECSA basa su funcionamiento en la confianza de los datos insertados por el

Representante nombrado por la UO y por la revisión efectuada por el *Funcionario ER*. Utilizando los metadatos del CD emitido por la ACSCC, se completan los datos del Emisor y el CORE de *PGCD* genera el nuevo certificado al instante. Cuando esto ocurre se genera una notificación de e-mail para el Titular con el enlace de descarga del certificado en formato PKCS #12 *(<archivo.p12>)*.

1.. Certificados PFirma.

a) En el caso de los certificados para Firma Digital, el permiso de emisión va acompañado de un fichero digital en formato PKCS #10, que contiene la llave pública del Titular.
b) La AC ETECSA-EC valida la autenticidad e integridad del permiso de emisión y a partir de la información contenida en el fichero PKCS #10, genera y firma el certificado digital del Titular.

1.4. Aceptación del certificado

1.. Forma en la que se acepta el certificado

El contrato firmado entre la AC ETECSA y la entidad *Representante* del Titular, contiene el reconocimiento legal y los términos y condiciones sobre los usos correctos y prohibiciones asociados al certificado que se le entregará. Como respaldo a estos acuerdos, la AC ETECSA recomienda que cada entidad contratada recoja en su Código de Ética, en su plan de Seguridad Informática o a través de Actas de Responsabilidad, el compromiso de cada Titular de proteger y no divulgar los elementos de seguridad vinculados al certificado digital que ha recibido.

Además, como parte de la ayuda a la correcta comprensión sobre la aplicación de los servicios de Llave Pública, la AC ETECSA entrega a la entidad contratada una copia de esta DPC, para que la utilice como guía de trabajo.

2.. Publicación del certificado

Una vez generado y firmado el certificado por la AC ETECSA-EC, este se habilita para que sea descargado directamente por el Titular a través de un enlace enviado al e-mail insertado en su solicitud. Tanto el *Representante* como los *Funcionarios ER* y *EC* solo pueden ver el estado "Emitido" y los detalles del certificado, pero sin permisos para descargarlo. El Titular es el único responsable de descargar su certificado y protegerlo del uso por terceros.

Aun cuando el proceso de aprobación del CD ocurriera presencialmente, el *Funcionario ER* no tendrá a su disposición funciones de descarga del criptomaterial. La documentación usada como material de consulta y configuración de las aplicaciones recomendadas para ejercer la Firma Digital de documentos, pueden obtenerse en la sección *Documentación* del sitio oficial de la Autoridad.

3.. Administración de las Llaves de los Titulares

Los servicios asociados a la administración de las llaves de los Titulares suministradas por la AC ETECSA serán gestionados por la *PGCD* y la llave privada se destruirá mediante borrado seguro una vez sea descargada por el Titular.

1.. Uso de la llave privada por parte del Titular

El Titular poseedor de un CD está en la obligación de:

a) Emplear responsablemente el certificado digital de llave pública y sus medios criptográficos para los usos establecidos en su emisión y para las tareas establecidas en sus funciones administrativas.
b) No transferir a otra persona la llave privada ni la contraseña que la protege.
c) Solicitar inmediatamente a la ER correspondiente la revocación de su CD, en caso de tener conocimiento o sospecha del comprometimiento de la seguridad de su llave privada, o por cualquiera de las causas siguientes: pérdida o robo del dispositivo de almacenamiento con una copia del CD, conocimiento por terceros de la contraseña o detección de inexactitudes en la información del CD.
d) Notificar en un plazo no mayor de las 24 horas, a su dirección inmediata superior, a los funcionarios de seguridad y protección de su órgano,

organismo, entidad u otros, así como a la ER que lo aprobó, cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

2.. Uso del certificado y la llave pública por un Tercero de buena fe

Los Terceros de buena fe pueden depositar su confianza en los certificados emitidos para el uso que establece esta DPC.

Además, se requiere de los Terceros de buena fe:

a) No realizar acciones o intentos de acciones de monitoreo, manipulación o de ingeniería inversa sobre la implantación técnica – hardware y software – de los servicios de certificación.
b) Notificar a la AC ETECSA cualquier hecho o situación anómala relativa a los certificados, así como informaciones o sospechas de comprometimiento o violación de la seguridad del servicio.

1.5. Renovación de un certificado

Se entiende por renovación de un certificado al proceso de emisión de una nueva llave privada y su certificado, independientemente que este haya expirado o no; y, por consiguiente, su revocación inmediata en caso de no haber llegado a su término de expiración. Cada Titular de un CD recibe en su sesión de usuario en la *PGCD*, una notificación del tiempo restante para la expiración de su certificado vigente. El descuento se notifica con 30 días de antelación y un recordatorio a los 15 días, estableciendo un margen de tiempo para solicitar la renovación por parte de su *Representante*.

Esta notificación es recibida igualmente por el *Representante* del Titular, el cual se encargará de pedir la renovación desde su sesión en la *PGCD* y, además, enviará como confirmación al *Funcionario ER* correspondiente, por e-mail, el "Modelo de solicitud de Certificados Firma Digital" firmado.

La solicitud de renovación es Aprobada si el *Funcionario ER* comprueba que la petición del solicitante y los datos del modelo coinciden. Con la aprobación, la solicitud es enviada al *Funcionario EC* para el proceso correspondiente.

En la EC, este tipo de solicitud se procesa como la emisión de un nuevo certificado digital, con estado "Emitido".

Faltando 24 H para la expiración del certificado, el *Funcionario EC*, que está informado de este límite de vigencia mediante el Dashboard de su sesión de trabajo en la *PGCD*, debe proceder a revocar el CD, de forma tal que este último no supere su tiempo de vigencia.

1.. Circunstancias para la renovación de un certificado

Un certificado digital puede ser renovado a solicitud del Titular o su Representante, pocos días antes de culminar su tiempo de vigencia o cuando se cumple al menos una de las condiciones listadas en el artículo 32, Res 2/16 emitida por el MININT.

2.. Personas habilitadas para solicitar la renovación

Las personas habilitadas para solicitar la renovación son: el Representante del Titular.

3.. Procesamiento de la solicitud del certificado

El procesamiento se realiza tal como se establece en el numeral 4.1.2 de esta DPC.

4.. Conducta constitutiva de la aceptación del certificado

Es la misma que se establece en el numeral 4.1.2 de la esta DPC.

5.. Publicación del certificado renovado

Para descargar el certificado renovado, el Titular recibirá un enlace por e-mail. Además, será publicado de inmediato en el repositorio de la AC ETECSA, como ocurre con un nuevo certificado digital, para garantizar el proceso de validación de los Terceros de buena fe.

1.6. Cambio de clave del certificado

Dentro de la sesión de Titular en la *PGCD*, no se permite el cambio de clave de un certificado. Si por cuestiones de seguridad de la llave privada, el Titular considera la posibilidad de cambiar la contraseña que resguarda dicha llave, debe utilizar aplicaciones de tipo *Desktop* que lo permitan. En caso de que un Titular olvide la contraseña de la llave privada o detecte que un tercero la

conoce, debe comunicarse con su Representante o con la ER que lo aprobó, aplicando lo especificado en el numeral 4.1.8 de la presente DPC.

1.7. Modificación del certificado

Durante el ciclo de vida de un certificado digital, la AC ETECSA no tiene como política modificar los campos de un certificado en tanto se encuentre vigente. Cuando se requiera modificar algún campo de este, se aplica el numeral 4.1.8.2 de la presente DPC.

1.8. Suspensión y revocación del certificado

1.. Circunstancias para la revocación.

Son circunstancias para la revocación de un certificado emitido por la AC ETECSA:

a) Expiró el tiempo de validez del certificado digital.

b) Solicitud del Suscriptor a través del *Representante*.

c) Violación o puesta en peligro del secreto de los datos de creación de Firma Digital del Titular, o la utilización indebida de dichos datos por un tercero. Esto incluye olvido de la contraseña o pérdida de la llave privada.

d) Resolución Judicial o Administrativa.

e) Fallecimiento del Suscriptor.

f) Extinción de alguno de los atributos legales del Titular para hacer uso del certificado, informado por su jefe, o como resultado de investigaciones, auditorías y controles establecidos por la legislación vigente.

g) Fallecimiento del *Representante* del Suscriptor.

h) Cierre de la Entidad.

i) Incapacidad parcial o total del Suscriptor.

j) Terminación o extinción de la Representación.

k) Extinción o disolución de la persona jurídica del Suscriptor.

l) Alteración de las condiciones de custodia o uso de los datos de creación de la Firma Digital que estén reflejadas en los certificados expedidos.

m) Cese del Prestador.

n) Alteración de datos aportados o modificación de las circunstancias verificadas.

o) Incumplimiento en el pago de los Servicios Criptográficos contratados.

2.. Procedimiento de solicitud de la revocación

Tanto Titular como *Representante* pueden efectuar la solicitud de revocación de un CD e informar al *Funcionario ER* que lo aprueba, a través de la *PGCD*. El campo "Motivos de la revocación" debe contener alguna de las razones expresas en el numeral 4.1.8.1.

El *Funcionario EC* dento del listado de solicitudes que recibe, puede identificar las que tengan el estado "Pendiente de Revocación". Posterior a su visualización, podrá revocar el CD definitivamente. Este proceso se debe efectuar en un periodo de tiempo no superior a las (24) horas hábiles posteriores al momento de recepción de la solicitud de revocación.

Con cada revocación efectiva se actualiza el listado de certificados con ese estado y, por tanto, la AC ETECSA genera una nueva CRL, haciéndola pública de inmediato. El Titular y su *Representante* reciben una notificación por e-mail (de manera automática) con la efectividad de la revocación del CD.

3.. Tiempo dentro del cual la Autoridad Intermedia debe procesar la solicitud de revocación

La AC ETECSA procesará una solicitud de revocación en un plazo no mayor a 24 H luego de recibida la misma.

4.. Frecuencia de emisión de la CRL

La AC ETECSA mantiene publicadas las CRL permanentemente en la URL que se lista en el numeral 2.1.3.3 de la presente DPC. La frecuencia de emisión es de 15 días, siempre que no se hayan producido revocaciones de certificados digitales. La AC ETECSA actualiza la CRL luego de una revocación de certificado en un término no mayor a las veinticuatro (24) horas.

5.. Disponibilidad de la verificación en línea de la revocación

La verificación del estado en línea que se puede realizar sobre los CD se puede realizar consultando la siguiente URL, usando el protocolo OSCP.

a) http://certificados.etecsa.cu/ocsp/

6.. Requerimientos especiales para el caso del comprometimiento de la llave privada

En caso de comprometimiento de la llave privada de la AC ETECSA, se procederá a detener el servicio, se notificará la afectación en la web oficial del servicio y se revocarán todos los certificados vigentes hasta el momento.

La AC ETECSA iniciará un proceso de identificación de las causas de la afectación, un proceso de mitigación/aceptación de los riesgos y una vez controlada la eventualidad, se gestionará con la ACSCC la emisión de un nuevo par de llaves.

Obtenidas las nuevas llaves criptográficas se procederá a la emisión de los nuevos certificados a los Titulares que tenían certificados vigentes en el momento de producirse el comprometimiento. Si los CD revocados formaban parte de un contrato de prestación de servicios de Llave Pública, la AC ETECSA los emitirá libre de costo.

7.. Circunstancias para la suspensión de un certificado

La AC ETECSA no tiene concebido dentro del flujo de trabajo de su servicio de Llave Pública la suspensión de actividad de CD. Por consiguiente, la suspensión de un CD implica directamente la revocación del mismo y se consideran los motivos mencionados en el numeral 4.1.8.1 de la presente DPC.

8.. Procedimiento para solicitar la suspensión

Para solicitar la suspensión de un certificado digital se debe seguir la descripción del numeral 4.1.8.2 de la presente DPC.

9.. Límite del periodo de suspensión

No aplica.

1.9. Servicios de estado del certificado digital

Para la validación de los CD, se proporciona información sobre el estado de los certificados emitidos por la AC ETECSA mediante las siguientes variantes:

a) Listas de Certificados Revocados (*CRL*), las cuales pueden ser descargadas desde la dirección URL que se lista en el numeral 2.1.2.b)
b) Protocolo de comprobación del estado de un certificado en línea (*OCSP*), verificable desde la URL listada en el numeral 4.1.8.5.

1.. Características operacionales.

Cualquier información publicada por la AC ETECSA respecto al estado de los certificados emitidos, se emitirá firmada digitalmente.

2.. Disponibilidad del servicio.

El servicio de comprobación del estado de los certificados emitidos por la AC ETECSA es accesible de forma ininterrumpida los 365 días del año.

1.10. Finalización de la suscripción.

Se dará por finalizada la suscripción de un certificado digital en los siguientes casos:

a) Caducidad de la vigencia del certificado digital.

b) Por revocación del certificado, por cualquiera de las circunstancias señaladas en el numeral 4.1.8.1.

1.11. Custodia y recuperación de llaves

1.. Políticas y prácticas de recuperación de llaves

Según establece en la Res. 2/2016 del MININT, las llaves privadas que se entregan a Titulares, deben ser eliminadas de forma segura de la plataforma que las genera, una vez se haya descargado la única copia del CD por el propio Titular del mismo. Es competencia de la AC ETECSA aplicar borrado seguro a las llaves privadas de Firma Digital, SSL o VPN que se generen en la *PGCD*, culminado el proceso de entrega.

5. CONTROLES FÍSICOS Y OPERACIONALES

1.1. Controles físicos

Los aspectos referentes a los controles de seguridad física se encuentran descritos en el documento “Políticas de Seguridad de la Información para la PKI de la empresa”, del Plan de Seguridad Informática de la AC ETECSA. En este apartado se van a recoger las medidas adoptadas más relevantes.

La AC ETECSA tiene implementadas medidas de seguridad para la protección física de los locales donde realiza sus operaciones.

Las estaciones de trabajo de los funcionarios ER y EC se encuentran en locales que se cierran con llave y con sellos diariamente. Los accesos de estas PC a la *PGCD* se regulan por direcciones IP y poseen contraseña en el BIOS; y los permisos y roles son gestionados desde la interfaz de administración. Sus chasis permanecen con los sellos puestos por el personal técnico responsable de tal nivel de protección.

Como otra medida que contempla al hardware involucrado para la emisión de CD, se encuentra el empleo de un disco duro encriptado, garantizando con esto que al encender la máquina virtual sea necesario desencriptar el volumen de disco duro.

La contraseña del disco duro encriptado, la define y es de conocimiento del responsable de Seguridad Informática y se guarda en sobre lacrado y sellado en el local de la dirección de la Empresa.

La contraseña del usuario del Sistema Operativo (no root) es definida por el Administrador de Red y se guarda en un sobre lacrado, en el local de la dirección de la Empresa.

En el hardware en cuestión están deshabilitados la torre de CD y los puertos USB.

1.. Ubicación y construcción del local

La PKI de la AC ETECSA se encuentra hospedada en uno de los Centros de Datos Virtuales (CDV), ubicado en un perímetro físico de seguridad de la empresa, donde se almacenan un conjunto de servidores que prestan entre otros el servicio de gestión de CD a través de la *PGCD* en esta URL: https://certificados.etecsa.cu

La descripción constructiva y de localización del edificio donde está ubicado el CDV está reflejada en el documento “<nombre del documento>”, con número de referencia <tal>, resguardado en la OCIC.

Cumple los siguientes requisitos físicos:

a) Ubicado en el núcleo del edificio para una máxima protección contra desastres naturales.
b) Sistema de protección y prevención de incendios: detectores, extintores, formación del personal para actuar ante incendios.

c) Sistema de detección contra intrusos en la puerta.
d) Sistema de alimentación ininterrumpida (UPS).

2.. Acceso físico

El acceso al CDV está restringido al personal autorizado y se presenta en la puerta de entrada al local: Director/a General, Director/a de Tecnología, Administrador/a de la red y Responsable de Soporte Técnico. En compañía del Administrador de Red, están autorizados los demás directores y el Responsable de Seguridad Informática. El resto del personal que lo requiera, deberá contar con la autorización de la máxima dirección de la Empresa.

3.. Alimentación eléctrica y aire acondicionado

El CDV cuenta con las condiciones de alimentación eléctrica y estabilización de voltaje necesarios, para evitar fallas y otras anomalías eléctricas. Los equipos se encuentran conectados a fuentes de alimentación ininterrumpidas (UPS) que garantizan el apagado controlado del equipamiento, durante la ausencia de fluido eléctrico, así como la protección del mismo ante fluctuaciones de voltaje.

Los sistemas de aire acondicionado garantizan las condiciones de temperatura y humedad adecuadas para el correcto funcionamiento y mantenimiento del equipamiento.

4.. Almacenamiento de los medios

La AC ETECSA ha establecido el “Procedimiento de salvas y recuperación de Datos”, indispensablle para regular las acciones de aseguramiento de copias de respaldo de toda la información y documentación relativa a la gestión de los certificados. Las bases de datos con los datos de CD emitidos se conservarán durante un período de hasta quince (15) años, en archivos protegidos con técnicas criptográficas de cifrado y control de acceso, según las regulaciones vigentes.

5.. Protección del equipamiento y seguridad del cableado

El CDV cuenta con los siguientes medios de protección de sus diferentes estructuras:

a) Sistema de protección y prevención de incendios: detectores de humo, extintores y personal preparado para actuar ante incendios.

b) Sistema de detección de intrusos en la puerta.

El cableado de la red eléctrica está protegido de interferencias o daño, mediante el uso de canaletas.

6.. Mantenimiento de los equipos

Todo trabajo de reparación o mantenimiento a un equipo de la AC ETECSA solamente podrá ser realizado por el equipo de Soporte Técnico y debe ser registrado en los documentos Registro de Incidencias de la Seguridad de la Información de la AC ETECSA.

7.. Seguridad en la reutilización o eliminación de los equipos

Antes de autorizar la salida de cualquier equipo que contenga datos relacionados con la gestión de CD, para realizar operaciones de mantenimiento planificadas o no, se procederá a resguardar los discos duros en la OCIC. Y en el caso de que sea necesario cambiar o deshacerse de algún equipo obsoleto, a los discos duros se les aplicará borrado seguro y desmagnetización.

8.. Retiro de activos

Para realizar el retiro de cualquier activo perteneciente a la AC ETECSA se deberá contar con la autorización del Jefe de la AC ETECSA, de conjunto con el Administrador de la plataforma, quienes hacen constar en acta cada activo retirado.

9.. Protección de los activos

El acceso a los activos dentro de la PKI de la AC ETECSA está dado por:

a) Controles de acceso a locales donde se procese información de gestión de los certificados.

b) Acceso controlado por roles y por canal seguro *HTTPS* a la *PGCD*, para cada funcionario dentro de la AC ETECSA.

c) Los roles definidos dentro de la AC ETECSA solo tienen acceso a los módulos que les permita realizar sus funciones en la *PGCD*.

1.2. Controles de procedimientos

1.. Roles de confianza

Los roles de confianza establecidos por la AC ETECSA son los siguientes:

(1) Representante:

- Funcionario seleccionado por la máxima dirección de la Unidad Organizativa solicitante del servicio de Llave Pública para tramitar las solicitudes de los suscriptores.

(2) Para el trabajo de la AC ETECSA como ER:

- Jefe: Jefe del Grupo de Prevención de Fuga de Información
- Atención a usuarios: Especialista (1) del Grupo de Prevención de Fuga de Información
- Verificador: Especialista (2) del Grupo de Prevención de Fuga de Información

(3) Para el trabajo de la AC ETECSA como EC:

- Jefe de la Autoridad: Director de la Dirección de Seguridad Tecnológica
- Custodio de llave privada: Administrador de Red y el Responsable de Seguridad Informática
- Receptor de permisos de emisión: Esp. A (1) del Grupo de Prevención de Fuga de Información
- Inspector auditor: Jefe del Grupo de Prevención de Fuga de Información
- Administrador de la plataforma: Esp. A (2) del Grupo de Prevención de Fuga de Información
- Custodio de material criptográfico: Administrador de Red (responsable de la Máquina Virtual donde se encuentra el software para la PKI) y *Representante* (responsable del traslado)
- Generación de certificados digitales: Integrada a la Autoridad de Certificación: Director de la Dirección de Seguridad Tecnológica, Jefe del Grupo de Prevención de Fuga de Información y Esp. A (3) del Grupo de Prevención de Fuga de Información (todos con rol de *Funcionario EC* para emitir CD)

Para el trabajo de una ER subordinada a la AC ETECSA, pero perteneciente a un tercero, donde media contrato, se sugieren los siguientes funcionarios:

(1) Jefe: Director(a) de Capital Humano.

(2) Representante: Especialistas de la Dirección de Capital Humano en cada una de las Direcciones.

(3) Verificador: Especialista en Seguridad Informática de la Empresa.

2.. Número de personas requeridas por tareas

El trabajo ininterrumpido de la AC ETECSA puede estar condicionado por la cantidad de solicitudes de CD que se realicen, la cantidad de personas que reciban y ejecuten tales solicitudes y por la estabilidad de los recursos destinados a sostener el servicio.

La relación de personas por *rol* queda como sigue:

a) Para el trabajo de las AC ETECSA-ER:

- Jefe: Una (1) persona.
- Representante: de (1) a (3) personas.
- Verificador: de (1) a (3) personas.

b) Para el trabajo de la AC ETECSA-EC:

- Jefe: Una (1) persona.
- Custodio de llave privada: (2) personas.
- Receptor de permisos de emisión: (1) personas.
- Inspector auditor: (1) persona.
- Administrador del Sistema: (1) persona.
- Custodio de material criptográfico: (1) persona.
- Emisión de certificados digitales [2]: (2) persona.

c) Para la realización de las funciones diarias, se requiere la presencia de:

- Jefe de la AC ETECSA-ER, Jefe de la AC ETECSA-EC, Atención a Usuarios y Verificador.

[2] Cuando se trate de la prestación del servicio a terceros, la cantidad de funcionarios en estas funciones dependerá de la demanda que exija el servicio.

3.. Identificación y autenticación por cada rol

Cada funcionario posee su propio certificado digital emitido por la AC ETECSA. Las acciones que puede ejecutar cada uno dentro de la *PGCD* son asignadas de acuerdo las funciones que estos realicen, directamente por el Administrador de este; a partir de la Resolución o Instrucción emitida por la máxima autoridad de la AC ETECSA.

4.. Roles que requieren separación de funciones

Los roles de la AC ETECSA-ER son incompatibles con los roles de la AC ETECSA-EC y viceversa.

Los roles de Inspector auditor y Administrador de sistema son incompatibles con todos los roles.

5.. Actividades Críticas

Las actividades críticas del proceso de certificación identificadas se listan a continuación:

(1) Asignar roles a usuarios
(2) Crear una Autoridad de Registro (RA)
(3) Asignar rol de funcionario EC
(4) Asignar rol de funcionario ER
(5) Asignar funcionario ER como administrador de una RA
(6) Solicitar certificado digital
(7) Aprobación de solicitudes de certificados digital por parte de la ER
(8) Firma de certificados digitales aprobados por parte de la EC
(9) Solicitud de revocación de certificados por un Titular o su *Representante*
(10) Solicitud de renovación de certificados por un *Representante*
(11) Revocación de certificados emitidos por la EC
(12) Renovación de certificados solicitados por la ER

El sistema posee un módulo de *Trazabilidad* que garantiza el control, seguimiento y registro de las acciones ejecutadas por los funcionarios con roles asignados dentro de este.

1.3. Controles del personal

1.. Sanciones por acciones no autorizadas

Las actuaciones y acciones no autorizadas por parte de los funcionarios y los PSCC que forman parte de la PKI de la AC ETECSA, violatorias del régimen de seguridad y de roles especificados para la operación de estas entidades, se califican como hechos sancionables administrativa o penalmente, en correspondencia con la gravedad de los daños provocados y la legislación vigente.

2.. Documentación suministrada al personal

La AC ETECSA proporciona a sus funcionarios, a Titulares y Terceros de buena fe toda la documentación necesaria para el correcto desempeño de sus responsabilidades. Entre la documentación que se entrega se encuentran:

(1) Declaración de Prácticas de Certificación de la Autoridad Certificadora

(2) Manuales de operaciones de cada Funcionario ER y EC con la *PGCD*

(3) Manuales de configuración de aplicaciones para Firma Digital para Usuarios

(4) Plantillas de solicitudes por tipos de certificados

1.4. Archivo de registros

1.. Tipos de registros archivados

La AC ETECSA archiva toda la información relacionada con:

(1) Ciclo de vida de las llaves de la autoridad.

(2) Ciclo de vida de los certificados digitales.

(3) Ciclo de vida del sistema automatizado para la gestión de los certificados digitales.

(4) Controles de acceso a locales y equipamiento.

(5) Modificaciones a los procedimientos y metodologías de trabajo.

(6) Modificaciones a las DPC.

(7) Auditorias y controles.

Los controles, modificaciones y auditorías procederán y serán registrados como es debido de acuerdo al Manual de Seguridad Informática de ETECSA.

2.. Período de conservación del archivo

La AC ETECSA conservará los registros de gestión de los certificados digitales durante un período mínimo de quince (15) años. Los restantes archivos se conservarán de acuerdo a la política de control de archivos de la Empresa.

3.. Protección del archivo

Los registros se archivan protegidos con técnicas criptográficas de cifrado y control de acceso, de forma que nadie pueda acceder a ellos, salvo los funcionarios autorizados para llevar a cabo verificaciones de integridad.

Además, se establecen medidas de protección física y de control de acceso al local donde se encuentran archivados los registros.

4.. Procedimiento para la copia de seguridad del archivo

Según procedimiento para la salva de Información de ETECSA contenido en el documento Plan de Seguridad Informática, numeral 5.3.3.3 Sistemas de Salva de Respaldo.

5.. Procedimiento para el sellado de tiempo de los registros

Todos los registros se archivan con información de fecha y hora. Para el caso de los involucrados con los servicios de la AC ETECSA, se cuenta con un NTP para la sincronización de dichos servicios, según la hora de Cuba, para garantizar la coincidencia de la fecha y hora de los equipamientos con la hora oficial del país.

6.. Procedimiento para obtener y verificar la información del archivo

La obtención y verificación de la información sólo se realiza por el personal debidamente autorizado, el cual hará uso de las herramientas de verificación y control aprobadas por la Dirección de ETECSA para tales fines.

1.5. Cambio de llaves

El tiempo de validez del certificado de la AC ETECSA entregado por la ACSCC es superior al período de validez de los certificados para Titulares. Una vez este certificado expira, todas las llaves que haya generado la Autoridad y se

encuentren vigentes también expirarán. El tiempo de vigencia de un certificado de Autoridad Certificadora es habitualmente de diez (10) años. Por consiguiente, *como mínimo, tres (3) meses antes de expirar este periodo*, la AC ETECSA debe solicitarle a la ACSCC la generación de un nuevo par de llaves.

Este periodo previo de solicitud se realiza para asegurar la tenencia de un certificado sustituto al que quedará sin efecto. Además, tras la actualización del certificado de Autoridad Certificadora, se minimiza el tiempo de restablecimiento del servicio a la totalidad de usuarios.

Los *Representante*s de terceros son notificados un (1) año antes de este vencimiento, para que decrescan las nuevas solicitudes de CD hasta tanto se produzca la actualización de certificado raíz de la Autoridad o soliciten certificados digitales con tiempo de vigencia igual a un (1) año.

Una vez recibido el nuevo certificado raíz de la Autoridad, se procede, de forma inmediata, a renovar los certificados de los Titulares, de forma tal que todo certificado que se genere en la PKI, luego del cambio de llaves de la AC ETECSA, tenga en su cadena de certificación el nuevo certificado de la Autoridad Intermedia.

La AC ETECSA continúa emitiendo CRL firmadas con la llave privada previa, hasta la fecha de vencimiento del último certificado emitido por esta; y se incorpora la validación de los nuevos certificados emitidos por la nueva llave.

1.6. Recuperación ante el comprometimiento y desastres

1.. Procedimientos para la gestión de incidentes y comprometimiento

El Jefe de la AC ETECSA y sus funcionarios, ante la ocurrencia de cualquier incidente de seguridad de los recursos puestos en función de la gestión de certificados digitales, debe aplicar lo descrito en el Plan de Contingencia determinado para el Servicio PKI, donde se identifican todos los riesgos que pueden provocar la inutilización o degradación de los servicios que presta, así como las acciones a realizar ante cada uno de estos eventos, de forma tal que permita dar continuidad a la prestación de sus servicios esenciales.

2.. Alteración de los recursos de hardware, software y/o datos

Ante una sospecha o alteración de los recursos de hardware, software y/o los datos, la AC ETECSA detendrá su funcionamiento, informando de inmediato a todos los Titulares para que detengan la utilización de los CD bajo su custodia y para que estén atentos a las informaciones que defina la Autoridad Certificadora. Además, procederá a efectuar una auditoría para identificar la causa de la alteración y asegurar su eliminación.

Una vez restablecida la seguridad del entorno, se procederá a la restitución de los servicios, dando prioridad a la publicación de las CRL.

La administración del tiempo de vida del hardware criptográfico utilizado por la AC será definida por el Administrador de Red de la empresa ETECSA.

3.. Procedimiento ante el comprometimiento de la llave privada

El comprometimiento de la clave privada de la AC es considerado como un *desastre* y para su documentación se deben adicionar según corresponda en los documentos siguientes:

(1) Plan de Prevención de Riesgos

(2) Manual de Procedimientos de Seguridad Informática, que incluye: Plan de Contingencia, Registro y Gestión de Incidencias de Seguridad de la Información de ETECSA, Procedimiento de Salva de Información

El comprometimiento de la clave privada de la AC debe contrarrestarse inmediatamente con la solicitud de revocación a la ACSCC y la notificación a esta de las irregularidades detectadas, ya sea vía correo electrónico o teléfono. También se debe notificar a los Titulares y *Representantes* de que se procederá a la revocación de la totalidad de certificados emitidos que se encuentren vigentes.

En un plazo no mayor de 24 horas la AC ETECSA gestionará con la ACSCC la generación de un nuevo para de llaves y un nuevo certificado digital firmado como Autoridad de Certificación.

A partir de ese momento procederá a la emisión de los nuevos certificados a los Titulares que tenían certificados vigentes en el momento de producirse el comprometimiento de la llave privada.

La AC ETECSA mantendrá en sus repositorios los certificados revocados, incluyendo el suyo, con el objetivo de garantizar la verificación de que dichos certificados fueron emitidos durante el período de funcionamiento.

4.. Capacidad de la continuidad de las operaciones después de un desastre

La AC ETECSA tiene previsto en su Plan de Contingencia las acciones a realizar ante cualquier evento, para garantizar la continuidad de sus operaciones. El comportamiento será el descrito en el numeral 5.1.5 de esta DPC.

1.7. Cese de las operaciones

La AC ETECSA en su condición de Autoridad de Certificación dentro de la jerarquía de los PSCC de la República de Cuba, podrá cesar sus actividades de servicios de certificación por decisión de la Dirección de ETECSA debido a condiciones que lo justifiquen. Una vez tomada la decisión, esta se comunicará por los canales informativos de la Empresa, así como en la web oficial donde se expone el servicio PKI de la AC.

6. CONTROLES DE SEGURIDAD TÉCNICA

1.1. Generación e instalación del par de llaves

1.. Generación del par de llaves

El par de llaves de la AC ETECSA es generado y entregado por la ACSCC en dispositivo de almacenamiento extraíble, con métodos criptográfico aplicados y se resguarda en la OCIC, junto a la contraseña que se preserva en sobre lacrado y acuñado.

2.. Importar el par de llaves de la AC en la *PGCD*

Para importar el par de llaves, firmadas por la ACSCC y recogida por el *Representante* de la AC ETECSA, el Administrador de Red debe buscar el dispositivo extraíble que la contiene en la OCIC y copiarla en la ruta de carpetas de la *PGCD*, con permisos de escritura, junto al Responsable de Seguridad Informática, ambos responsables de su custodia.

El Administrador de la *PGCD* debe recoger en la OCIC el sobre lacrado con la contraseña de la llave privada de la AC; acceder al Módulo de Administración y

seleccionar la opción para insertar la contraseña de la llave privada, que se cargará automáticamente de la ruta de carpetas donde fue copiada.

El sobre lacrado y el dispositivo extraíble que contienen información sobre la llave privada de la AC deben devolverse a la OCIC.

Durante la inclusión del par de llaves en la *PGCD* de la AC ETECSA, estarán presentes cuatro (4) personas:

(1) Jefe de la Autoridad de Certificación
(2) Administrador de la *PGCD*
(3) Administrador de Red
(4) Representante de la Autoridad de Certificación

3.. Descarga de la llave privada por parte de cualquier funcionario del PSCC

Tras la emisión de los certificados digitales por un funcionario EC o por el servicio automático que se encarga de este proceso, se enviará una notificación de emisión satisfactoria directamente al Titular del CD, usando el e-mail correspondiente; propocionado durante el registro de su solicitud. El resto de los actores del PSCC solo recibirán la notificación de emisión correspondiente, dejando constancia de su estado vigente. *Ni el Representante del Titular, ni los funcionarios ER o EC tiene la posibilidad de efectuar la descarga de un CD más allá del suyo propio*.

4.. Entrega de la llave privada al Titular del certificado digital

La llave privada solo puede ser descargada desde la sesión del Titular en la plataforma *PGCD*. Para los casos VPN y SSL, que son impersonales, se enviarán a la sesión del *Representante* de la RA, encargado de tales solicitudes. La opción de descarga se habilita tras la inserción de un código de verificación enviado previamente al e-mail proporcionado durante la solicitud de registro. Se habilitará un único intento de descarga. Una vez descargada la llave privada, se elimina de la *PGCD* y se mantiene la llave pública disponible en la sesión del usuario. El Titular pasa a ser el único responsable del resguardo y custodia de su CD para Firma Digital. Lo mismo ocurre con los SSL y VPN respecto al *Representante* de la RA. Todas estas acciones se llevan a cabo mediante el uso de un canal seguro usando el protocolo *HTTPS*.

La plataforma *PGCD* estará disponible para Titulares, *Representante*s, la Entidad de Certificación, Entidades de Registro propias de la Empresa y para entidades subordinadas. Por política de seguridad de la AC ETECSA, no se permite la visibilidad de esta plataforma a Terceros de buena fe.

5.. Descarga de la clave pública de la Autoridad a los Terceros de buena fe

Al encontrarse limitado el acceso a la plataforma *PGCD* para Terceros de buena fe, la clave pública de la AC ETECSA se puede descargar desde la siguiente URL: https://www.etecsa.cu/servicios/CertificadoACEtecsa

6.. Tamaño de las llaves

El algoritmo utilizado por la AC ETECSA para la firma de los certificados digitales es SHA512 con RSA.

Los tamaños mínimos de llaves RSA, establecidos por la Dirección de Criptografía del MININT, para la PKI son:

	Longitud mínima de las llaves
ACSCC	8192 bits
AC ETECSA	4096 bits
Titulares	2048 bits
SSL y VPN	4096 bits

7.. Parámetros para la generación de llaves públicas y control de calidad

La generación de las llaves y el control de su calidad se realizan por los parámetros establecidos por la Dirección de Criptografía para las llaves RSA.

8.. Propósito de uso de la llave

Los propósitos para el uso de la llave, se establecen en cada certificado en el campo "*Uso de la clave*". Los usos críticos más empleados son: Firma Digital, No repudio, Cifrado de llave, firma de certificados y de CRL.

Los usos críticos extendidos de la llave más utilizados son: Autenticación TLS para Cliente y Servidor Web, Firma de código, Protección de e-mail.

1.2. Protección de la llave privada y controles del módulo criptográfico

1.. Normas y controles para la AC ETECSA

La AC ETECSA se encuentra virtualmente instalada en el centro de datos de la DOPS, y en ella se realiza la instalación de las llaves generadas por la ACSCC.

El centro de datos de ETECSA que brinda el servicio de *hosting* cumple con todos los requerimientos y normas de seguridad, de control de acceso establecidos por la Dirección de Criptografía de MININT; al igual que la virtualización realizada para soportar la PKI de la AC ETECSA cumple con todos los requisitos de criptografía exigidos por la ACSCC.

2.. Control multipersonal de la llave privada

Para el acceso físico a la AC ETECSA y la realización de operaciones sobre esta se requiere la concurrencia de al menos tres (3) funcionarios:

(1) Administrador de la *PGCD*

(2) Administrador de Red

(3) Representante de la Autoridad de Certificación

3.. Custodia de la llave privada

La emisión de una llave privada de cualquier tipo de certificado no se concreta hasta tanto Titular o *Representante* no ingrese la contraseña de protección que se generó durante la etapa de Aprobación de la solicitud por parte de un funcionario ER y que recibió previamente por e-mail. Durante el proceso de creación de las llaves, la *PGCD* se encarga de proteger la integridad de la información con que se construyen. Una vez descargada una llave privada, la AC ETECSA no almacena las llaves privadas emitidas, constituyendo el solicitante del certificado en el único responsable por la custodia del mismo.

4.. Archivo de la llave privada

La copia de respaldo de la llave privada de la AC ETECSA se clasifica como *Secreto* y, por tanto, se almacena en la OCIC de la DOPS. El sobre lacrado que contiene la contraseña para manejar la llave privada también es clasificado como un documento *Secreto* e igualmente se almacena en dicha oficina.

Las llaves privadas entregadas por la Autoridad Raíz para la creación de certificados SSL y VPN se mantienen en el dispositivo de almacenamiento extraíble en que son trasladadas y resguardadas en la OCIC de la DOPS.

1.3. Otros aspectos de la gestión de llaves

1.. Archivo de llave pública

La AC ETECSA mantiene el registro de los certificados emitidos para su consulta y validación de la cadena de confianza. Ambos procesos pueden consultarse desde los servicios propuestos por la Autoridad desde su sitio oficial, además de la disponibilidad del repositorio de las llaves públicas correspondientes a certificados emitidos.

2.. Períodos operacionales del certificado y períodos de uso de las llaves

Los períodos de uso de las llaves están determinados por el tiempo de vigencia del certificado, una vez transcurrido este no se pueden utilizar las llaves. La Dirección de Criptografía del MININT ha establecido los siguientes períodos para el uso de los certificados:

	Tiempo máximo de vigencia del certificado
ACSCC	15 años
AC ETECSA	5 años
Titulares, SSL – VPN	2 años

1.4. Controles de seguridad computacional

1.. Requerimientos técnicos específicos de seguridad computacional

Todo el equipamiento que gestiona certificados digitales tiene instalada protección contra virus y malware, la cual se actualiza diariamente. Además, existen controles de accesos físicos para dispositivos USB, sistemas de protección de la información y análisis de esta.

1.5. Controles técnicos del ciclo de vida

1.. Controles del desarrollo de los sistemas

El software que se utiliza en la AC ETECSA fue desarrollado y cuenta con el mantenimiento de un equipo multidisciplinar de la propia Empresa. La tecnología utilizada es multiplataforma, estandarizada, en correspondencia a la política nacional enfocada a la soberanía tecnológica.

Se utilizan procedimientos de control de cambios para las nuevas versiones y actualizaciones de los componentes tanto criptográficos como generales.

2.. Controles de gestión de seguridad

La AC ETECSA mantiene un inventario de todos los activos que se utilizan en los procesos de registro y gestión de certificados digitales, restringiendo los accesos al BIOS, a los puertos USB y a través de asociaciones IP en el caso de las PC de los funcionarios del PSCC.

3.. Controles de seguridad del ciclo de vida

A lo largo del ciclo de vida del PSCC y sus servicios, los funcionarios se encargan de efectuar controles que garanticen la continuidad de las operaciones. Anualmente se escoge el 2% de los certificados emitidos para verificar su información, se guardan los documentos que declaran a funcionarios de la AC y a los *Representantes* nombrados en sus funciones.

7. PERFILES DE CERTIFICADOS Y LISTAS DE REVOCACIÓN (CRL)

1.1. Perfil del certificado

Los certificados emitidos por la infraestructura de Llave Pública de la República de Cuba se ajustan a las siguientes normas:

- ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection - The Directory: Authentication Framework.
- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.

a) Los certificados emitidos por la AC ETECSA tendrán como mínimo los siguientes campos:

Campo	Valor
Versión	V3
Número de Serie	Valor único (en formato hexadecimal) generado por la Autoridad que emite el certificado
Algoritmo de firma	sha512 RSA
Algoritmo Hash de firma	sha512
Emisor	CN = ETECSA OU = ETECSA O = MINCOM L = Playa ST = La Habana C = CU
Válido desde	Especifica la fecha y hora a partir de la cual el certificado es válido.
Válido hasta	Especifica la fecha y hora a partir de la cual el certificado deja de ser válido.
Sujeto	De acuerdo al tipo de Titular
Clave pública	Se codifica de acuerdo con la RFC 5280. La longitud mínima de la llave es 2048 bits y algoritmo RSA.

b) Para personas

Sujeto	SERIALNUMBER = Número de identidad permanente CN = Nombre(s) y Apellidos OU = Unidad Organizativa O = Organización L = Municipio ST = Provincia C = CU

c) El certificado de la Autoridad de Certificación Intermedia ETECSA es:

Campo	Valor
Versión	v3
Número de Serie	009bff1cac01
Algoritmo de firma	sha512RSA
Algoritmo hash de firma	sha512
Emisor	CN = Autoridad de Certificación Servicio Central Cifrado OU = Autoridad Raíz O = Infraestructura de Llave Pública de la República de Cuba L = Boyeros

	S = La Habana C = CU E = admonpki@mail.mn.co.cu
Válido desde	miércoles, 28 de julio de 2021 11:18:03 GMT
Válido hasta	lunes, 27 de julio de 2026 11:18:03 GMT
Sujeto	CN = ETECSA OU = ETECSA O = MINCOM L = Playa S = La Habana C = CU
Clave pública	RSAEncryption (4096 bit) 30 82 02 0a 02 82 02 01 00 ec 29 82 4f 10 76 c6 94 cf da df 5e 2d 13 46 0f 08 b0 55 d5 b4 c8 d9 7b 4c d4 2d 09 6e 5e 82 be 9f 58 9b 71 21 25 1f 30 c3 f2 d2 9b ae ed 7d af d1 2c 6f 80 cc e6 a9 aa 01 e1 82 67 9c 4c 36 04 17 c8 ef d1 4e 3c 0d c9 2c f7 89 c1 ee 13 94 0c 5b 86 13 6c 07 fc 96 3d c7 e8 c2 71 e2 17 b1 c7 16 12 41 20 2c 71 8d 31 2f 68 4b 70 b2 68 3f 91 b3 5b fb bc 4a 71 c0 48 d5 c6 68 90 3c 66 25 3d 8a ac f9 41 23 90 12 7e ab 4b 3a 84 4b 3c 0e be 9f 99 d4 60 36 18 1e 4b da 75 d1 7a 13 58 a5 73 32 87 32 8d 77 43 7e 80 5c f4 1f ec cb c3 75 00 c9 db 77 5c 07 d5 78 55 fe 3f d8 1e be 90 1c 77 f2 21 69 ca d5 34 00 d7 9f ff f6 2e f8 a4 09 62 67 ea d8 e3 7e 4e 04 f2 97 1e 98 a9 66 d3 3d de 0b 36 20 3d 39 43 cb 1c f8 1b 4c 83 f9 ca 45 6a 95 5c f2 68 10 45 bf 88 e9 a1 ed 39 51 b7 d6 bf f8 6a 52 ce c4 f3 39 ef ee 68 c8 3e 5d b5 16 b2 cb d0 07 6a fc 2d c8 c6 3c eb 2f 5b 2f 6d 2f 32 cf 25 0c b5 ea ae be 53 79 aa f1 3b e8 99 09 af 7b 4c b9 ce 88 ec 5e 46 29 76 28 32 a1 c5 af af 4c 9e 38 5f 08 dc c1 ea ac 01 ae af 6b ad 41 9d 9e cb 7b 07 c5 65 c1 a7 ba e1 f5 1d da b9 73 98 1b 95 f4 3c bd c3 74 fa 6f 48 2a ca 0b 21 ec f7 f9 5b 57 f2 37 24 41 56 b6 86 55 98 74 78 5a 6c dd 32 96 5f 24 ed eb cb 5e 5e 12 00 87 85 5d b3 b3 e6 8e 7c 46 4c 0a b8 5f f0 c4 0e 99 4e 68 9f 34 8f a2 fc 86 2e 1b 56 53 2c 45 ab 8c be a7 c5 5e 77 7b 13 89 49 e3 e9 75 2e 68 a8 90 27 1a 58 66 a9 39 d7 1b 46 ba 46 ca 78 55 2a 23 a3 df 15 98 b3 08 1a 7a 56 cb d5 2c 85 68 29 e7 0b 57 aa 76 11 a3 65 af 6d 52 75 de 48 8c e6 d2 a3 b3 39 1c 0e 7f 1a f4 c5 3d 52 fa 8c 6d f8 b0 df ac f3 02 03 01 00 01
Restricciones básicas	Tipo de asunto=Entidad de certificación (CA) Restricción de longitud de ruta=Ninguno
Identificador de clave del	b31b560cc928a52eec6dcd46555e9b3c5a371f76

Titular	
Identificador de clave de entidad emisora	Id. de clave=0a99a2e67166dde9d26101c3cd17e93c87631e91 Emisor de certificado: Dirección del directorio: CN=Autoridad de Certificación Servicio Central Cifrado OU=Autoridad Raíz O=Infraestructura de Llave Pública de la República de Cuba L=Boyeros S=La Habana C=CU E=admonpki@mail.mn.co.cu Número de serie del certificado=02540be401
Puntos de distribución CRL	Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://certificados.etecsa.cu/getCRL
Comentario de Netscape	Certificado Digital Generado para la Autoridad de Certificación Intermedia: ETECSA
Algoritmo de identificación	sha 1
Huella digital	d0e10dfdc8c68e3eb4db8966d2b365d7dea2f09f

4.. Número de la versión

Todos los certificados emitidos por la AC ETECSA serán X.509 versión 3.

5.. Extensiones de los certificados

Las extensiones de los certificados permiten codificar información adicional en los mismos.

En los certificados emitidos por la AC ETECSA, se utilizarán como mínimo los siguientes campos de las extensiones estándar X.509.

Campo	**Valor**
Uso de la clave	Especifica los usos permitidos de la llave.
Puntos de distribución CRL	Es utilizado para indicar la dirección donde se encuentra publicada la CRL.

6.. Identificador de objeto del algoritmo

El algoritmo criptográfico utilizado por la AC ETECSA es *SHA512 with RSA Encription*.

7.. Formato de Nombres

Es el definido en el numeral 3.1.1 de la presente DPC.

1.2. Perfil de la CRL

Las listas de certificados revocados, emitidas por la AC ETECSA cumplen con la RFC 5280 y contienen los siguientes elementos básicos:

Campo	Valor
Versión	V2
Emisor	CN = Autoridad de Certificación Servicio Central Cifrado OU = Autoridad Raíz O = Infraestructura de Llave Pública de la República de Cuba L = Boyeros S = La Habana C = CU E = admonpki@mail.mn.co.cu
Fecha efectiva	Especifica la fecha de emisión de la CRL.
Próxima actualización	Especifica la fecha en que será publicada la próxima CRL. La frecuencia de emisión es la establecida en el numeral 2.1.3.3 de la presente DPC.
Algoritmo de firma	sha512RSA
Algoritmo hash de firma	sha512
Certificados revocados	Lista de certificados revocados, incluyendo el número de serie y la fecha de revocación.

8.. Número de versión

La AC ETECSA emite las CRL en formato X.509 versión 2.

9.. Extensiones de la CRL

La extensión de la CRL emitida por la AC ETECSA es la siguiente:

Campo	Valor
Número CRL	Número consecutivo

8. ANEXO 1: MANUAL DE OPERACIONES DE AUTORIDAD CERTIFICADORA.

MANUAL DE OPERACIONES

ENTIDAD CERTIFICADORA DE LA AUTORIDAD CERTIFICADORA ETECSA (AC ETECSA-EC)

La Entidad Certificadora (EC) es la encargada de certificar la validez de un certificado digital, aprobado por la Entidad de Registro (ER). Esta parte del PSCC puede emitir, revocar y renovar certificados digitales. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario, servicio de red o canal de comunicación.

Para el trabajo de la AC ETECSA –EC, se definen los siguientes roles:

- Jefe: Director de la Dirección de Seguridad Tecnológica
- Custodio de llave privada: Representante de la AC y el Administrador de Red
- Receptor de permisos de emisión: Esp. A (1) del Grupo de Prevención de Fuga de Información
- Inspector auditor: Jefe del Grupo de Prevención de Fuga de Información
- Administrador de la plataforma: Jefe del Grupo de Prevención de Fuga de Información
- Custodio de material criptográfico: Administrador de Red (responsable de la Máquina Virtual donde se encuentra el software para la PKI) y Representante de la AC (responsable del traslado de este material)
- Aprobación de solicitudes de certificados digitales: Representante de la AC

Acciones a realizar por parte de los Funcionarios EC son:

- Emitir, Revocar y Renovar certificados para Firma Digital, SSL y VPN.
- Listar los tipos de certificados, según sus estados vigentes.

GENERALES

- El servicio de la Autoridad Certificadora ETECSA debe ser realizado por sus Funcionarios todos los días del año.

- Los Funcionarios de la AC tienen la responsabilidad de comprobar los datos insertados en la plataforma con cada solicitud escrita recibida a través de correo electrónico, antes de ejecutar alguna acción. Ante cualquier duda, en el *Dashboard* que aparece al iniciar la sesión se listan los datos de contacto del Representante de una Unidad Organizativa y del Funcionario ER que aprueba sus solicitudes, por si fuera necesario consultarlos.
- La *PGCD* tiene dos (2) modos de operación: uno *Manual*, donde las acciones precitadas las realiza un funcionario; y otro *Automático*, donde inicialmente la acción de emitir se realiza a través de flujos automatizados en la plataforma. Estos modos son configurables desde la interfaz del Administrador de la Plataforma.
- El modo Manual es el comportamiento tradicional donde una persona con los permisos suficientes de acuerdo a su papel dentro del PSCC, elige cada solicitud que reciba y efectúa la acción correspondiente, siempre y cuando esta tenga toda la información exigida.
- El modo Automático elimina a la persona como intermediario y las demoras en tiempos de respuesta en la actividad de emitir un certificado. Este modo no reemplaza a los Funcionarios EC. Las actividades asociadas a la revocación de certificados no pasan por este modo. Para efectuarla se requiere la evaluación y acción humana. Además, se facilita y propicia la capacidad de listar los tipos de certificados, por sus estados, de todas las Unidades Organizativas que se hayan creado en la AC ETECSA.
- De esta forma se pueden obtener estadísticas en tiempo real de cantidad de certificados emitidos, revocados, o renovados; cantidades de solicitudes por tipo, cantidad de Unidades Organizativas, qué certificados están próximos a vencerse, entre otras informaciones.
- Los accesos a la *PGCD* desde las PC de los funcionarios se controlan por listados de IP autorizados, los cuales se solicitan al personal especializado de Soporte, que atiende este tipo de configuraciones. Además, cada vez que sea necesario asignar un rol dentro de esta plataforma, estará precedido de las plantillas correspondientes, firmadas por la máxima autoridad de la Unidad Organizativa solicitante, que designe a dicha persona y corroborado por el Representante de la AC.

- Cada rol de confianza definido para interactuar con las diferentes interfaces de la *PGCD* tiene restringidas las actuaciones según el tipo de actividad que tenga predefinida realizar, mediante reglas establecidas por código fuente y por los flujos de permisos propios del *Frameware* utilizado.

2. Actuación por Roles

Jefe de la Autoridad Certificadora

- Es el máximo responsable de la dirección de la AC ETECSA. Revisa periodicamente, controla y autoriza el accionar de los flujos de trabajo dentro de la Autoridad y sus funcionarios, de acuerdo a las regulaciones legales vigentes en Cuba y a las indicaciones de la Autoridad Raíz.
- Sus permisos están asociados a los de un Funcionario EC, desde donde tiene acceso a toda la información que manejan los Funcionarios de menor jerarquía; y así supervisar sus acciones. También, debe trabajar de conjunto con el Administrador de la plataforma para monitorear las configuraciones que la mantienen funcionando y así poder supervisar el funcionamiento de la Autoridad.

Ningún rol dentro de la plataforma tiene autorización al control total de operación o visualización de los módulos que la componen. Para obtener una panorámica completa del trabajo de la AC, tienen que realizarse mesas de trabajo donde participen varios funcionarios de la AC.

Custodios de llave privada

- El Administrador de la Red y el Representante de la AC son los encargados de establecer el entorno donde se despliega la llave privada con la que se firmarán los certificados emitidos.

Receptor de permisos de emisión

- Esta función está reservada para aquellos especialistas que les sean asignadas las tareas de emisión, revocación y renovación de los certificados digitales solicitados a través de la Plataforma de Gestión de Certificados Digitales. Es decir, funge como Funcionario EC.

- Dentro de sus funciones está conservar las solicitudes de emisión firmadas por el Funcionario ER que las aprueba.

INSPECTOR AUDITOR

- Esta responsabilidad está reservada para el Jefe del Grupo de Prevención de Fuga de Información, como principal evaluador de los procesos en el área. Para ejecutar esta acción debe trabajar de conjunto con el Administrador de la Red, para acceder a los registros del SO de la MV que hospeda la plataforma.
- Se encarga de organizar la revisión bianual de la Declaración de Prácticas de Certificación.

ADMINISTRADOR DE LA PLATAFORMA

- El Jefe del Grupo de Prevención de Fuga de Información es el encargado de establecer el modo de funcionamiento de la Autoridad, la creación de sus nomencladores, el establecimiento de los roles, permisos sobre las unidades organizativas que se vayan incorporando mientras el servicio crece; y, se encarga además de la auditar el proceso de operación de la Autoridad.

CUSTODIO DE MATERIAL CRIPTOGRÁFICO

- Esta función es realizada el Administrador de Red y el Representante de la AC. El primero se ocupa de copiar los materiales criptográficos recogidos por el segundo en las instalaciones de la Autoridad Raíz.

APROBACIÓN DE SOLICITUDES DE CERTIFICADOS DIGITALES

- Esta función está reservada para aquellos especialistas que les sean asignadas las tareas de verificación y *aprobación* de las solicitudes los certificados digitales a través de la Plataforma de Gestión de Certificados Digitales. Es decir, funge como Funcionario ER.
- Dentro de sus funciones está recibir el “Modelo de Nombramiento de Representante” completado por las Unidades Organizativas solicitantes del Servicio y revisarlo de conjunto con el Administrador de la Plataforma, para que este realice la inserción de la tupla Autoridad de Registro – Representante – Funcionario ER correspondiente.

- Además, debe conservar las solicitudes de aprobación firmadas por el Representante de una Unidad Organizativa, firmarlas si están correctas y compartirlas con el Funcionario EC para que puedan ser emitidos los certificados.

3. Eventos en la Plataforma PGCD

A continuación se especifican los pasos a seguir por los Funcionarios EC cuando operen en su sesión de trabajo:

1. Autenticarse en el sistema

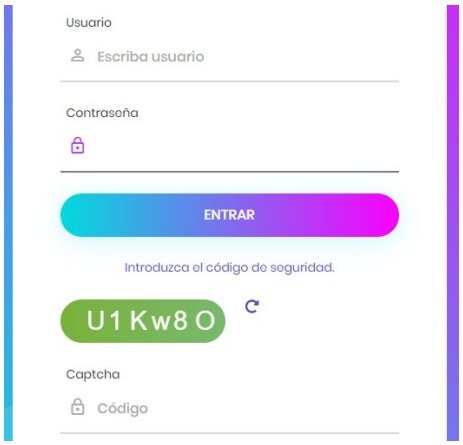

Figure 1..Acceso al sistema.

2. Pantalla principal

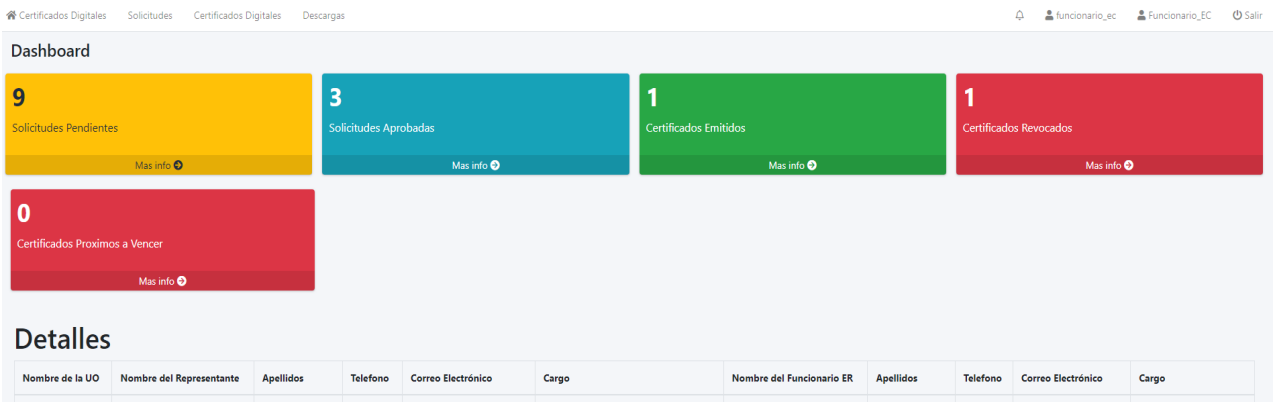

Figure 2..Dashboard general.

2.1 Solicitudes Pendientes

Una vez *Aprobada* la solicitud de un CD por parte del Funcionario ER, el Funcionario EC selecciona el enlace "Más info" de la sección "Solicitudes Pendientes". La interfaz seleccionada muestra los detalles de las solicitudes pendientes, como muestra la siguiente imagen.

Figure 3..Encabezado de solicitudes pendientes, con filtros activos.

En dependencia del *Estado* en que se encuentre una solicitud, serán las *Acciones* que se le asociarán, como la imagen mostrada a continuación.

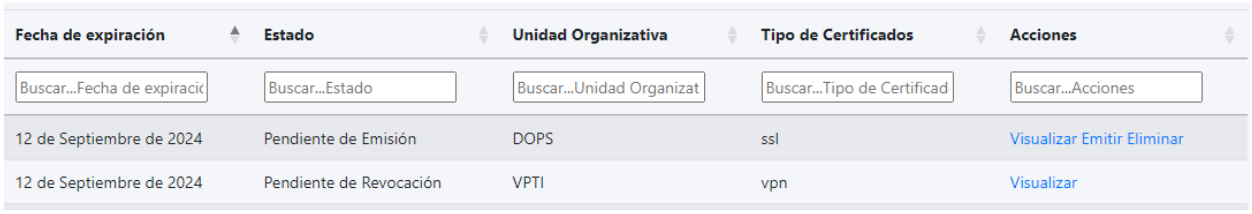

Figure 4..Acciones disponibles según Estado de la solicitud.

Las solicitudes con estado "Pendiente de Emisión" se deben Visualizar y si todo está correcto, Emitir el certificado. Si por el contrario se encuentra alguna irregularidad con los datos requeridos, se puede Eliminar justificando el motivo.

Figure 5..Emitir un certificado.

Las solicitudes con estado “Pendiente de Revocación” se deben Visualizar y si está seleccionado el motivo de revocación, revocar el certificado. De lo contrario consultar con el Funcionario ER que se muestra en el *Dashboard*, para verificar qué motivo originó la solicitud de revocación.

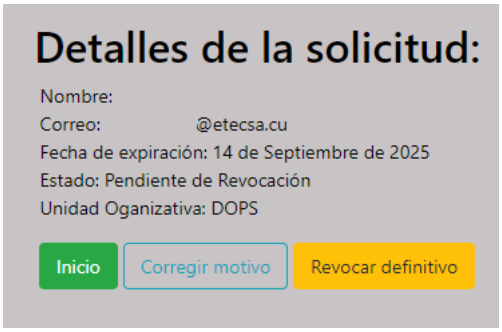

Figure 6..Revocar un certificado.

2.2 Números de Emitidos y Revocados vigentes

Para visualizar los detalles de estos valores es suficiente con acceder al enlace “Más info” de cada una de las siguientes secciones.

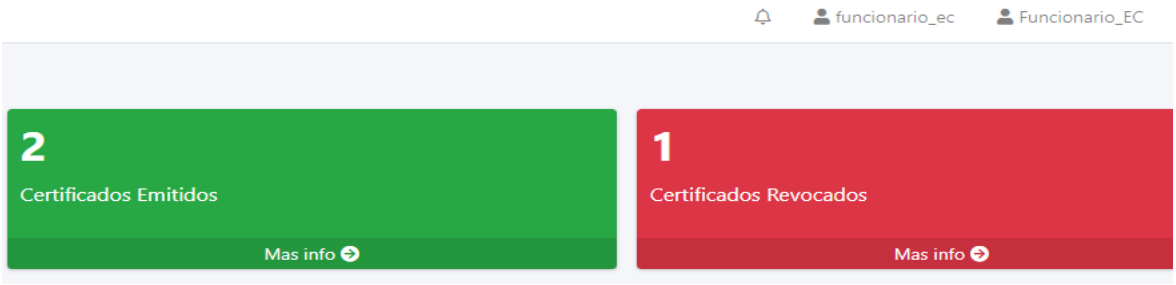

Figure 7..Secciones de Emitidos y Revocados.

3. Compartir Llave pública de la AC

Parte de la responsabilidad de los funcionarios es brindar confianza tanto a Titulares como a terceros, y para cumplir con ello se comparte en la interfaz Dashboard un enlace de descarga de la Llave pública de la AC. Así se puede obtener más rápidamente, en caso de necesitarla para algún tipo de verificación por partes interesadas.

4. Publicación de la CRL y verificación en línea (OCSP)

La CRL se encuentra publicada en:
http://certificados.etecsa.cu/ocsp/crl-download/

La CRL se genera “a demanda”, es decir, cada vez que se solicita se genera un nuevo fichero, aunque no existan nuevos certificados revocados. La validez de la CRL es de 15 días. Para garantizar la confianza de que la Autoridad fue quien la generó, la AC la firma digitalmente.

El OCSP se encuentra publicada en:
http://certificados.etecsa.cu/ocsp/

5. Descarga de llaves por un Titular

Los Titulares a los cuales se les genera uno o varios certificados, encuentran en el enlace *Descargas* el espacio para acceder a sus llaves.

Figure 8..Interfaz de descarga de certificados por un Titular.

6. Flujos de actividades para un Funcionario EC

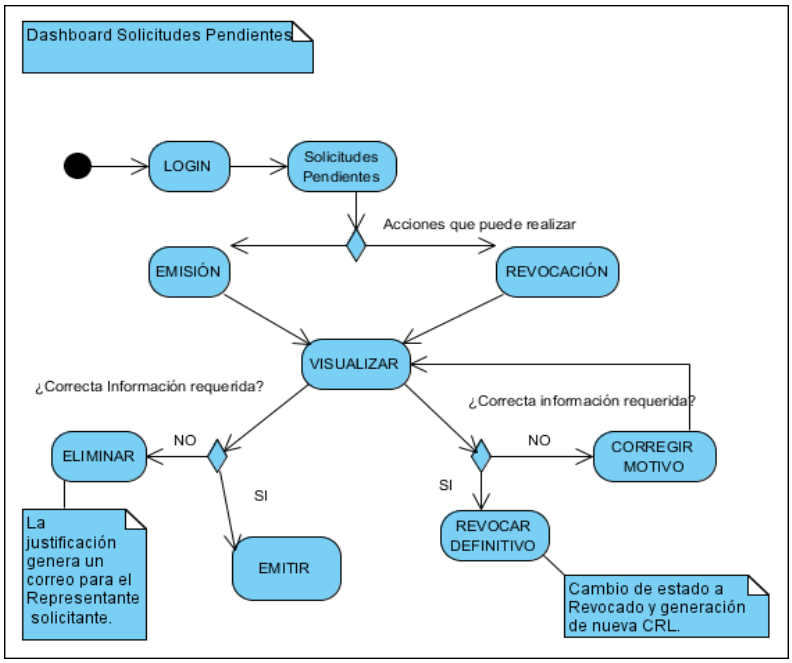

Figure 9..Acciones dentro del dashboard Solicitudes Pendientes.

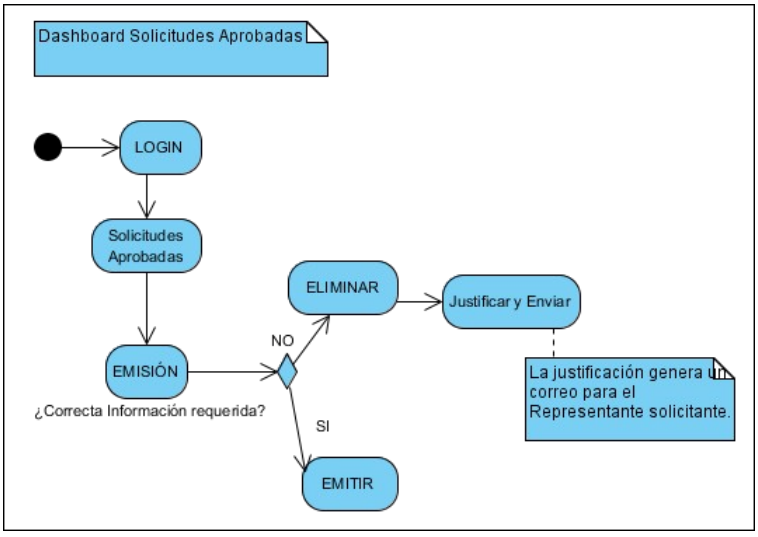

Figure 10..Acciones dentro del dashboard Solicitudes Aprobadas.

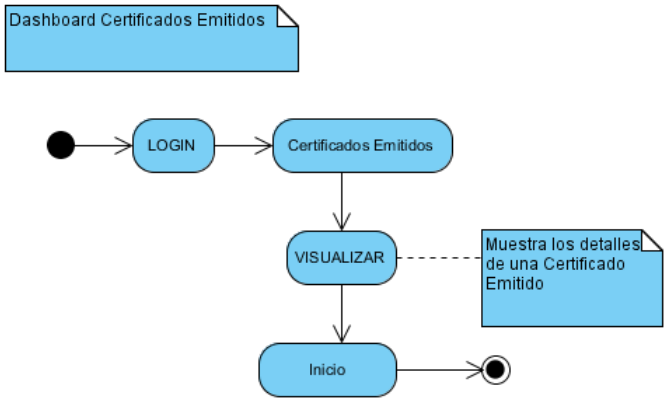

Figure 11..Acciones dentro de Certificados Emitidos.

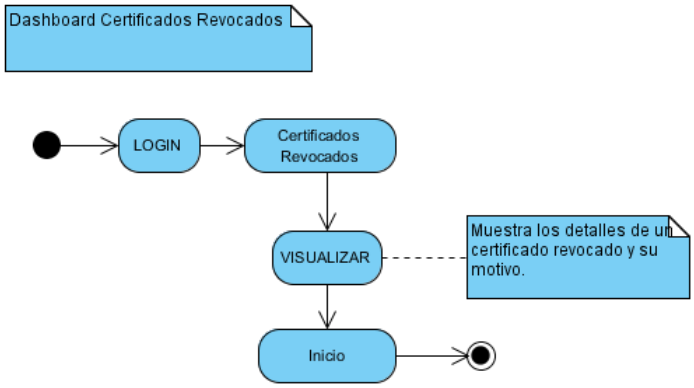

Figure 12..Acciones dentro de Certificados Revocados.

9. ANEXO 2: MANUAL DE OPERACIONES DE LA ENTIDAD DE REGISTRO

MANUAL DE OPERACIONES

ENTIDAD DE REGISTRO DE LA AUTORIDAD DE CERTIFICACION ETECSA (AC ETECSA-ER)

La actuación de la Entidad de Registro es la más importante dentro de un PSCC. Sus **Func*ionarios ER*** son los responsables de verificar la correspondencia entre los datos personales o institucionales reflejados tanto en una solicitud de certificado digital efectuada por un *Representante* de Unidad Organizativa (UO) –en lo adelante *Representante*- mediante el modelo correspondiente y la insertada en la *PGCD*. Esta entidad se encarga de gestionar además las solicitudes de *revocación* y *renovación* de certificados digitales.

Dentro de la AC ETECSA el papel del ***Representante de una Unidad Organizativa*** es tan importante como el del *Funcionario ER*. En su caso, se encarga de verificar los datos de los *Candidatos* que representa, contra C.I. Esta verificación es obligatoria. Además, gestiona las diferentes solicitudes relacionadas a los certificados digitales a través de la *PGCD*, las cuales deben estar en correspondencia con las aprobaciones de la dirección de la Unidad Organizativa que se encuentra representando.

Bajo ningún concepto añadirá datos a la *PGCD* que no hayan sido aprobados o que sean falsos. Ello puede conllevar sanciones administrativas o penales, en dependencia del perjuicio que sus actos provoquen.

El Representante se encarga de intercambiar con el *Funcionario ER* que lo atiende para tramitar dudas, inconformidades; solicitudes de nuevos servicios, capacitación, etc.

De la solicitud de certificado digital para Firma Digital

Una solicitud puede recibirse de dos orígenes diferentes:

1. A través de la *PGCD*, por el *Representante* de los solicitantes de certificados digitales de una Unidad Organizativa determinada.

2. Con la presencia física del solicitante en la oficina donde ejerce la Entidad de Registro, la cual es insertada por el *Funcionario ER* en la *PGCD*. *(fase posterior, de atención a personas naturales)*

Las solicitudes recibidas en la *PGCD*, deben ser atendidas en un periodo de tiempo inferior a las 72 H después de su recepción. *Las solicitudes presenciales se completan en el momento en que se solicitan.*

En ambos casos el *Funcionario ER* debe chequear los datos insertados en cada solicitud para verificar que no existan inconsistencias, aun cuando estos provengan de Bases de Datos generales integradas a dicho sistema (BDUT-ETECSA, Ficha Única del Ciudadano u otras). El criterio de búsqueda fundamental es el C.I.

Si los datos del Candidato verificados tanto en el modelo de solicitud como en la PGCD son correctos, el *Funcionario ER* debe "*Aprobar"* dicha solicitud. La aprobación genera una solicitud de emisión del certificado que se listará como una solicitud "Pendiente de Emisión" en la interfaz del Funcionario EC.

El *Representante* puede comprobar el estado en que se encuentran sus solicitudes, si se encuentran vigentes como certificado válido o se encuentra revocado.

Invalidantes

Si se detecta una irregularidad con los datos ofrecidos en una solicitud o con el *status* del solicitante, el *Funcionario ER* debe rechazar la solicitud eligiendo la opción para eliminarla. Se notificará al *Representante* los motivos del rechazo.

La contraseña que protege la llave privada se generará de forma automática y aleatoria, de acuerdo con flujos operacionales codificados para tal efecto en el núcleo de la *PGCD*, cumpliendo con estructuras de complejidad y seguridad definidas como Buena Práctica en la Empresa, siguiendo las reglas que se dictan a continuación.

Los requerimientos estructurales de la contraseña para proteger un certificado digital, sin importar el tipo, son los siguientes:

1. Frase con una longitud superior a 10 caracteres,
2. Debe contener números, letras y caracteres especiales,

3. Mayúsculas y minúsculas.

DE LA SOLICITUD DE CERTIFICADO DIGITAL PARA SSL/VPN

Este tipo de solicitud se realiza a través de la *PGCD* por el *Representante* de Unidad Organizativa solicitante. Igual que en el flujo anterior, este *Representante* debe enviar por correo electrónico la plantilla de solicitud correspondiente al tipo de certificado digital requerido al Funcionario ER que lo atiende. Este último se encargará de comparar los datos de la plantilla con los insertados en la *PGCD*.

Con esta información el *Funcionario ER* "*Aprueba*" la solicitud. El *Representante* estará informado de los estados de sus solicitudes hasta que se conviertan en certificados emitidos.

Sin embargo, este nivel de información llega hasta ese punto. Los enlaces de descarga de los certificados y sus contraseñas sólo son recibidos por sus Titulares vía correo electrónico. Dicho enlace los conduce a autenticarse en la *PGCD*, creándose una sesión de usuario desde donde puede descargar el o los certificados emitidos a su favor.

La contraseña se genera de forma automática y aleatoria desde la *PGCD*, cumpliendo con estructuras de complejidad y seguridad señaladas para certificados de Firma Digital.

El *Funcionario ER* tendrá a su disposición el listado de los certificados digitales y su estado en que se encuentran en cada momento, permitiendo conocer a qué entidad, *Representante*, servicio o canal de comunicación fueron destinados.

DE LA SOLICITUD DE REVOCACIÓN DE UN CERTIFICADO DIGITAL

La revocación de un certificado digital se lleva a cabo cuando se cumple al menos una de las condiciones listadas en el artículo 32, Res 2/16 emitida por el MININT. Estas son manejadas a través de la *PGCD* y pueden ser solicitadas por el *Representante* o por la propia AC. Cada solicitud de revocación debe especificar el motivo que la respalda, tanto en el modelo que completa el Representante como en los campos de la *PGCD*. Si el motivo no se especifica, no se procederá a revocar el certificado y permanecerá como "*Emitido*".

El *Funcionario ER* no se encargará de "*Aprobar*" las Solicitudes de Revocación. Dichas solicitudes una vez generadas se listarán directamente en la interfaz del

Funcionario EC para ser revocadas. Si el motivo está especificado, podrán pasar a estado *Revocado*.

Tanto el *Funcionario ER* como el *Funcionario EC* pueden acceder al enlace "Certificados Revocados" para visualizar los certificados que ya se encuentren en estado "*Revocado*". Al seleccionar uno, pueden visualizar los detalles del certificado y el "Motivo de la Revocación" que le fue especificado.

El *Representante* recibirá por e-mail la confirmación efectiva de la revocación, una vez realizada por el *Funcionario EC*.

De la solicitud de renovación de un certificado digital

El proceso de *Renovación* de un certificado digital puede realizarse desde la interfaz *PGCD* del *Representante de la UO*.

Si el certificado al que se le solicita renovación aún está vigente, primero debe ser "*Revocado*" por el *Funcionario EC* y seguido de ello, la *PGCD* generará automáticamente una nueva solicitud de un nuevo certificado en la interfaz del *Funcionario ER*. Esta solicitud tendrá los metadatos guardados en la *PGCD*, pero con fechas de vigencia e identificador diferentes.

El *Funcionario ER* percibe en su interfaz que este tipo de solicitud se comporta como un nuevo certificado –en eso consiste, en un nuevo certificado-. Antes de aprobar dicha solicitud debe corroborar el modelo de solicitud recibido por correo electrónico. A partir de ese punto, el comportamiento es el descrito en acápites descritos con anterioridad.

Método de distribución de certificados digitales emitidos

Dentro de la información exigida para completar las solicitudes de certificados digitales se encuentra la tenencia de un correo electrónico, tanto para *Representante*s como para *Candidatos*. Cuando un certificado es emitido, se envía un enlace de descarga únicamente al correo electrónico del Titular.

Igualmente se notifica al *Representante*, como constancia de la terminación satisfactoria del proceso de solicitud.

Equipo de trabajo

Para el trabajo de las AC ETECSA –ER, se definen los siguientes roles:

- Jefes: Jefe del Grupo de Prevención de Fuga de Información
- Atención a usuarios: Especialista (1) del Grupo de Prevención de Fuga de Información
- Verificador: Especialista (2) del Grupo de Prevención de Fuga de Información

CONTROL DEL PERSONAL POR ROLES

El acceso a los módulos dentro de la *PGCD* se asigna por el Administrador de la plataforma, tomando como referencia la Instrucción, Resolución o modelo de nombramiento dictada por el máximo dirigente de la Unidad Organizativa que autoriza tal responsabilidad. En esta se establece el rol que desempeñará el funcionario dentro de la AC ETECSA, garantizándose así el nivel de acceso a las funciones críticas del sistema.

- *Representante*: acceso por canal seguro HTTPS al módulo con permisos para:
  - Insertar solicitudes de los diversos tipos de certificados digitales,
  - Solicitar la revocación y renovación de certificados digitales,
  - Listar los Titulares de su Unidad Organizativa,
- *Funcionario ER*: acceso por canal seguro HTTPS al módulo Entidad de Registro (ER). Tiene permitido:
  - Aprobar solicitudes de nuevos certificados digitales de Firma Digital, SSL o VPN.
  - Visualizar certificados revocados, renovados y emitidos; de tipo Firma Digital, SSL o VPN, que corresponden a las Unidades Organizativas que atiende,
- *Funcionario EC*: acceso por canal seguro HTTPS al módulo Entidad de Certificación (EC). Tiene permitido:
  - Emitir, revocar y renovar certificados digitales. Visualiza el estado de todos los certificados que emite la Autoridad.
- Administrador de la plataforma: acceso por canal seguro HTTPS al módulo Administración que incluye el de Auditoría.

EVENTOS EN LA PLATAFORMA PGCD

A continuación, se especifican los pasos a seguir por los Funcionarios ER cuando operen en su sesión de trabajo:

1. Autenticarse en el sistema

Figure 13..Autenticación en la plataforma.

2. Pantalla principal

Figure 14..Dashboard general

3. Solicitudes Pendientes

El Funcionario ER es el encargado de aprobar las solicitudes de certificados en estado “Pendiente de Aprobación” que le aparecen en la sección “Solicitudes Pendientes”.

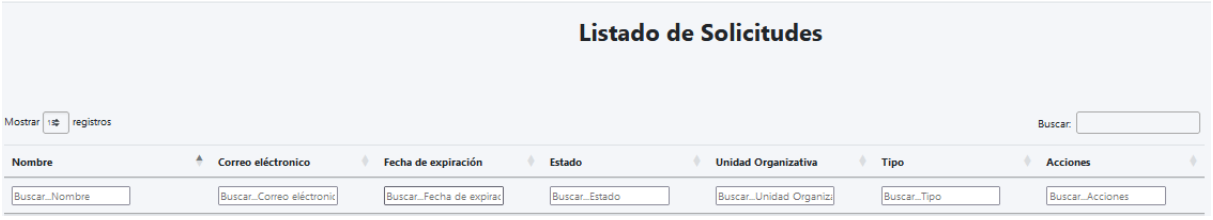

Figure 15..Encabezado de solicitudes pendientes, con filtros activos.

Cada solicitud muestra dos (2) acciones: Aprobar / Eliminar. Al seleccionar Aprobar se muestran los detalles de la solicitud. Si los datos son correctos, se selecciona el botón Aprobar.

Figure 16..Detalles de la aprobación de un certificado digital.

Si existiese alguna incongruencia al verificar esos datos contra el modelo recibido por correo electrónico, se selecciona cancelar para luego escoger Eliminar. La PGCD le solicitará que justifique porqué está eliminándose la solicitud.

Esta justificación llegará vía correo electrónico al Representante para que la corrija.

Figure 17.. Justificación al eliminar una solicitud.

4. Números de solicitudes Aprobadas y certificados Emitidos y Revocados

Para visualizar los detalles de estos valores es suficiente con acceder al enlace "Más info" de cada una de las siguientes secciones.

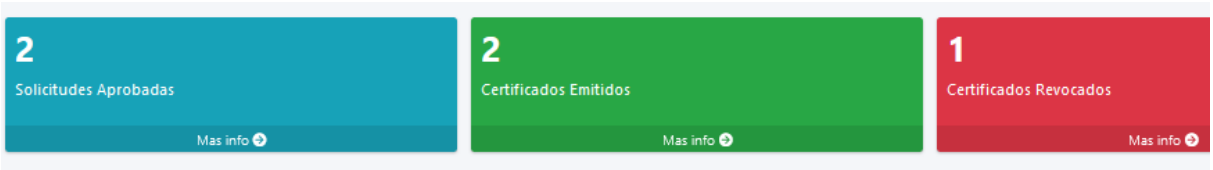

Figure 18.. Listados de solicitudes aprobadas o de certificados: emitidos o revocados de su UO.

10. ANEXO 3: ROLES DE CONFIANZA

Los roles de confianza establecidos para el trabajo con la PGCD de la AC ETECSA son los siguientes:

(1) Usuario Titular:

- Se refiere a la persona que se le emite al menos un certificado digital y con ello se crea una sesión de trabajo en la PGCD, desde donde puede efectuar su descarga segura. No tiene autorización a añadir solicitudes de nuevos certificados, ni revocar o renovar los que se encuentren emitidos a su nombre.

(2) Representante:

- Funcionario seleccionado por la máxima dirección de la Unidad Organizativa solicitante del servicio de Llave Pública de la AC ETECSA con la capacidad de añadir solicitudes de nuevos certificados, revocar o renovar los que se encuentren emitidos en la Unidad Organizativa que representa.

(3) Para el trabajo de la AC ETECSA –ER, se encuentran los usuarios que pueden llegar a aprobar las solicitudes de nuevos certificados digitales:

- Jefe: Jefe del Grupo de Prevención de Fuga de Información
- Atención a usuarios: Especialista (1) del Grupo de Prevención de Fuga de Información
- Verificador: Especialista (2) del Grupo de Prevención de Fuga de Información

(4) Para el trabajo de la AC ETECSA –EC, se encuentran los usuarios que pueden llegar a emitir las solicitudes de nuevos certificados digitales, revocar o renovar los que se encontraban en estado *Emitido*:

- Jefe: Director de la Dirección de Seguridad Tecnológica
- Custodio de llave privada: Representante de la AC y el Administrador de Red
- Receptor de permisos de emisión: Esp. A (1) del Grupo de Prevención de Fuga de Información
- Inspector auditor: Jefe del Grupo de Prevención de Fuga de Información
- Administrador de la plataforma: Jefe del Grupo de Prevención de Fuga de Información
- Custodio de material criptográfico: Administrador de Red (responsable de la Máquina Virtual donde se encuentra el software para la PKI) y Representante de la AC (responsable del traslado de este material)
- Aprobación de solicitudes de certificados digitales: Representante de la AC

Para el trabajo de una ER subordinada a la AC ETECSA, pero perteneciente a un tercero donde media contrato, se sugieren los siguientes funcionarios:

(1) Jefe: Director(a) de Capital Humano.

(2) Representante: Especialistas de la Dirección de Capital Humano en cada una de las Direcciones.

(3) Verificador: Especialista en Seguridad Informática de la Empresa.