DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

AUTORIDAD DE CERTIFICACIÓN INTERMEDIA DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA DE SOFTEL

(Versión 3.0)

12 de abril de 2024
"AÑO 66 DE LA REVOLUCIÓN"

1. INTRODUCCIÓN

SOFTEL, empresa perteneciente al Grupo Empresarial de Informática y Comunicaciones (GEIC) del Ministerio de Comunicaciones (MINCOM) ha detectado la necesidad de garantizar el empleo en el país de certificados digitales como medio de autenticación segura, firma digital, aseguramiento de confidencialidad y habilitación de canales de infocomunicaciones y sitios web seguros, entre otras aplicaciones.

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 firmante. La contribución a la economía nacional está en minimizar las importaciones de insumos de oficina y para equipos de impresión. La sustitución de los documentos impresos por documentos digitales firmados a través de certificados digitales, fortalece la comprobación de la validez de los datos, agiliza la tramitación y procesamiento de la información 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.

El presente documento muestra las principales pautas que regulan el funcionamiento de la Infraestructura de Llave Pública de SOFTEL.

1.1. Presentación.

El objetivo de este documento es describir las prácticas y procedimientos implementados por SOFTEL para brindar Servicios Criptográficos dentro de la empresa y a terceros, con los que comercializa certificados digitales emitidos a través de la plataforma INTEGRO-PKI.

El presente documento será publicado en el sitio web de la Entidad (http://www.softel.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" (versión 2) de la Autoridad de Certificación Intermedia de SOFTEL.

1.3. Participantes de la Infraestructura de Llave Pública.

Estructura general de la Infraestructura de Llave Pública.

La Infraestructura de Llave Pública de SOFTEL, se subordina a la Autoridad Raíz constituida por la Autoridad de Certificación Servicio Central Cifrado.

La Autoridad de Certificación Intermedia de SOFTEL implementa lo pautado en esta Declaración de Prácticas de Certificación hacia lo interno y comercializa y extiende su experiencia a sus clientes, cautivos y potenciales.

A través de esta Infraestructura de Llave Pública se puede establecer y mantener un entorno seguro de registro y gestión de los certificados digitales, tanto para los Administradores de la Autoridad de Registro como para los propios Titulares de certificados, a través del uso del producto INTEGRO-PKI.

Con esta plataforma, dentro de SOFTEL como en los clientes cautivos, se automatiza, se registra, se controla y se gestionan tanto certificados emitidos por usuario como las propias acciones de los responsables de dichas acciones. Se incluyen además los servicios de la Autoridad de Validación que posibilitan la verificación de validez de cada uno de los certificados emitidos, posibilitando el uso de la firma digital, la autenticación de

usuarios y aplicaciones y la protección de canales de comunicación con una amplia gama de aplicaciones.

Autoridades de Certificación.

La Autoridad de Certificación Raíz de la República de Cuba, es la máxima autoridad de la Infraestructura de Llave Pública en el país y es el tope de la cadena de certificación y de confianza entre los participantes en la Infraestructura. Este rol lo asume la Autoridad de Certificación Servicio Central Cifrado.

Las Autoridades de Certificación Intermedias como SOFTEL, están subordinadas a la Autoridad de Certificación Raíz.

La Autoridad de Certificación Intermedia SOFTEL realiza la generación de llaves para firma digital para los suscriptores de SOFTEL y para sus clientes cautivos, a partir del generador de la infraestructura INTEGRO-PKI. Los certificados SSL utilizan esta misma plataforma, pero se generan a partir de los criptomateriales (PEM) entregados por la Autoridad de Certificación Servicio Central Cifrado. La Autoridad de Certificación Intermedia SOFTEL cumple los roles de Autoridad de Certificación y de Registro cuando se trata de la propia entidad, y como Autoridad de Certificación cuando se trata de los clientes contratados.

Su certificado digital es generado por la Autoridad de Certificación Raíz.

Autoridades de Registro.

Son las encargadas de atender y registrar las peticiones para poseer certificados digitales. Realizan la comprobación de la veracidad de los datos del solicitante y envían la solicitud a la Autoridad de Certificación correspondiente para la generación y firma del certificado digital. Pueden funcionar de manera autónoma o formar parte de la Autoridad de Certificación como es el caso de la Infraestructura de Llave Pública de SOFTEL.

Titulares.

Son los Usuarios de Servicios Criptográficos de Certificación, las personas, los dispositivos tecnológicos, las aplicaciones informáticas, etc., que tienen asignado un certificado digital para cumplir las funciones en dependencia de su designación.

Los usuarios o titulares finales son los mismos definidos como titulares, exceptuando a los Prestadores de Servicios Criptográficos de Certificación.

Terceros de buena fe.

Son las personas o entidades (diferentes al titular del certificado) que deciden aceptar y confiar en un certificado de Llave Pública emitido por la Autoridad de Certificación Intermedia de SOFTEL.

1.4. Uso de los certificados.

Los certificados digitales que emite la Infraestructura de Llave Pública de SOFTEL tienen un marcado uso, de acuerdo a la autorización otorgada por la Autoridad Raíz. Se incluyen las firmas digitales para trámites, correspondencias y servicios a la población, el comercio minorista, gobierno e industria local; para el funcionamiento de infraestructuras técnicas no críticas para la seguridad del país y para las informaciones de contenido *no clasificado*. También se tienen en cuenta para garantizar la interacción de las empresas cubanas con entidades homólogas extranjeras y el comercio electrónico internacional.

Estos certificados constituyen la garantía de la protección de la información que se procesa, trasmite o almacena con la utilización de las tecnologías de la información y otros medios electrónicos. Se emitirán de acuerdo con lo normado en los "Requerimientos técnicos, organizativos y de seguridad provisionales para el servicio criptográfico basado en la infraestructura de llave pública"

Uso apropiado de los certificados.

Atendiendo a su uso permitido, los certificados digitales 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.

Prohibición en el uso de los certificados.

Los certificados digitales sólo podrán emplearse de acuerdo a lo establecido en el numeral 1.4.1.

1.5. Detalles del Contacto

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

Esta Declaración de Prácticas de Certificación fue redactada por el grupo creado en SOFTEL con el objetivo de la implantación de la Infraestructura de Llave Pública, bajo la supervisión de la Dirección General de la Empresa y el personal técnico especializado de la Dirección de Criptografía del Ministerio del Interior de la República de Cuba.

Colectivo técnico de contacto.

Todo comentario o sugerencia relativa a esta Declaración de Prácticas de Certificación, puede ser dirigido a la Dirección General de SOFTEL, teléfonos 7 835 8257, o a la dirección de correo integropki@softel.cu.

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 Desarrollo de SOFTEL. Grupo de Tecnología, teléfono: 7 835 8258 o a la dirección de correo integropki@softel.cu.

Procedimiento de aprobación de las Declaraciones de Prácticas de Certificación.

El procedimiento de aprobación de la Declaración de Prácticas de Certificación de la Autoridad de Certificación Intermedia de SOFTEL se elaboró según lo establecido en el acápite 1.5.4 de la Declaración de Prácticas de Certificación de la Autoridad de certificación Raíz de la República de Cuba.

1.6. Definiciones y acrónimos.

Definiciones.

Son las establecidas en los "Requerimientos técnicos, organizativos y de seguridad provisionales para el servicio criptográfico basado en la infraestructura de Llave Pública"

Acrónimos.

AC	Autoridad de Certificación
ACIS	Autoridad de Certificación Intermedia de SOFTEL
ACIS-ER	Entidad Registradora de la Autoridad Intermedia SOFTEL
ACIS-EC	Entidad Certificadora de la Autoridad Intermedia SOFTEL
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
AR	Autoridad de Registro
AV	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
ILP	Infraestructura de Llave Pública
MININT	Ministerio del Interior
OCSP	Protocolo de verificación en línea del estado de los certificados
PIN	Clave personal de acceso
PSCC	Prestador de Servicios Criptográficos de Certificación

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIOS.

1.1. Repositorios.

La ACIS dispone de repositorios donde se publica su certificado firmado por la ACSCC, los certificados emitidos por la ACIS, las CRL, la DPC y sus actualizaciones y otras informaciones relativas a la ACIS y a la ILP de SOFTEL.

Dado el importante número de clientes de diferentes sectores empresariales y/o presupuestados que solicitaron la prestación de los servicios que provee la ACIS, la Dirección de la ACIS, de conjunto con asesores técnicos y comerciales y la aprobación de la ACSCC, se determinó crear Autoridades Intermedias subordinadas a la ACIS. De esta manera se garantizaba mejor

manejo de las solicitudes, mejor control y regulación de los accesos a las plataformas de gestión de certificados por las diferentes entidades, se balanceó la carga de solicitudes asociada a la plataforma raíz y se consiguió ampliar la seguridad de la infraestructura.

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, el servicio se restablecerá en el menor tiempo posible.

1.2. Publicación de información sobre certificación.

Es responsabilidad de la ACIS publicar su certificado digital firmado por la ACSCC, el cual puede ser descargado desde la dirección https://pkisoftel.softel.cu/getCACertificate. Las Autoridades Intermedias subordinadas a la ACIS (aunque están tecnológicamente separadas su certificado de autorización fue emitido por el certificado raíz de la ACIS) cuentan con sus propios puntos de publicación de información sobre certificación:

1. Intermedia para las EES y MIPYMES y para la creación de los SSL: https://pkisoftelint.softel.cu/getCACertificate
2. Intermedia destinada a funcionarios de Oficinas ONAT de todo el país: https://pkionatocc.softel.cu/getCACertificate
3. Intermedia que utiliza la Fiscalía General de la República y la Organización Nacional de Bufetes Colectivos: https://pkijuridica.softel.cu/getCACertificate
4. Intermedia asociada a las empresas del grupo BioCubaFarma: https://pkibiocubafarma.softel.cu/getCACertificate
5. Intermedia que utiliza la empresa ALIMATIC para distribuir los servicios de Llave Pública a las entidades del Ministerio de la Industria Alimentaria: https://pkiminal.softel.cu/getCACertificate

6. Intermedia que utiliza la ONAT para distribuir los servicios de Llave Pública a sus Contribuyentes a nivel nacional:
   https://contribuyenteocc.softel.cu/getCACertificate
7. Intermedia que está planificada para que los Distribuidores Joven Club, Movitel, CEDISAP y GCOM distribuyan los servicios de Llave Pública a sus clientes a nivel nacional:
   https://pkidistribuidores.softel.cu/getCACertificate
8. Intermedia que está hosteada en el CDV de DESOFT destinada a distribuir los servicios de Llave Pública a sus Divisiones Provinciales y a EES, MIPYMES y Personas Naturales a nivel nacional:
   https://srvpki.zoom.cu/getCACertificate

a) Publicar y mantener actualizada los certificados emitidos a cada titular.
b) Publicar y mantener actualizadas las listas de los certificados revocados (CRL), las cuales pueden ser descargadas desde las direcciones URL:
   (1) https://pkisoftel.softel.cu/ank-webfront-public/GetCRL
   (2) https://pkisoftelint.softel.cu/ank-webfront-public/GetCRL
   (3) https://pkionatocc.softel.cu/ank-webfront-public/GetCRL
   (4) https://pkijuridica.softel.cu/ank-webfront-public/GetCRL
   (5) https://pkibiocubafarma.softel.cu/ank-webfront-public/GetCRL
   (6) https://pkiminal.softel.cu/ank-webfront-public/GetCRL
   (7) https://contribuyenteocc.softel.cu/ank-webfront-public/GetCRL
   (8) https://pkidistribuidores.softel.cu/ank-webfront-public/GetCRL
   (9) https://srvpki.zoom.cu/ank-webfront-public/GetCRL

c) Esta dirección se encuentra en los certificados digitales emitidos, especificada en el campo Punto de distribución CRL.

d) Publicar y mantener actualizada la DPC, la llave Pública de ACSCC y la llave Pública de ACIS en el sitio http://www.softel. cu

1.3. Frecuencia de publicación.

Certificado digital de la Autoridad Intermedia SOFTEL.

El certificado firmado por la ACSCC se incluye en el software INTEGRO-PKI y se publicó a partir de una actualización realizada por la ACSCC en 2020. El nuevo certificado tiene un período de validez de ocho (8) años, es decir, está vigente hasta 2028.

Certificados digitales emitidos por la Autoridad Intermedia SOFTEL.

Los certificados digitales emitidos por la ACIS se publicarán después de haber sido firmados, en un término no mayor a las veinticuatro (24) horas.

Lista de los certificados revocados.

Las CRL correspondientes a la ACIS se publican en:

a) https://pkisoftel.softel.cu/ank-webfront-public/GetCRL (1.8)

b) https://pkisoftelint.softel.cu/ank-webfront-public/GetCRL (1.8.1)

c) https://pkionatocc.softel.cu/ank-webfront-public/GetCRL (1.8.2)

d) https://pkijuridica.softel.cu/ank-webfront-public/GetCRL (1.8.3)

e) https://pkibiocubafarma.softel.cu/ank-webfront-public/GetCRL (1.8.4)

f) https://pkiminal.softel.cu/ank-webfront-public/GetCRL (1.8.5)

g) https://contribuyenteocc.softel.cu/ank-webfront-public/GetCRL(1.8.6)

h) https://pkidistribuidores.softel.cu/ank-webfront-public/GetCRL (1.8.7)

i) https://srvpki.zoom.cu/ank-webfront-public/GetCRL (1.8.8)

Cuando se realice un cambio de estado en los certificados emitidos que modifique la anterior CRL, esta se actualizará en un término no mayor a las veinticuatro (24) horas.

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

Declaración de Prácticas de Certificación.

La ACIS realizará cada dos años la revisión de la DPC. Las nuevas versiones de la DPC se publicarán, en forma inmediata, luego de su aprobación por la Dirección de Criptografía.

1.4. Controles de acceso a los repositorios.

El acceso a la información que publica la ACIS sólo permitirá su lectura y/o descarga. La modificación o actualización de la información, queda restringida a los funcionarios de la ACIS que cumplen ese rol.

3. IDENTIFICACIÓN Y AUTENTICACIÓN.

1.1. Nombres.

Tipos de nombres.

La ACIS genera y firma certificados con tipos de nombres acordes al estándar X.509.

Para el certificado ACIS, el nombre distinguido (DN), tanto del titular (subject) como del emisor (issuer), está formado por los siguientes atributos:

- CN = Autoridad de Certificación Intermedia de SOFTEL
- O = Infraestructura de Llave Pública de la República de Cuba
- OU = Autoridad Intermedia
- L = Boyeros
- S = La Habana

- C = CU

Necesidad de que los nombres sean significativos.

La ACIS garantiza que los nombres distinguidos (DN) de los certificados emitidos por ella son significativos, lo que permite establecer la identificación unívoca del titular del certificado y vincular su identidad con la clave pública.

Reglas para la interpretación de los diferentes formatos de nombres.

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

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.

Solución de conflictos relativos a nombres.

La ACIS no actúa como árbitro o mediador, ni resuelve disputa alguna respecto a la titularidad de nombres de personas, con previa verificación de los datos personales necesarios para avalar su identidad. De igual manera, se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

1.2. Validación inicial de identidad.

Autenticación de la identidad de una persona.

La solicitud del certificado se realiza por el propio titular a través de la interfaz pública de INTEGRO-PKI, en cualesquiera sean las Intermedias existentes. En el caso de la ACIS-ER la solicitud es validada en un término de tres (3) días hábiles posteriores a la fecha de la solicitud del certificado.

En el caso de que un cliente cautivo constituya una Autoridad de Registro subordinada a la ACIS, los funcionarios a cargo de la

administración de dicha autoridad deciden en qué momento validan la solicitud realizada por sus titulares.

Información no verificada del titular.

No se aceptará, por parte de la ACIS, información de un titular a ser incluida en el certificado digital, que no pueda ser objeto de verificación.

Validación de Autoridad.

El solicitante que requiera acreditar en su certificado digital, un cargo determinado, deberá presentar, además de los datos personales necesarios para avalar su identidad, la documentación pertinente que acredite el mismo en el órgano, organismo o entidad correspondiente.

Criterios para la Interoperación.

La ACIS funge como autoridad de enlace técnico con la ACSCC y esta a su vez con autoridades raíces de otros países y de organizaciones internacionales, para asegurar la interoperabilidad de los certificados digitales cubanos y de la Infraestructura con sistemas similares del resto del mundo, en las transacciones electrónicas de Cuba con el extranjero, que estén aprobadas por los órganos y organismos de la Administración Central del Estado competentes.

1.3. Identificación y Autenticación de solicitudes de renovación de claves.

La renovación de claves implica la renovación del certificado y por tanto, el registro de los datos del titular así como la emisión de un nuevo certificado digital.

Los procedimientos para la renovación de un certificado se describen en el numeral 4.1.6 de esta DPC.

1.4. Identificación y Autenticación de solicitudes de revocación.

El Director de Capital Humano, en virtud del rol que desempeña dentro de la PKI de SOFTEL como Jefe de ACIS-ER, envía la solicitud de revocación a la ACIS-EC a través de la plataforma INTEGRO-PKI, con la respectiva justificación de por qué se ha solicitado la revocación del certificado. De esta manera se asegura la trazabilidad de los motivos de revocación ante posteriores reclamaciones o auditorías al servicio.

En el caso de las entidades que cuentan con sus ER subordinadas a la ACIS, operan igualmente a través de la plataforma INTEGRO-PKI, de manera tal que la ACIS pueda tener constancia en cualquier instante dentro del contrato comercial con dicha entidad o posterior a este, de las razones de revocación aplicadas en determinado momento a un certificadora digital.

En tal caso, la firma de la solicitud garantiza que la ACIS puede comprobar la autenticidad de la solicitud.

4. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS.

1.1. Solicitud de certificados.

Habilitados para solicitar certificados.

Los titulares de los certificados digitales emitidos por la ACIS-ER o por las ER de los clientes cautivos, a través de la plataforma INTEGRO-PKI, son los trabajadores contratados, respectivamente.

Proceso de solicitud y responsabilidades.

Para realizar la solicitud del certificado, el candidato a titular envía a la ER correspondiente, en formato electrónico mediante la interfaz pública de la plataforma INTEGRO-PKI, la relación de sus datos, necesarios para el llenado de los campos obligatorios establecidos para la emisión del certificado. Tras el proceso de

solicitud, el candidato a titular y el Jefe de la ER reciben un correo electrónico con el reporte del estado de la solicitud.

La protección de la información de los solicitantes está dada por:

- La información de los titulares de certificados viaja por canal seguro HTTPS.
- Los permisos sobre la Infraestructura INTEGRO-PKI se asignan de acuerdo a los roles definidos en el numeral 5.1.2.1 de la presente DPC.
- La solicitud de certificados solo es visible para el Jefe de la ER y otros funcionarios que tengan responsabilidades similares, dentro de la plataforma INTEGRO-PKI.

1.2. Procesamiento de la solicitud del certificado.

Realización de las funciones de identificación y autenticación.

Las funciones de identificación y autenticación se realizan por parte de los roles: Jefe y Verificador de la ER, los cuales han sido acreditados por la máxima dirección de sus entidades y poseen los medios necesarios para la realización de estas tareas.

Una vez recibida la solicitud en la ER, se realiza la comprobación de la identidad de cada candidato a titular.

De existir contradicciones con los datos identificativos presentados de los futuros titulares de certificados, la Entidad de Registro rectifica la solicitud en la interfaz de INTEGRO-PKI correspondiente.

Si todos los datos son correctos, el candidato a titular ingresa un usuario y una contraseña que servirán de protección a dichos datos ante usos indebidos por terceros. Mediante este mecanismo y tras la posterior emisión por la ACIS, solo el titular podrá descargar su llave privada de la plataforma INTEGRO-PKI.

Aprobación o denegación de la solicitud.

Cada ER tiene la función de aprobar o denegar las solicitudes de certificados.

A partir de la recepción de la solicitud de certificado digital, la ACIS-ER tiene un período de tres (3) días hábiles para la ejecución de todo el proceso de aprobación o denegación de la solicitud. En el caso de una ER de cliente cautivo, este puede establecer periodos de aprobación o denegación diferentes.

Las solicitudes de certificación serán rechazadas, cuando estas no cumplan con los requerimientos de información establecidos, cuando no sea posible la verificación de la información brindada por el titular, o cuando se compruebe la no veracidad de la información proporcionada.

En todos los casos, se notificará al titular la denegación de la solicitud y sus causas.

En el caso de aprobación de la solicitud por parte de la ER correspondiente, a través de la plataforma INTEGRO-PKI se envía una solicitud de emisión del certificado digital aprobado al(los) Jefe(s) de la ACIS-EC, con la información necesaria para la emisión del certificado digital. Este proceso es notificado a los involucrados mediante mensajes de correo electrónico, notificándose en cada caso qué tipo de solicitud se está realizando y qué usuario está relacionado.

Plazo para el procesamiento de la solicitud de un certificado.

A partir de la recepción de la solicitud de certificado digital, la ACIS-ER tiene un período de tres (3) días hábiles para la ejecución de todo el proceso de la solicitud de un certificado.

En el caso de una ER de un cliente cautivo, este puede establecer periodos de procesamiento de solicitudes diferentes.

1.3. Emisión del certificado.

Acciones de la Autoridad Intermedia durante la emisión del certificado.

Una vez recibido en la ACIS-EC el permiso de emisión del certificado, esta tiene un plazo no mayor a los tres (3) días, para emitir el CD y publicárselo al titular en formato PKCS #12, a través de la plataforma INTEGRO-PKI.

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 ACIS-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 en la ACIS.

1.4. Aceptación del certificado.

Forma en la que se acepta el certificado.

El contrato firmado entre la ACIS 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 ACIS 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 ACIS entrega a la entidad contratada una copia de esta DPC, para que la utilice como guía de trabajo.

Publicación del certificado.

Una vez generado y firmado el certificado por la ACIS-EC, este se habilita para que sea visualizado por los funcionarios de la ER correspondiente.

El funcionario debe revisar la interfaz de certificados emitidos pasadas las 72 horas convenidas, posterior a la aprobación. Si el CD de un titular ha sido emitido, el funcionario debe solicitarle que se presente en la ER correspondiente con un dispositivo de almacenamiento extraible para recoger la llave privada en formato PKCS #12, la llave pública y la documentación necesaria para: instruirse en la configuración de las aplicaciones recomendadas para ejercer la firma digital de documentos y otros que declaren la responsabilidades y buenas prácticas referidas al certificados digital que ha recibido.

La ACIS-ER destruirá mediante borrado seguro las llaves de los certificados emitidos para firma digital una vez entregada la misma al titular.

Administración de las Llaves de los Titulares.

Los servicios asociados a la administración de las llaves de los titulares suministradas por la ACIS serán gestionados por la plataforma INTEGRO-PKI, aunque en ningún momento SOFTEL guardará las Llaves Privadas.

1.5. Uso del certificado y el par de llaves.

Uso de la llave privada por parte del titular.

El titular, poseedor de un certificado está en la obligación de:

a) Emplear 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.
c) Solicitar inmediatamente, a la ER correspondiente, la revocación o suspensión del certificado, en caso de tener

conocimiento o sospecha del comprometimiento de la seguridad de su llave privada, correspondiente a la llave pública contenida en el certificado, entre otras causas por: pérdida, robo, compromiso potencial, conocimiento por terceros de la clave personal y detección de inexactitudes en la información.

d) Notificar, en un plazo no mayor de las 24 horas, a su dirección superior inmediata, a los funcionarios de seguridad y protección de su órgano, organismo o entidad, así como a la ACIS, cualquier hecho o situación anómala relativa al certificado y que pueda ser considerado como causa de revocación del mismo.

Uso del certificado y la llave pública por el tercero de buena fe.

Los terceros de buena fe sólo pueden depositar su confianza en los certificados 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 ACIS, cualquier hecho o situación anómala relativa a los certificados, así como informaciones o sospechas de comprometimiento o violación de la seguridad del sistema.

1.6. Renovación de un certificado.

Se entiende por renovación de un certificado, el proceso de emisión de un nuevo par de llaves y su certificado correspondiente, para sustituir a uno que haya expirado. Es decir, comenzar el proceso desde el Registro en la plataforma INTEGRO-PKI, con la debida autorización de la dirección de la entidad (sector estatal) de la necesidad de la renovación.

Circunstancias para la renovación de un certificado.

Un certificado es renovado, cuando expira el tiempo de vigencia del mismo y el titular necesita continuar utilizando un certificado digital; o, cuando por determinadas razones el titular olvida la contraseña de manejo del certificado, notifica lo ocurrido, se le revoca el certificado y por sus funciones necesita continuar utilizando un certificado digital.

Personas habilitadas para solicitar la renovación.

Las personas habilitadas para solicitar la renovación, son las mismas que se establecen en el numeral 4.1.1.1 de esta DPC.

Procesamiento de la solicitud del certificado.

El procesamiento se realiza tal como se establece en el numeral 4.1.1.2 de esta DPC.

Conducta constitutiva de la aceptación del certificado.

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

Publicación del certificado renovado.

El certificado renovado será publicado, de inmediato en el repositorio de la ACIS para el acceso de los terceros de buena fe y del titular, siempre que éste autorice su publicación.

1.7. Cambio de clave del certificado.

En la ILP de SOFTEL, no se permite el cambio de clave de un certificado. En caso de que un titular olvide la contraseña de la llave privada o detecte que un tercero la conoce, se aplica el numeral 4.1.9 de la presente DPC.

1.8. Modificación del certificado.

En la ILP de SOFTEL, durante el ciclo de vida de un certificado, no está permitido efectuar modificaciones en ninguno de sus campos. Cuando se requiera realizar la modificación de algún campo, se aplica el numeral 4.1.9 de la presente DPC.

1.9. Suspensión y revocación del certificado.

Circunstancias para la revocación.

Son circunstancias para la revocación de un certificado emitido por la ACIS:

a) Solicitud formulada por el titular del certificado.
b) 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.
c) Resolución judicial o administrativa que lo disponga.
d) 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.
e) Extinción del estatus establecido por el titular, firmante del contrato de emisión y validez del certificado.
f) Alteración de las condiciones de custodia o uso de los datos de creación de la firma digital que estén reflejadas en los certificados expedidos.

Procedimiento de solicitud de la revocación.

Si un funcionario de una ER recibe una solicitud de revocación, por los canales establecidos en su entidad, categorizada como una de las variantes del numeral 4.1.9.1, realiza un dictamen previo en coordinación con los implicados y procede a acceder a la interfaz de los certificados emitidos en la plataforma INTEGRO-PKI, selecciona el titular en cuestión, escribe en el campo Observación la razón de la revocación y solicita la misma. Este proceso se debe realizar en un periodo de tiempo no superior a las (24) horas hábiles posteriores al momento de recepción de la solicitud de revocación.

La ACIS-EC procede a hacerla efectiva de inmediato, una vez que sea de su conocimiento. La ER que efectuó la solicitud de

revocación y también el titular en cuestión reciben una notificación por correo electrónico (de manera automática) con los efectos de la solicitud.

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

La ACIS procesará de manera inmediata cualquier pedido de revocación, una vez que sea de su conocimiento.

Frecuencia de emisión de la CRL.

La ACIS mantiene publicadas las CRL permanentemente en las URL que se listan en el numeral 2.1.3.3 de la presente DPC. La ACIS actualiza la CRL luego de una revocación de certificado en un término no mayor a las veinticuatro (24) horas.

Disponibilidad de la verificación en línea de la revocación.

Toda la información sobre la revocación de los certificados estará disponible en las siguientes URL. Para este propósito se utiliza el protocolo OSCP.

a) https://pkisoftel.softel.cu/Ocsp/HttpOcspServlet (1.8)
b) https://pkisoftelint.softel.cu/Ocsp/HttpOcspServlet (1.8.1)
c) https://pkionatocc.softel.cu/Ocsp/HttpOcspServlet (1.8.2)
d) https://pkijuridica.softel.cu/Ocsp/HttpOcspServlet (1.8.3)
e) https://pkibiocubafarma.softel.cu/Ocsp/HttpOcspServlet (1.8.4)
f) https://pkiminal.softel.cu/Ocsp/HttpOcspServlet (1.8.5)
g) https://contribuyenteocc.softel.cu/Ocsp/HttpOcspServlet (1.8.6)
h) https://pkidistribuidores.softel.cu/Ocsp/HttpOcspServlet (1.8.7)
i) https://srvpki.zoom.cu/Ocsp/HttpOcspServlet (1.8.8)

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

En caso de comprometimiento de la llave privada de la ACIS, ésta revocará todos los certificados emitidos y lo notificará a los

titulares de CD y 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 titulares que tenían certificados vigentes en el momento de producirse el comprometimiento.

Circunstancias para la suspensión de un certificado.

Son circunstancias para la suspensión de un certificado, las mismas que se establecen para la revocación y que aparecen en el numeral 4.1.9.1 de la presente DPC.

Procedimiento para solicitar la suspensión.

La ACIS no contempla dentro de sus procederes como Autoridad la suspensión de un certificado.

Los procedimientos para solicitar la suspensión de un certificado son los mismos que se establecen para la revocación, los cuales aparecen en el numeral 4.1.9.2 de la presente DPC.

Límite del periodo de suspensión.

Se aplica el numeral 4.1.9.2 de esta DPC.

1.10. Servicios de estado del certificado.

Para la validación de los certificados, se proporciona información sobre el estado de los certificados emitidos por la ACIS:

a) Listas de certificados revocados (CRL), las cuales pueden ser descargadas desde las direcciones URL que se listan en el numeral 2.1.3.3.
b) Protocolo de comprobación del estado de un certificado en línea (OSCP), verificables desde las URL listadas en el numeral 4.1.9.5.

Características operacionales.

Cualquier información publicada por la ACIS respecto al estado de los certificados emitidos por ella, es firmada digitalmente por la ACIS.

Disponibilidad del servicio.

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

1.11. 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 4.1.9.1.

1.12. Custodia y recuperación de llaves.

Políticas y prácticas de recuperación de llaves.

En el marco de la ILP de la República de Cuba, ni la ACIS, ni cualquier otro PSCC, almacenarán la llave privada de ningún certificado digital de titular, emitido para firma digital.

5. CONTROLES FÍSICOS Y OPERACIONALES.

1.1. Controles físicos.

Los aspectos referentes a los controles de seguridad física se encuentran recogidos en detalle en el acápite "4.1 Políticas de Seguridad de la Información para la PKI de la empresa", del Plan de Seguridad Informática de la ACIS. En este apartado se van a recoger las medidas adoptadas más relevantes.

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

Ubicación y construcción del local.

La ACIS se encuentra distribuida de (2) maneras. La primera corresponde al perímetro físico de seguridad de la ACIS donde se almacena el conjunto de servidores requeridos para prestar el servicio de validación de los certificados digitales emitidos bajo la plataforma https://pkisoftel.softel.cu.

En ella fueron creados cierta cantidad de certificados, con los que se firmaron documentos de algunos clientes pero fueron revocados posterior al cambio de certificado de Autoridad Intermedia, actualizado por la ACSCC. Esta plataforma continúa brindando servicios de verificación, como establece el Reglamento, y el perímetro de seguridad está en el centro de datos de Softel.

Cuenta con una arquitectura de mampostería, ventanas reforzadas con barrotes y una puerta de entrada al local. Y 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 y en las ventanas.
d) Sistema de alimentación ininterrumpida (en inglés, UPS).

La infraestructura actual de la ACIS bajo la raíz https://pkisoftel.softel.cu se encuentra hospedada en los centro de datos virtual de ETECSA, bajo un contrato de *hosting*.

Acceso físico.

El acceso al centro de datos es restringido al personal autorizado: Directora General, Director de Tecnología, Administrador 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 Directora General o el Director de Tecnología.

Además, el hardware involucrado en la emisión del certificado digital a través de la plataforma INTEGRO-PKI, contiene un disco duro encriptado garantizando con esto que al encender la máquina virtual es necesario desencriptar el volumen de disco duro.

La contraseña del disco duro encriptado, la definió el responsable de seguridad informática y se guardó en sobre lacrado y sellado en el local de la dirección de la empresa.

La contraseña del usuario del sistema (no root), estará compuesta por dos contraseñas de no menos de 6 caracteres complejos, las cuales será definidas por los administradores de la red de SOFTEL de forma independiente y se guardarán en sobres lacrados y acuñados, en el local de la dirección de la empresa. Este usuario una vez autenticado podrá escalar a usuario root usando el comando *sudo*.

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

Alimentación eléctrica y aire acondicionado.

El centro de datos cuentan 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, hasta (2) horas.

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

Almacenamiento de los medios.

La ACIS ha establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información y documentación relativa a la gestión de los certificados, se conservará durante un período mínimo de quince (15) años, en archivos protegidos con técnicas criptográficas de cifrado y control de acceso.

Protección del equipamiento y seguridad del cableado.

El centro de datos dispone de los medios adecuados.

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

b) Sistema de detección contra intrusos en la puerta y en las ventanas.

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

Mantenimiento de los equipos.

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

Seguridad en la reutilización o eliminación de los equipos.

Antes de autorizar la salida de cualquier elemento del equipo que contenga dispositivos de almacenamiento de la ACIS que contengan datos para realizar operaciones de mantenimiento, se procederá a su borrado físico y a su desmagnetización en caso de que se proceda a su eliminación.

Retiro de activos.

Para realizar el retiro de cualquier activo perteneciente a la ACIS se deberá contar con la autorización del Jefe de la ACIS y

el Administrador del Sistema, quienes hacen constar en acta cada activo retirado.

Protección de los activos

El acceso a los activos dentro de la ILP de la ACIS está dado por:

a) Controles de acceso.

b) Acceso al software INTEGRO-PKI por canal seguro *HTTPS*.

c) Sistema *CAPTCHA* integrado al software INTEGRO-PKI.

d) Los roles definidos dentro de la ACIS solo tienen acceso a los recursos que le permita realizar sus funciones en el software INTEGRO-PKI.

1.2. Controles de procedimientos.

Roles de confianza.

Los roles de confianza establecidos para el trabajo de la Autoridad Raíz son los siguientes:

a) Para el trabajo de la ACIS –ER:

- Jefes: Director(a) de Capital Humano.
- Atención a usuarios: Especialistas de la Dirección de Capital Humano en cada una de las Direcciones.
- Verificador: Coincide con el rol anterior.

b) Para el trabajo de la ACIS -EC:

- Jefe: Director (a) General.
- Custodio de llave privada: Dos Administradores de Red y el Responsable de Seguridad Informática.
- Receptor de permisos de emisión: Integrada a la Autoridad de Certificación, en el caso de Softel, Secretaria y asesores de la Dirección General.
- Inspector auditor: Responsable de Seguridad Informática.
- Administrador del Sistema: Jefe del Grupo de Infraestructura.

- Custodio de material criptográfico: Administrador de Red, responsable del local del Nodo donde se encuentra el software para la PKI.
- Generación de certificados digitales: Integrada a la Autoridad de Certificación, en el caso de Softel, el Director(a) General, asesores de la Dirección General y personal especializado del área de Servicios Informáticos, mediante la plataforma INTEGRO-PKI.

Número de personas requeridas por tareas.

Se garantiza el trabajo interrumpido de la ACIS pues la responsabilidad de cada rol es asignada a cuadros y directivos de la empresa que responden los mecanismos de política de cuadros y plazas designadas como es el caso de los Administradores de Red y el Especialista de Seguridad Informática. Se rige por los Decretos 196 y 197 correspondiente a la política de cuadros y lo estipulado en el convenio colectivo de SOFTEL para las plazas por designación.

La relación de personas por Rol queda como sigue:

a) Para el trabajo de las ACIS -ER:
   - Jefe: Una persona.
   - Atención a usuarios: de (1) a (3) Personas.
   - Verificador: de (1) a (3) Personas.

b) Para el trabajo de la ACIS -EC:
   - Jefe: Una Persona.
   - Custodio de llave privada: (3) Personas.
   - Receptor de permisos de emisión: (3) Personas.
   - Inspector auditor: (1) Persona.
   - Administrador del Sistema: (1) Persona.
   - Custodio de material criptográfico: (1) Persona.
   - Generación de certificados digitales: (1) Persona.

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

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

Identificación y autenticación por cada rol.

Cada funcionario posee su propio certificado digital emitido por la ACIS.

Las acciones permitidas para cada rol en la plataforma INTEGRO-PKI son asignadas de acuerdo las funciones que estos realicen.

Roles que requieren separación de funciones.

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

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

Actividades Críticas

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

(1) Crear Autoridades de Registro.

(2) Crear usuario administrador de AC.

(3) Crear usuario administrador de AR.

(4) Solicitar certificado digital.

(5) Aprobación de solicitudes de certificados digital por parte de la AR.

(6) Firma de certificados digitales aprobados por parte de la AC.

(7) Solicitud de revocación de certificados emitidos por una AR.

(8) Revocación de certificados emitidos por la AC.

(9) Asignar roles a los usuarios.

Se les realiza el control, seguimiento y registro a través del software INTEGRO-PKI donde se recogen las trazas correspondientes.

1.3. Controles del personal.

Sanciones por acciones no autorizadas.

Las actuaciones y acciones no autorizadas, por parte de los funcionarios de las autoridades y prestadores de servicios de certificación en la ILP de SOFTEL, y en particular la ACIS, violatorias del régimen de seguridad y de roles especificados para la operación de estas entidades, se califican como hechos sancionables administrativamente, en correspondencia con la legislación vigente.

Documentación suministrada al personal.

La ACIS proporciona a su personal toda la documentación necesaria para el correcto desempeño de sus responsabilidades. Entre la documentación que se entrega se encuentra:

(1) Código de Ética para las TIC.

(2) Declaración de Prácticas de Certificación.

(3) Plan de Seguridad Informática de SOFTEL.

(4) Documentación relativa a las funciones y procedimientos de cada rol.

1.4. Archivo de registros.

Tipos de registros archivados.

La ACIS 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, auditorías y controles procederán y serán registrados como es debido de acuerdo al Manual de Seguridad Informática de SOFTEL.

Período de conservación del archivo.

La ACIS conservará los registros durante un período mínimo de quince (15) años.

Protección del archivo.

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

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

Procedimiento para la copia de seguridad del archivo.

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

Procedimiento para el sellado de tiempo de los registros.

Todos los registros se archivan con información de fecha y hora. La ACIS posee un procedimiento para garantizar la coincidencia de la fecha y hora de los equipamientos con la oficial del país.

Se configuró un Servidor de Estampado de Tiempo (NTP) según la hora de Cuba.

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 SOFTEL para esos fines.

1.5. Cambio de llaves.

El tiempo de validez del certificado de la ACIS es superior al período de validez de los certificados que emite.

Las llaves de la Autoridad Intermedia expiran en el momento que su certificado deja de tener validez. Una vez expirado el certificado, la ACIS solicita a la ACSCC la generación de un nuevo par de llaves y el nuevo certificado digital firmado por ella.

Una vez concluido este proceso, se procede, de forma inmediata, a renovar los certificados de los titulares, de forma tal que todo certificado que se genere en la ILP, luego del cambio de llaves de la ACIS, tenga en su cadena de certificación, el nuevo certificado de la Autoridad Intermedia.

La ACIS continúa emitiendo CRL firmadas con la llave privada original, hasta la fecha de vencimiento del último certificado emitido usando el par de llaves original.

1.6. Recuperación ante el comprometimiento y desastres.

Procedimientos para la gestión de incidentes y comprometimiento.

La ACIS posee un plan contra desastres, 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 los eventos, de forma tal que permita dar continuidad a la prestación de sus servicios esenciales.

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 ACIS detendrá su funcionamiento, informando de inmediato a todos los titulares, y 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 definido por el Administrador de red de la empresa SOFTEL.

Procedimiento ante el comprometimiento de la llave privada.

El plan contra desastres de la ACIS, considera el compromiso o sospecha de comprometimiento de su clave privada como un desastre. Se basa en los procedimientos que con este objetivo tiene definidos SOFTEL, estos son:

(1) Plan de Prevención de Riesgos.

(2) Manual de Procedimientos de Seguridad Informática, que incluye: Plan de Contingencias, Registro y Gestión de Incidencias de Seguridad de la Información de las ACIS, Procedimiento de Salva de Información.

En ese caso se prevé la revocación inmediata de su certificado y la notificación, vía correo electrónico, a todos los titulares para impedir la confianza en el mismo. Igualmente procederá a la revocación del resto de los certificados emitidos.

En un plazo no mayor de 24 horas la ACIS gestionará con la ACSCC la generación de un nuevo para de llaves y un nuevo certificado digital de la Autoridad de Certificación Intermedia.

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.

La ACIS mantendrá en sus repositorios los certificados revocados, incluyendo el suyo, con el objetivo de garantizar la verificación de los certificados emitidos durante el período de funcionamiento.

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

La ACIS tiene previsto en su plan contra desastres, las acciones a realizar ante cualquier evento, para garantizar la continuidad de sus operaciones.

1.7. Cese de las operaciones.

La ACIS en su condición de Autoridad Intermedia en la jerarquía de la ILP de la República de Cuba, podrá cesar sus actividades de servicios de certificación por decisión de la Dirección de SOFTEL debido a condiciones que lo justifiquen.

6. CONTROLES DE SEGURIDAD TÉCNICA

1.1. Generación e instalación del par de llaves.

Generación del par de llaves.

El par de llaves de la ACIS se genera en la ACSCC y se almacena en el módulo criptográfico, el cual cumple los parámetros de seguridad establecidos por la Dirección de Criptografía.

Inclusión del par de llaves en la plataforma INTEGRO-PKI.

Para la inclusión del par de Llaves firmado por la ASCC en INTEGRO-PKI, la contraseña de acceso al software está compuesta por dos contraseñas de no menos de 6 caracteres complejos, las cuales serán definidas por los administradores de la red de SOFTEL de forma independiente y se guardarán en sobres lacrados y acuñados, en el local de la dirección de la empresa.

Se deshabilitó en el BIOS, la torre de CD y los puertos USB.

Se habilitó contraseña en el BIOS, para acceder al SO, la cual se definió por el Responsable de Seguridad Informática de SOFTEL y se guardó en un sobre lacrado y acuñado, en la caja fuerte de la dirección de la empresa.

Durante la inclusión del certificado digital y la pareja de llaves en el sistema de la ACIS, estarán presentes cinco (5) personas:

(1) J. Grupo de Tecnología
(2) J. Grupo de Infraestructura.
(3) Administrador de red
(4) Especialista de la Dirección de Servicios Informáticos.
(5) Responsable de Seguridad informática

Descarga de la llave privada por parte del Jefe de la ACIS-ER.

En el caso de los CD-PFirma, la ACIS genera el par de llaves del titular y es responsable de su resguardo y custodia hasta su descarga por parte del Jefe de la ACIS-ER.

La entrega de la llave privada y el CD-PFirma del titular se realizan por porte del Jefe de la ACIS-ER mediante el uso de un canal seguro *HTTPS*.

Una vez entregados al titular el Jefe de la ACIS-ER es el encargado de eliminar la llave privada del sistema INTEGRO-PKI.

Entrega de la llave pública al titular del certificado.

La clave pública de la ACIS se puede descargar desde la interfaz visual de la plataforma INTEGRO-PKI mediante canal seguro HTTPS. Esta interfaz visual está disponible para los titulares, entidad de certificación y entidades de registro.

Por política de seguridad de la ACIS, no se permite la visibilidad de la plataforma a terceros de buena fe.

Entrega o envío de la clave pública de la autoridad a los terceros de buena fe.

Al encontrarse limitado el acceso a la plataforma INTEGRO-PKI para los terceros de buena fe, la clave pública de la ACIS se puede enviar utilizando la vía de correo electrónico.

Tamaño de las llaves.

El algoritmo utilizado por la ACIS 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 ILP son:

	Longitud mínima de las llaves
ACSCC	8192 bits
ACIS	4096 bits
Titulares finales	2048 bits

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.

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 (keyusage).

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

Normas y controles para la ACIS.

La ACIS se encuentra virtualmente instalada en el centro de datos de ETECSA, 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 ILP de a ACIS cumple con todos los requisitos de criptografía exigidos por la ACSCC.

Control multipersonal de la llave privada.

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

Custodia de la llave privada.

La ACIS almacena las llaves privadas de sus titulares y se responsabiliza con la protección y resguardo de estas hasta la descarga por parte del Jefe de la ACIS-ER de conjunto con el titular acorde al procedimiento establecido por ASCC.

Archivo de la llave privada.

La copia de respaldo de la llave privada de la ACIS se almacena, de manera cifrada, en una caja fuerte con control de acceso en la Dirección General de SOFTEL.

La llave privada de la ACIS se clasifica como SECRETO.

Los dos sobre PIN que contienen partes diferentes de la sucesión aleatoria para la activación de la copia de respaldo de la llave privada, son clasificados como documento SECRETO y se almacenan la caja fuerte, con control de acceso en la Dirección Contable Financiera de SOFTEL.

1.3. Otros aspectos de la gestión de llaves.

Archivo de llave pública.

La ACIS mantiene el registro de los certificados emitidos para su consulta y validación de la cadena de confianza.

Igualmente los mantiene archivados en sus bases de datos internas y en los respaldos que se realizan de las mismas, según procedimiento para esto, contemplado en el Manual de Procedimientos de Seguridad Informática.

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
ACIS	8 años
Titulares	2 años

1.4. Controles de seguridad computacional.

Requerimientos técnicos específicos de seguridad computacional.

La ACIS tiene aprobado su Reglamento de Seguridad Informática, el cual es de estricto cumplimiento para todos sus funcionarios.

Todo el equipamiento posee protección contra virus y malware, la cual se actualiza diariamente. Además existen controles de accesos físicos y lógicos a los mismos.

Todo movimiento de medios es registrado y controlado. Como está definido en el Manual de Procedimientos de Seguridad Informática.

1.5. Controles técnicos del ciclo de vida.

Controles del desarrollo de los sistemas.

Todo el hardware y software que se utiliza en la ACIS, así como sus configuraciones, pasaron una fase de prueba antes de ser puestos en explotación.

Se utilizan procedimientos de control de cambios para las nuevas versiones y actualizaciones de los componentes.

Controles de gestión de seguridad.

La ACIS mantiene un inventario de todos los activos que se utilizan en los procesos de registro y gestión de certificados digitales, y realiza una clasificación de los mismos de acuerdo

con sus necesidades de protección, de forma coherente con los análisis de riesgos efectuados.

Controles de seguridad del ciclo de vida.

Existen controles de seguridad a lo largo de todo el ciclo de vida de los sistemas de la Autoridad Intermedia, que permiten instrumentar y auditar cada fase de los mismos.

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 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 ACIS cumplen con estos requerimientos, como mínimo, tendrán 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 = Autoridad de Certificación de SOFTEL OU = GEIC O = MINCOM L = Boyeros 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 y apellidos OU = Dependencia O = Organismo L = Municipio S = Provincia C = CU

c) El certificado de la Autoridad Intermedia ACIS es:

Campo	**Valor**
Versión	V3
Número de Serie	210000000001
Algoritmo de firma	sha512WithRSAEncryption
Algoritmo hash de firma	sha512WithRSAEncryption
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	Feb 24 15:01:06 2020 GMT

Válido hasta	Feb 25 15:01:06 2028 GMT
Sujeto	CN = Autoridad de Certificación de Softel OU = GEIC O = Ministerio de Comunicaciones L = Boyeros S = La Habana C = CU
Clave pública	rsaEncryption (4096 bit) 9c:39:61:d2:8a:ef:b8:ef:fc:e3:a4:98:2f:76:af:2b:45 :12:4b:67:9e:18:e0:51:4c:02:4f:7a:6e:9b:c3:ac:92: 2e:b9:5a:8e:1d:2e:28:b7:b4:e5:46:ca:dc:28:2a:c 5:00:64:a5:01:0a:94:86:08:97:7b:27:7e:f3:66:ee:0f: 8c:34:0a:c5:f9:c2:ee:01:02:5c:a0:92:8e:8f:3f:80:f0 :4e:6a:37:5a:0f:88:6c:1c:78:15:f6:6a:d3:71:19:e9: 98:8a:4a:3d:40:dd:2e:2f:12:d5:40:41:80:0c:ed:21: cf:20:f8:c2:90:99:d0:bd:3e:41:2c:9b:5b:a7:ab:6a: 24:11:e2:61:c0:78:40:26:16:24:69:3b:ec:12:46:1d: 96:97:6f:8c:09:89:46:46:f4:20:46:be:f8:8a:8c:ec:18 :90:fa:15:e2:96:44:5c:7a:6e:df:39:6f:2a:23:4a:b2: c8:80:09:f8:e6:e0:ca:74:ee:6d:02:63:c0:0d:b1:ab :29:4b:21:4e:3e:59:c5:07:ce:37:24:f0:fd:44:12:7b: 96:69:a3:4e:36:99:d1:bf:f0:76:49:83:5d:00:51:0d:8 6:33:c6:97:a1:0f:00:67:2b:a5:41:b7:7d:07:41:9c:5 a:51:49:67:45:17:ab:7a:43:26:99:22:9f:b4:a0:a4:e b:4c:f6:a3:75:2d:27:02:13:51:1d:69:13:e0:0b:cf:a3 :af:9f:d2:58:12:8f:18:a3:7c:b1:6b:83:30:8f:d1:92:e 7:45:2b:e1:1f:57:d0:8b:9a:87:98:e5:d8:7d:eb:bc: a1:8a:85:71:7e:09:e6:49:0c:6b:3b:3b:63:0a:ee:45 :ac:26:85:b1:0d:10:b3:ad:76:6a:a2:bf:3a:be:a8:e 0:dc:f8:8e:92:c9:88:25:03:35:78:99:78:ad:41:f3:f8: bf:f9:44:71:5f:c7:03:e7:d0:ec:c2:a6:68:4c:6a:bd: 73:36:b6:86:75:c1:a4:78:ba:83:3f:a2:22:7c:95:7a: e9:ce:6f:41:9b:23:83:77:47:24:7e:cd:4f:1e:df:73:e 2:ec:63:92:6c:2b:a9:2b:7e:e6:b9:62:42:9a:ec:2a: 10:9f:9e:30:78:d4:25:34:70:6b:b7:9b:50:0a:79:c4:5 9:c3:39:6c:eb:f1:85:f9:ff:3e:fc:38:ec:e1:2e:71:be: 4a:41:32:9d:6c:f4:a8:30:75:cb:c8:ed:72:b0:7f:d6: a1:4b:21:89:1a:b4:2c:4b:23:fa:8a:20:f9:fd:5d:80:2 5:e5:a6:54:9e:d3:b8:46:3b:17:f8:12:f4:53:46:56:a0

	:69:60:b0:d3:3b:1e:ab:c4:26:d3
Restricciones básicas	Tipo de asunto=Entidad de certificación (CA)
Identificador de clave del titular	68:C0:8E:19:7F:34:BB:D9:B4:3D:9F:A8:F5:20:CC:3B:2E:62:CA:18
Identificador de clave de entidad emisora	Id. de clave= 0A:99:A2:E6:71:66:DD:E9:D2:61:01:C3:CD:17:E9:3C:87:63:1E:91 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
Puntos de distribución CRL	Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=https://pkisoftel.softel.cu/ank-webfront-public/GetCRL
Comentario de Netscape	Certificado Digital Generado para la Autoridad de Certificación Intermedia: Autoridad de Certificación de SOFTEL
Algoritmo de identificación	sha 1
Huella digital	0F:6F:E4:F6:11:54:55:7B:AF:AA:6D:35:04:F4:8C:5C:F5:8F:C3:AF

Número de la versión.

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

Extensiones de los certificados.

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

En los certificados emitidos por la ACIS, 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.

Identificador de objeto del algoritmo.

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

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 ACIS 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 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.

Número de versión.

La ACIS emite las CRL en formato X.509 versión 2.

Extensiones de la CRL.

La extensión de la CRL emitida por la ACIS 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 INTERMEDIA SOFTEL (ACIS-EC)

La entidad certificadora es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

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

- Jefe: Director (a) General.
- Custodio de llave privada: Dos Administradores de Red y el Responsable de Seguridad Informática.
- Receptor de permisos de emisión: Integrada a la Autoridad de Certificación, en el caso de Softel Secretaria y asesores de la Dirección General.
- Inspector auditor: Responsable de Seguridad Informática.
- Administrador del Sistema: Jefe del Grupo de Infraestructura.
- Custodio de material criptográfico: Administrador de Red, responsable del local del Nodo donde se encuentra el software para la PKI.
- Generación de certificados digitales: Integrada a la Autoridad de Certificación, en el caso de Softel, el Director(a) General, asesores de la Dirección General y personal especializado del área de Servicios Informáticos, mediante la plataforma INTEGRO-PKI.

Acciones a realizar por parte del Jefe de la ACIS-EC en la infraestructura INTEGRO-PKI:

- Emitir certificados de usuarios.
- Revocar certificados de usuarios.

A continuación se especifica los pasos a seguir por el Jefe de la ACIS-EC.

1. **Autenticarse en el sistema.**

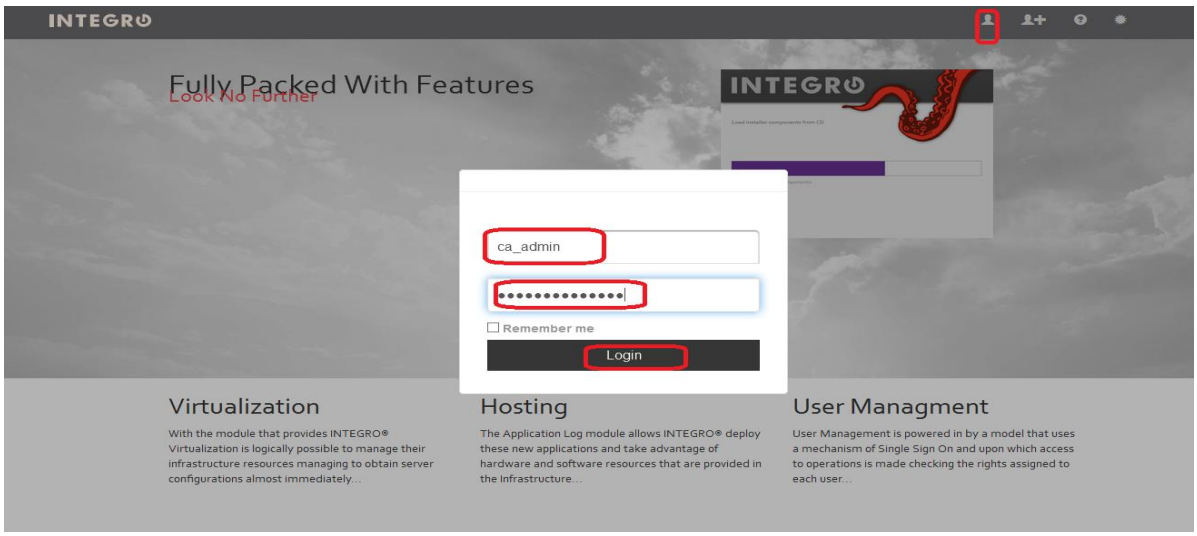

Fig. 1: Acceso al sistema.

2. **Emitir certificados de usuario.**

Una vez aprobada la solicitud de CD por parte del Jefe de la ACIS-ER, el Jefe de la ACIS-EC se autentica en la plataforma INTEGRO-PKI y desde la pestaña ¨*Approved*¨ es el encargado de Emitir el certificado. La generación del par de llaves del titular se realiza en el proceso de emisión del certificado.

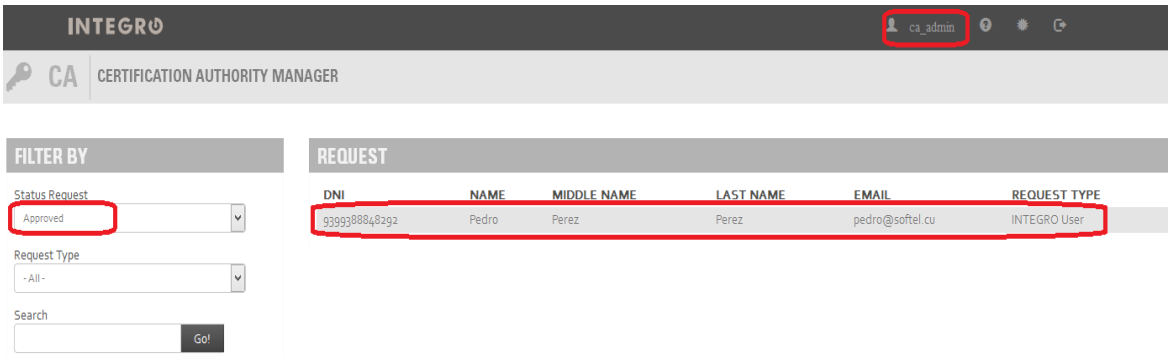

Fig. 2: Emitir certificado de usuario.

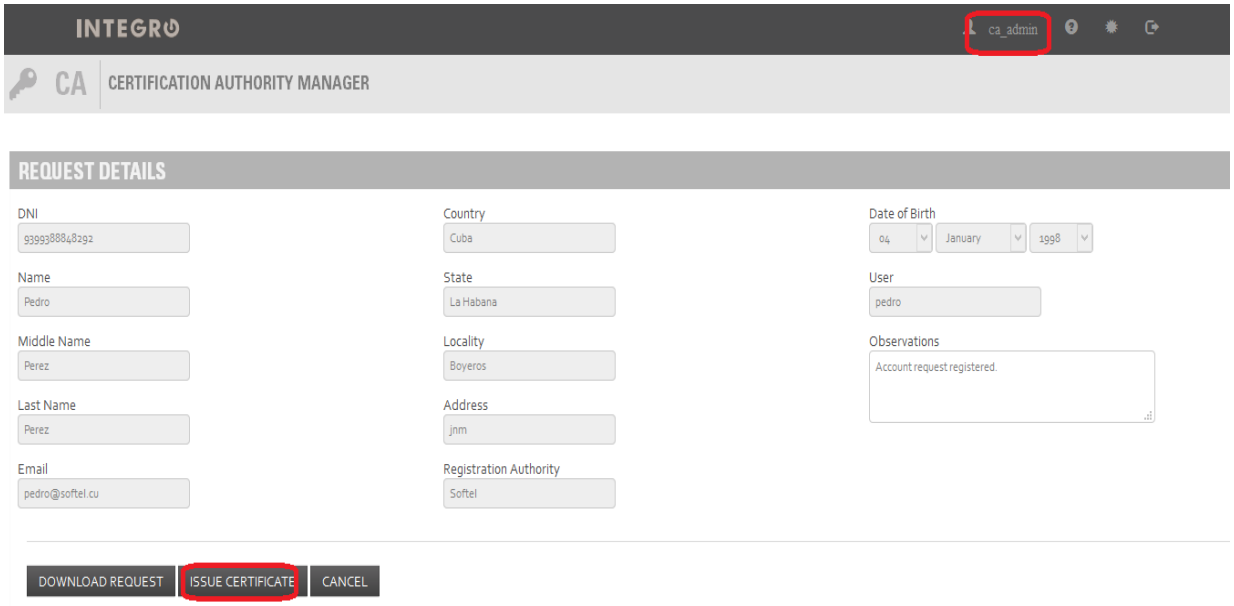

Fig. 3: Emitir certificado de usuario.

Una vez emitido el certificado este pasa al estado ¨With Certificates Issued ¨.

3. **Descargar solicitud de usuario**

El Jefe de la ACIS-EC es el encargado de descargar la solicitud de certificado firmada por el Jefe de la ACIS-ER a la cual se le realizó la solicitud.

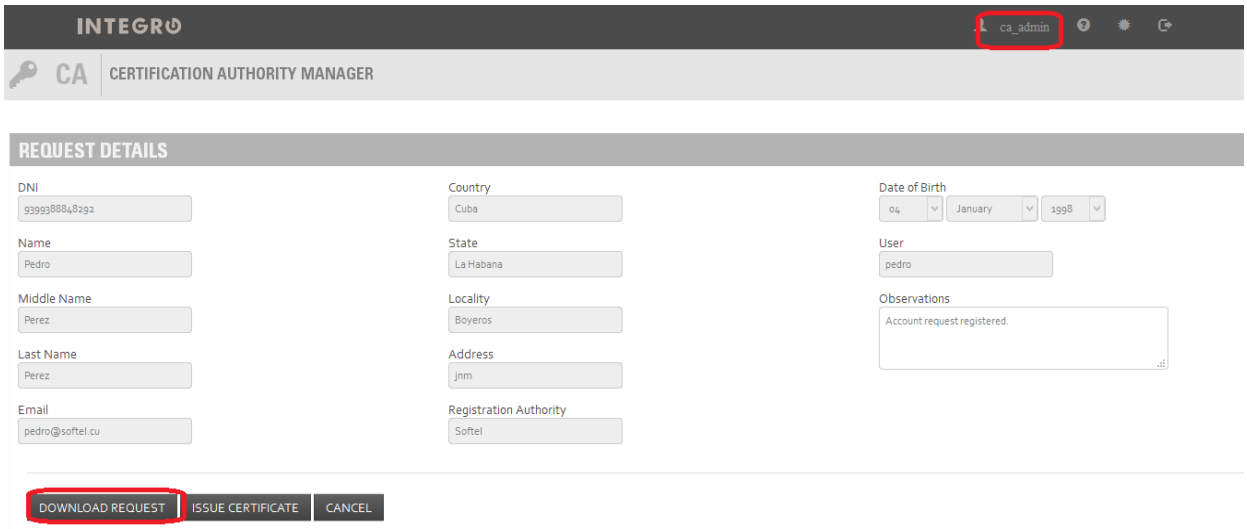

Fig. 4: Descargar solicitud de certificado de usuario.

4. **Revocar certificado de usuario**

Un certificado es revocado por el Jefe de la ACIS-EC desde dos estados: directamente desde certificados con estado ¨With Certificates Issued¨ o si el Jefe de la ACIS-ER solicita la revocación del certificado, el cual pasa al estado ¨With Revocation Request¨.

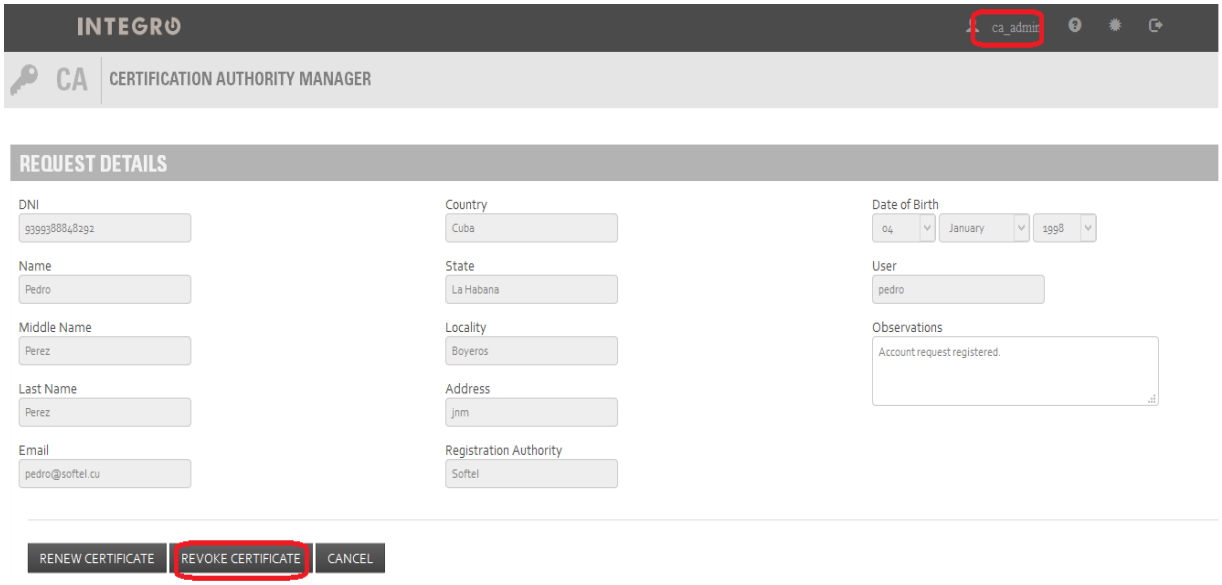

Fig. 5. Revocar certificado de usuario

5. **Publicación de la CRL.**

La CRL se encuentra publicada en:
https://pkisoftel.softel.cu/ank-webfront-public/GetCRL
El sistema realiza la publicación de la CRL siempre y cuando un certificado cambie al estado ¨Revoked¨.

9. ANEXO 1: MANUAL DE OPERACIONES DE AUTORIDAD DE REGISTRO.

MANUAL DE OPERACIONES

ENTIDAD REGISTRADORA DE LA AUTORIDAD INTERMEDIA SOFTEL

(ACIS-ER)

La entidad registradora es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.

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

- Jefes: Director(a) de Capital Humano.
- Atención a usuarios: Especialistas de la Dirección de Capital Humano en cada una de las Direcciones.
- Verificador: Coincide con el rol anterior.

El acceso a los recursos dentro del software INTEGRO-PKI se asigna de acuerdo a los roles definidos para el trabajo de la ACIS, limitándose a los controles de acceso.

- Jefe de la ACIS-ER: acceso por canal seguro HTTPS al módulo PKI, como usuario Jefe de la ACIS-ER.
- Jefe de la ACIS-EC: acceso por canal seguro HTTPS al módulo PKI, como usuario Jefe de la ACIS-EC.
- Administrador del sistema: Acceso por canal seguro HTTPS al módulo CONFIGURACIÓN, como usuario administrador.

Acciones a realizar por parte del Jefe de la ACIS-ER en el software INTEGRO-PKI:

- Aprobar solicitudes de usuario de certificados digitales.
- Solicitar revocación de certificado digital de usuario.
- Descargar certificados digitales de usuario.
- Eliminar la llave privada de los usuarios luego de la descarga de certificado de usuario.

A continuación se especifica los pasos a seguir por el Jefe de la ACIS-ER.

1. Autenticarse en el sistema.

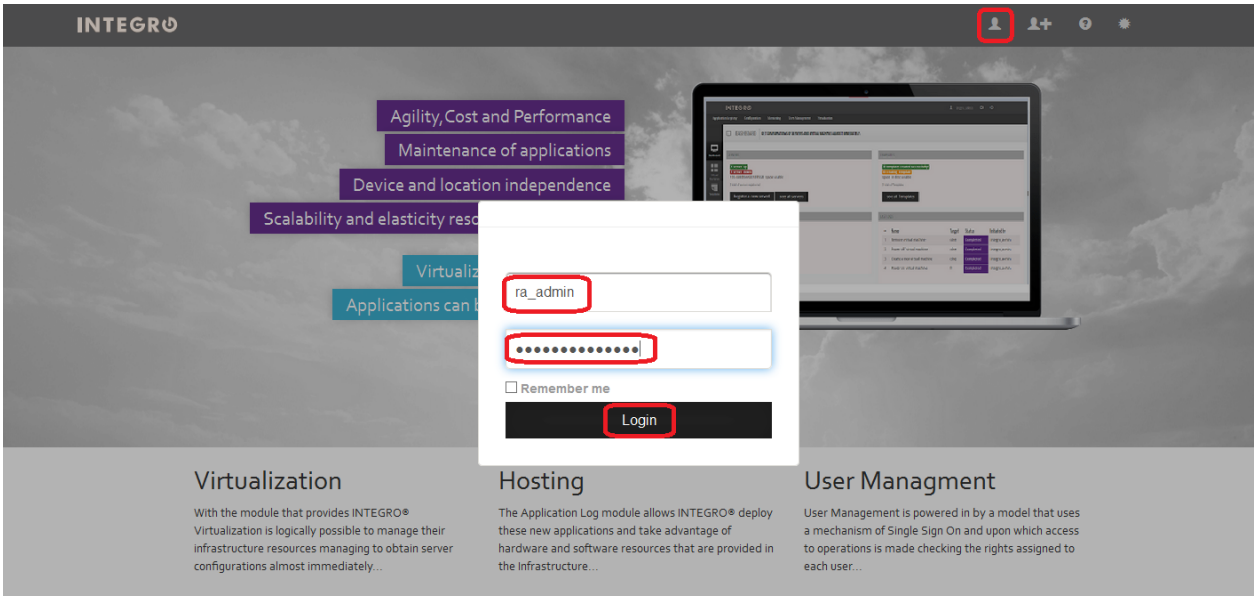

Fig. 1: Acceso al sistema.

2. Aprobar solicitud de certificado digital (CD)

El Jefe de la ACIS-ER es el encargado de aprobar las solicitudes de certificados en estado ¨Awaiting Approval¨. Una vez verificado y aprobados los datos de la solicitud esta pasa al estado ¨Approved¨ en la espera de acciones por parte del Jefe de la ACIS-EC.

En el proceso de aprobar la solicitud de certificado, el usuario final define sus credenciales en el sistema.

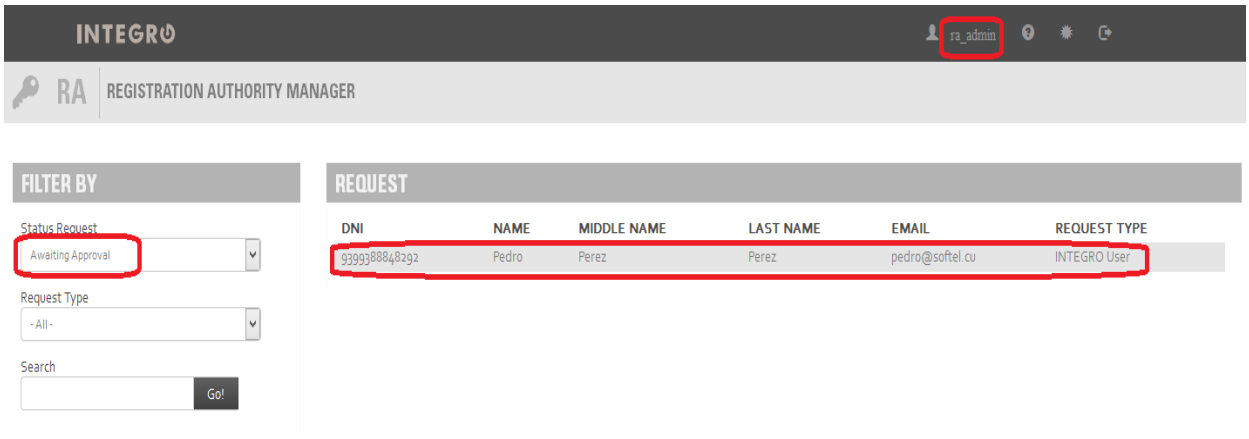

Fig. 2: Aprobar solicitud.

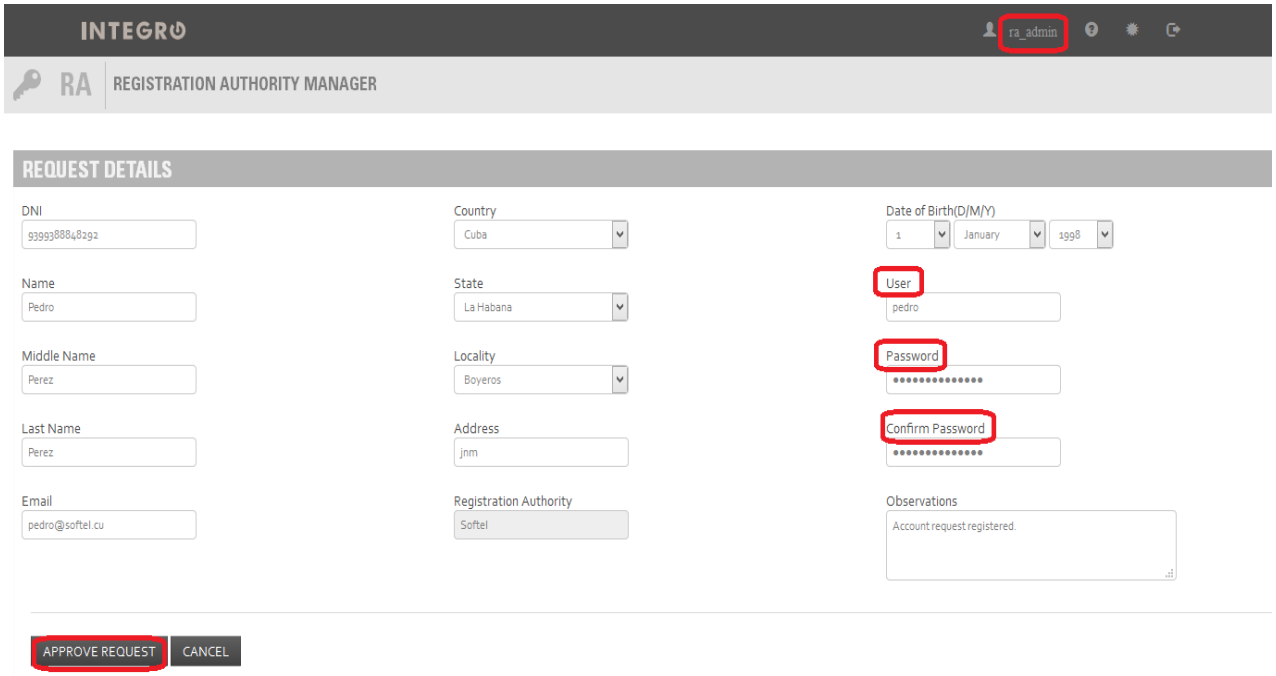

Fig. 3: Aprobar solicitud.

3. Solicitar revocación de un certificado de usuario a un usuario con certificado emitido.

El Jefe de la ACIS-ER es el encargado de solicitar la revocación de un certificado al Jefe de la ACIS-EC. Cuando se realiza esta solicitud de revocación, el certificado pasa del estado ¨With Certificates Issued¨ al estado ¨With Revocation Request¨ a la espera de acciones por parte del Jefe de la ACIS-EC.

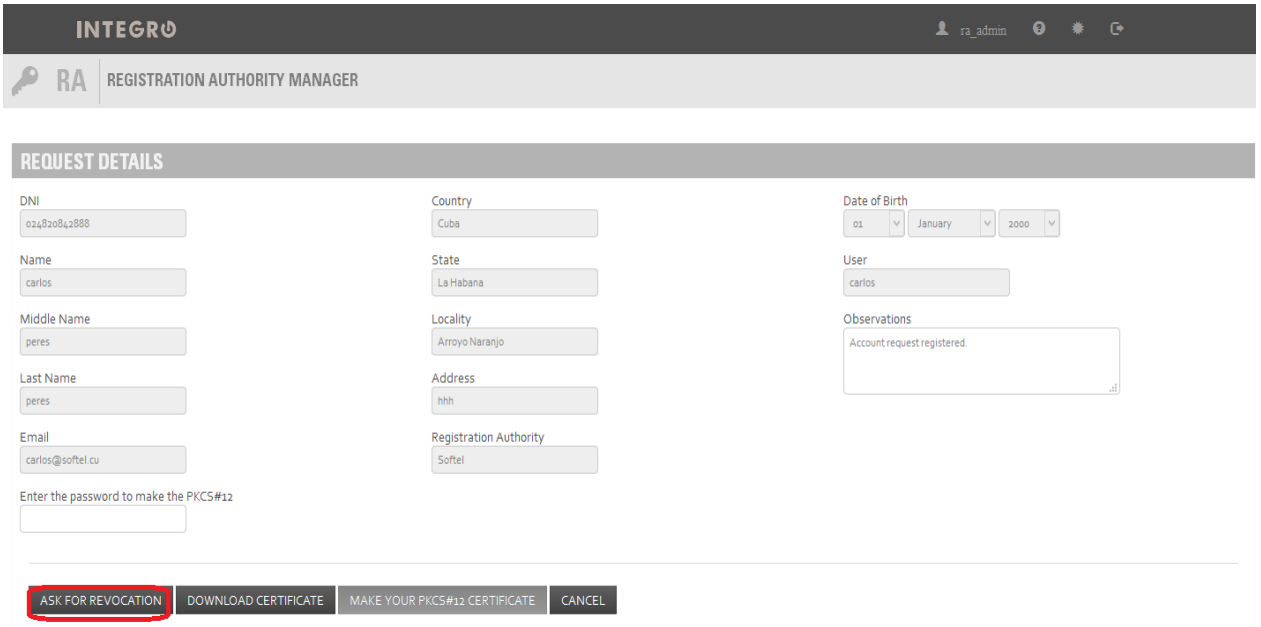

Fig. 4: Solicitar revocación de CD de usuario

El software INTEGRO-PKI permite configurar quien realizará la descarga de los certificados de usuario (certificado.cer o certificado PKSC# 12).

4. Descargar certificados de usuario.

La descarga de los certificados de usuarios se realizará por parte del Jefe de la ACIS-ER, siguiendo los procedimientos de entrega segura de llaves.

4.1 Descargar certificado de usuario (.cer)

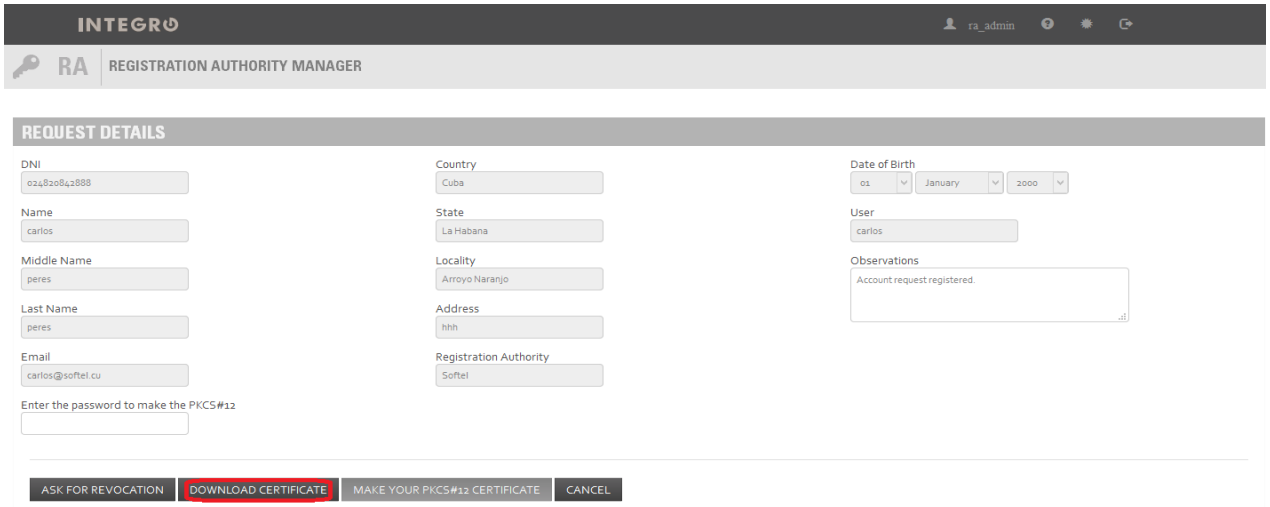

Fig. 5: Descargar CD de usuario (.cer)

4.2 Descargar certificado de usuario (PKSC#12)

Para la descarga del certificado de usuario en formato PKSC#12, el usuario final deberá introducir la contraseña de certificado.

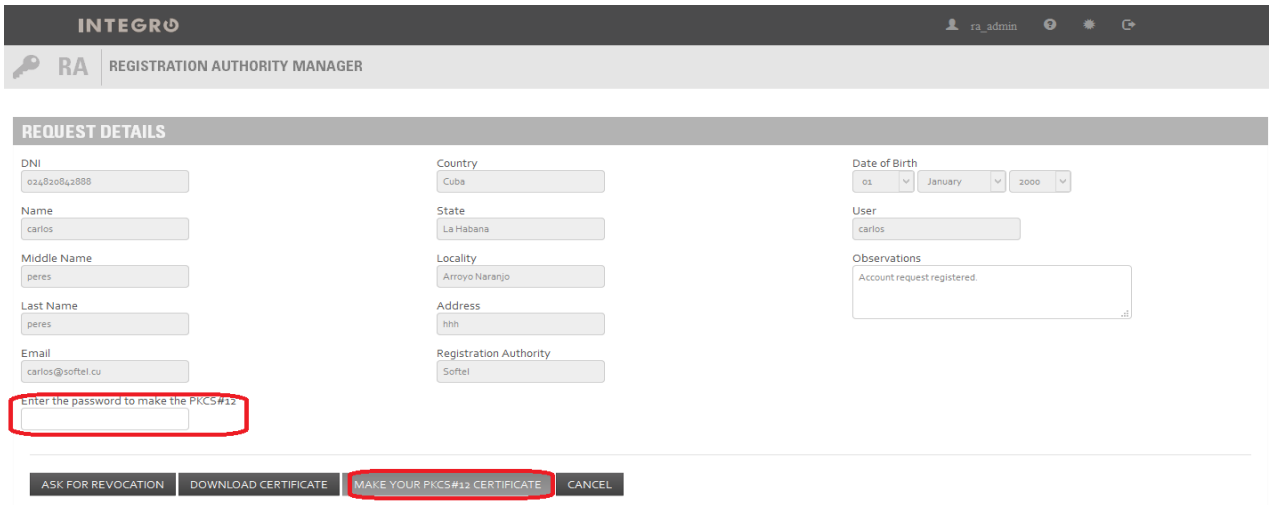

Fig. 6: Datos para generar el certificado PKSC# 12 del usuario.

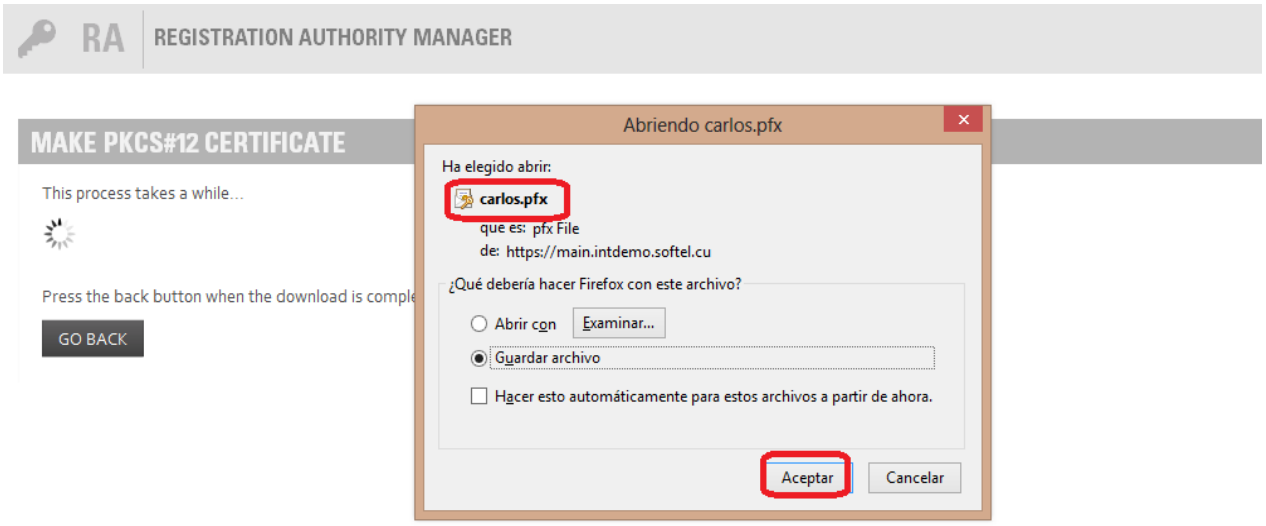

Fig. 7: Descarga de certificado PKSC# 12 de usuario

El jefe de la ACIS-ER entregará al titular sus certificados y los instructivos necesarios para el proceso de firma digital.

5. Eliminar llave privada del usuario.

Una vez descargado el certificado de usuario, el Jefe de la ACIS-ER eliminará la llave privada del usuario en el sistema INTEGRO-PKI.

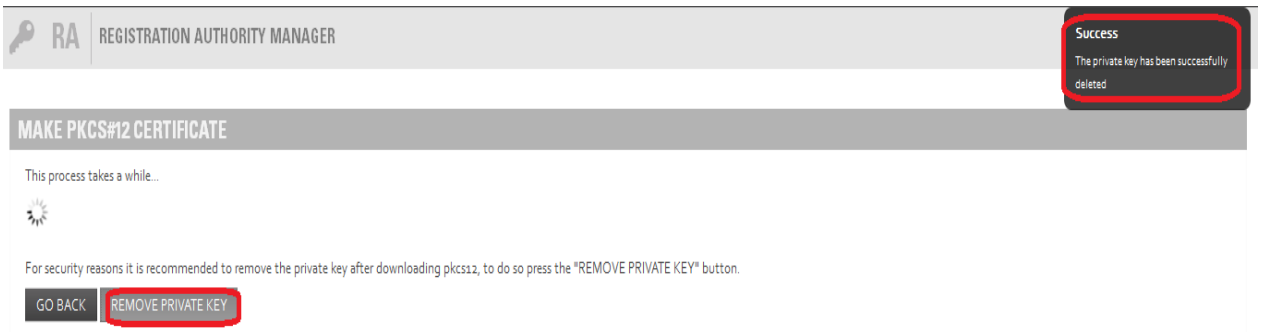

Fig. 8: Eliminar llave privada de usuario.

10. ANEXO 1: ROLES DE CONFIANZA.

Los roles de confianza establecidos para el trabajo de la Autoridad Raíz son los siguientes:

(1) Para el trabajo de las ACIS –ER.

- Jefes: Director(a) de Capital Humano.
- Atención a usuarios: Especialistas de la Dirección de Capital Humano en cada una de las Direcciones.
- Verificador: Coincide con el rol anterior.

(2) Para el trabajo de la ACIS -EC

- Jefe: Director (a) General.
- Custodio de llave privada: Dos Administradores de Red y el Responsable de Seguridad Informática.
- Receptor de permisos de emisión: Integrada a la Autoridad de Certificación, en el caso de Softel Secretaria y asesores de la Dirección General.
- Inspector auditor: Responsable de Seguridad Informática. Chequea y audita el funcionamiento interno de la ACIS de acuerdo a lo establecido en la Declaración de Prácticas de Certificación y el Manual de Procedimiento de la Seguridad de la Información de SOFTEL.
- Administrador del Sistema: Jefe del Grupo de Infraestructura.

- Custodio de material criptográfico: Administrador de Red, responsable del local del Nodo donde se encuentra el software para la PKI.
- Generación de certificados digitales: Integrada a la Autoridad de Certificación, en el caso de Softel, el Director(a) General, asesores de la Dirección General y personal especializado del área de Servicios Informáticos, mediante la plataforma INTEGRO-PKI.