MANUAL DE PROCEDIMIENTOS

Autoridad Certificante

1.- Introducción

Este Manual de Procedimientos forma parte de la documentación técnica emitida por la AC-STJ junto con los siguientes documentos:
· Política de Certificación
· Política de Seguridad
· Manual de Procedimientos de Seguridad
· Plan de Contingencias
· Plan de Cese de Actividades.

2.- Definición de roles

2.1.- Funciones del Director de la ACSTJ

a) Imparte las directivas necesarias para el cumplimiento de las actividades que se detallan en el presente manual y demás documentos que emita.
b) Modifica los procedimientos de acuerdo con las necesidades y dinámica de los cambios funcionales y operativos de las Autoridades Registrantes.
c) Controla el cumplimiento de los objetivos de la ACSTJ.

2.2.- Funciones del Operador Técnico de la AC-STJ

a) Administrar los recursos informáticos que integran la estructura de la AC-STJ.
b) Habilitar la intervención digital del Responsable y del Operador de la Autoridad de Registración y de los procesos de emisión y revocación de certificados
c) Archivar las copias de resguardo generadas por el sistema y la copia del software de la AC-STJ.-
d) Implementar y cumplir los procedimientos de seguridad.

2.3.- Funciones del Responsable de la Autoridad de Registración local y del Operador de la Autoridad de Registración

a) Recibir las solicitudes de nuevos certificados para suscriptores (OAR).
b) Verificar los datos de identidad y de competencia del solicitante (OAR).
c) Aprobar la emisión del certificado solicitado (RAR).
d) Aprobar la revocación de certificados (RAR).
e) Archivar la información respaldatoria (OAR).
f) Ser el depositario de la clave privada de la AC-STJ (RAR).
g) Firmar digitalmente los certificados de los suscriptores (RAR).
h) Firmar digitalmente las listas de certificados revocados (CRLs) (RAR)..

2.4.- En caso de utilizarse un esquema de Autoridades de Registración remotas, según se indica en el apartado 3.2.2, las funciones mencionadas serán cumplidas por el Responsable de la Autoridad de Registración remota.

2.5.- Funciones del Responsable de Seguridad Informática

Las funciones del Responsable de Seguridad Informática se definen en la Política de Seguridad de la ACSTJ y son cumplidos por el operador técnico de la ACSTJ.

2.6.- Designación

Cada uno de los responsables de los roles mencionados será designado por Resolución del Superior Tribunal de Justicia,comunicándose dicho nombramiento a cada una de las partes involucradas. Estas deberán notificarse debidamente, manifestando por escrito su aceptación del cumplimiento de las obligaciones inherentes a su función.

2.7.- Entrega de los dispositivos criptográficos

Al momento de la entrega de los dispositivos criptográficos al Responsable de la Autoridad de Registración, el director de ACSTJ procederá a labrar un acta como respaldo.
El Oficial Certificador y el Responsable de la Autoridad de Registración deben conservar los dispositivos criptográficos bajo su absoluto y exclusivo control, para lo cual cumplirán los procedimientos indicados en el Manual de Procedimientos de Seguridad. El RAR sólo utilizará el dispositivo criptográfico de firma en presencia de otro funcionario designado según lo establecido en el apartado anterior. (OAR u OT).-

2.8.- Funcionarios sustitutos

Los funcionarios designados como sustitutos para cubrir los roles descriptos en el apartado 2 reemplazarán a los responsables mencionados en caso de ausencia temporaria de éstos. El reemplazo continuará hasta tanto el responsable ausente se reintegre a sus actividades o se nombre un nuevo titular. El procedimiento a seguir se encuentra definido en el Plan de Contingencias.

2.9.- Cese de funciones

En caso de renuncia de alguno de los responsables, remoción en su cargo o cambio en el rol asignado, el sustituto designado lo reemplazará en forma permanente. En estos casos el responsable que no continúe con sus actividades debe entregar el dispositivo criptográfico que tenga en su poder al responsable de la ACSTJ. Se procederá asimismo a la destrucción de las claves de activación correspondientes al dispositivo y a su copia de resguardo, a la entrega del dispositivo al nuevo responsable, a la generación de la nueva clave de activación y a la entrega de la copia de resguardo y clave de activación al responsable de su custodia.
Todo lo actuado deberá figurar en un acta que será firmada por los responsables intervinientes y por el responsable de la ACSTJ.
Toda nueva designación para cubrir los roles mencionados en el apartado 2 así como cualquier modificación en los servicios brindados o documentación técnica a utilizar debe ser aprobada por el responsable de la ACSTJ y notificada según lo indicado en el presente apartado.

3.- Solicitud de emisión del certificado

Pueden otorgarse certificados de Firma Digital (CEFIDI) a Magistrados, Funcionarios y personal autorizado, integrantes de otros organismos públicos que lo soliciten, organizaciones o personas que actúen como auxiliares de la justicia o se relacionen administrativamente con ésta, con autorización del STJ.
En todos los casos, el certificado podrá obtenerse directamente mediante tramitación ante el REFIDI o mediante acuerdos con organizaciones u organismos referidos para la conformación de Autoridades de Registración.

3.1.- Iniciación del proceso

Todo solicitante de un certificado en los términos del presente documento debe iniciar el trámite de solicitud ingresando al sitio web de la ACSTJ (http://ca.juschubut.gov.ar). . Debe completar el formulario de solicitud de certificado, incluyendo sus datos identificatorios, generar su propio par de claves y remitir todo el conjunto de datos en formato PKCS#10 a la ACSTJ.
El solicitante obtendrá el valor de la función de hash SHA-1 para la clave pública del requerimiento

de certificado en formato PKCS#10. Este código identificatorio le será pedido para validar su identidad y la integridad de la solicitud ante la ACSTJ.
El procedimiento indicado debe ser cumplido por todos los suscriptores de certificados, independientemente del esquema de identificación utilizado por la ACSTJ según se describe en los apartados siguientes.

3.2.- Validación de la identidad del solicitante

Los procedimientos a utilizar para la identificación de los solicitantes de certificados diferirán en función de los distintos esquemas de registración admitidos por la ACSTJ.

3.2.1.- Registración Centralizada

3.2.1.1.- Verificación de datos por la Autoridad de Registración.

En este caso, el Responsable de la Autoridad de Registración tiene a su cargo la verificación de los datos del suscriptor. Este debe iniciar el pedido de emisión del certificado, ingresando al sitio web de la ACSTJ, completando el formulario de solicitud de certificado, generando su par de claves y remitiendo datos y clave pública a la ACSTJ.
Posteriormente debe presentarse personalmente ante el Responsable de la Autoridad de Registración, o remitir copia de la solicitud firmada por la autoridad responsable del Organismo en que se desempeña. La solicitud contendrá:
a) Nombre y Apellido
b) Nro. de Documento de Identidad (DNI u otro de validez nacional)y su fotocopia certificada.
c) Jurisdicción/Organismo/Dependencia/Cargo
d) Código de identificación del requerimiento.
e) Otros datos que la ACSTJ disponga.
Tanto el RAR o el OAR podrán dar comienzo al trámite para recepción de solicitudes concurriendo a los lugares de trabajo de los solicitantes y haciendo personalmente las verificaciones inciales. Cualesquiera de estos procedimientos se aplicarán a aquellos solicitantes que interactuan con el SAJ en cuanto fuera más adecuado.
El Responsable de la Autoridad de Registración verificará:
a) Que el documento corresponde a la persona que se presentó
b) Que dicha persona es aquella cuyos datos figuran en la nota presentada. A tal fin debe cotejar los datos del documento con los que figuran en la mencionada nota.
c) Que el código de identificación del requerimiento coincide con el cálculo de la función de hash SHA-1 aplicada a la solicitud que será utilizada para la emisión del certificado (ver apartado 4)
El Responsable de la Autoridad de Registración local está facultado para solicitar cualquier tipo de documentación adicional que considere necesaria a efectos de cumplimentar el proceso de identificación.
Efectuada la validación de identidad, el Responsable de la Autoridad de Registración devolverá el documento de identidad al solicitante, inicialará la fotocopia del mismo en prueba de conformidad si no estuviere certificada. Posteriormente, procederá a archivar toda la documentación de respaldo según lo previsto en el apartado 12.
Cumplida la etapa de validación de la identidad del solicitante, el Responsable de la Autoridad de Registración puede:
a) Aprobar la emisión del certificado
b) Suspender el requerimiento, si no se han reunido elementos de juicio suficientes para validar la identidad del solicitante según los procedimientos indicados. En este caso se informará al solicitante acerca de los elementos necesarios para finalizar satisfactoriamente el proceso de validación de su identidad. El solicitante tendrá un plazo de DIEZ (10) días para proveer la información complementaria que se le solicite, vencido el cual deberá reiniciar el proceso de solicitud de emisión del certificado, efectuando un nuevo requerimiento de emisión.
En caso que el proceso de validación de la identidad del solicitante no hubiera finalizado satisfactoriamente, debe dejarse constancia de lo acontecido en un acta que será firmada por el Responsable de la Autoridad de Registración local y el solicitante cuya identidad no se hubiera

podido verificar. En ella se indicará el plazo para la nueva presentación. Se efectuarán dos copias del acta, entregándose un ejemplar al solicitante quien acusará recibo. El otro ejemplar y el acuse de recibo de la copia serán archivados por el Responsable de la Autoridad de Registración local.
Si el proceso de validación de identidad ha sido exitoso, interviene el Oficial Certificador quien procede a verificar el cumplimiento de las distintas instancias del proceso, haciéndolo constar en la documentación recibida. A continuación, se iniciará el proceso de emisión del certificado.

3.2.1.2.- Verificación de datos en área de recursos humanos

a) El Responsable de la Autoridad Registración local, quien validará la identidad del suscriptor, concurriendo directamente al área de Recursos Humanos del organismo, donde hará las verificaciones correspondientes.

3.2.2.- Registración Descentralizada

Previo convenio con el STJ podrá admitirse la existencia de Autoridades de Registración fuera del organismo donde reside la ACSTJ. En tal caso, la Autoridad de Registración que se constituya tendrá a su cargo el proceso de validación personal de la identidad de los suscriptores de certificados que se postulen por su intermedio.
A fin de cumplir con los procedimientos de validación de identidad de los suscriptores, deberá designar un funcionario Responsable de la Autoridad de Registración remota y su correspondiente sustituto. Ambos deben ser designados por Resolución de la máxima autoridad del organismo donde se constituya la Autoridad de Registración, informándose a la ACSTJ de tal nombramiento.
Asimismo, las Autoridades de Registración constituidas en forma remota podrán recibir la colaboración de Auxiliares, quienes asistirán en el proceso de validación de la identidad de los suscriptores de certificados. Los mencionados auxiliares serán designados por Resolución de la máxima autoridad del organismo donde se constituyan.
En caso de constituir Autoridades de Registración en jurisdicción de los Poderes Judiciales provinciales, los respectivos Responsables y sustitutos serán designados por Acordada/Resolución de la Suprema Corte/Superior Tribunal de Justicia/Consejo de la Magistratura/Procuración General o Defensoría o bien por Resolución firmada por la autoridad responsable de la Superintendencia de la jurisdicción. Idéntica modalidad se utilizará para la designación de los auxiliares de los responsables mencionados. Los funcionarios integrantes de los organismos indicados participarán en los procesos de designación según lo establecido en los apartados 3.2.2.1.2 y 3.2.2.3.2.
Los procedimientos de designación de los responsables mencionados y de validación de la identidad de los suscriptores que utilicen el presente esquema de registración son los siguientes:

3.2.2.1.- Procedimiento de acreditación y solicitud del certificado de Firma Digital del Responsable de la Autoridad de Registración Remota (RARR):

El Responsable de la Autoridad de Registración Remota:
a) Ingresa al sitio web de la ACSTJ.
b) Efectúa el requerimiento y genera su par de claves.
c) Obtiene una nota de confirmación de su recepción que incluye:
I. Datos personales
II. Código de identificación del requerimiento
d) La máxima autoridad del organismo deberá asimismo intervenir en el formulario de requerimiento, acreditando de tal forma que el mismo fuera efectuado por el RARR designado. Deberá incluir el código de identificación del requerimiento.
e) Remite a la ACSTJ una nota de aceptación de condiciones y responsabilidades inherentes al cumplimiento de la función de RARR
La designación del Responsable de la Autoridad de Registración Remota, el requierimiento intervenido por el máximo responsable del organismo y la nota de aceptación de condiciones y responsabilidades son remitidas a la ACSTJ.

3.2.2.2. Procedimiento de Emisión del Certificado del RARR por el Director de la ACSTJ:

a) Recibe el nombramiento y las notas de aceptación y de confirmación
b) Verifica su integridad, la coincidencia de los datos indicados en las notas y las firmas.
c) Verifica que el código identificatorio del requerimiento informado en la nota de confirmación coincida con el cálculo de la función de hash SHA-1 aplicada a la solicitud que será utilizada para la emisión del certificado.
d) Si la verificación es exitosa aprueba los atributos del requerimiento, aprobando la emisión del certificado para el RARR.
e) Por último, archiva la documentación de respaldo del proceso de validación de identidad (nombramiento, requerimiento y nota de aceptación).
Firma el nuevo certificado incorporándolo a la lista de Autoridades de Registración habilitadas, informando al RARR de la emisión del certificado a través de un mensaje de correo electrónico firmado digitalmente.

3-2-2-3- Procedimiento de solicitud de certificados ante el RARR

1. Solicitante

a) Ingresa al sitio web de la ACSTJ.
b) Efectúa el requerimiento y genera su par de claves.
c) Envía el requerimiento a la ACSTJ. Obtiene una nota de confirmación de su recepción, que incluye:
I. Nombre y Apellido del solicitante
II. Organismo al que pertenece
III. Cargo
IV. Código de identificación del requerimiento
d) Imprime y firma la nota recibida.
e) Valida su identidad ante el RARR presentando la nota de confirmación firmada y su documento de identidad.

2. Responsable de la Autoridad de Registración Remota

a) Verifica integridad de la nota de confirmación
b) Valida la identidad del solicitante mediante la verificación de su documento de identidad
c) Firma la nota como constancia de verificación de la identidad del solicitante y de la realización del requerimiento
d) Verifica la validez de los datos que figuran en la nota y su correspondencia con los que figuran en la interfaz web, incluyendo el código de identificación del requerimiento
e) Si los controles son exitosos, aprueba la emisión del certificado
f) Informa la aprobación a la AC-STJ a través un correo electrónico firmado digitalmente
g) Archiva la documentación de respaldo del proceso de validación (nota de confirmación y fotocopia de documento de identidad)
El responsable del RARR podrá contar con un auxiliar con las atribuciones y competencias establecidas para el OAR (Punto 2.2.)

3. ACSTJ:

La ARL (Autoridad de Registración Local)
a) Recibe la aprobación emitida por el RARR.
b) Firma el nuevo certificado informando al suscriptor acerca de su emisión a través de un mensaje de correo electrónico firmado digitalmente.
En caso de constituir Autoridades de Registración en jurisdicción de los Poderes Judiciales provinciales, se admitirá la intervención del Secretario del Juzgado a fin de firmar la nota de confirmación como constancia de realización de los controles indicados en 3.2.2.3.2.a y 3.2.2.3.2.b
A continuación, remitirá la nota mencionada al RARR, continuando el proceso de emisión con los procedimientos previstos. Si el solicitante fuera el titular del Juzgado, la nota de confirmación podrá

ser firmada por dicho funcionario, remitiéndola posteriormente al RARR.

4- Emisión del certificado

Una vez finalizado exitosamente el proceso de validación de la identidad del suscriptor según los procedimientos indicados en el apartado 3, se iniciará el proceso de emisión del certificado.
Este comprende los siguientes procedimientos:
a) El Responsable de la Autoridad de Registración local accede al sistema, selecciona el requerimiento de certificado, verifica sus atributos con los que figuran en la nota presentada y controla que su código de identificación coincida con el informado. De ser exitosos los controles, ingresa su dispositivo de firma a fin de firmar la aprobación de la emisión. En caso de intervenir una Autoridad de Registración remota en la validación de la identidad del solicitante, el procedimiento mencionado será efectuado en forma remota por el Responsable de dicha Autoridad de Registración (RARR). De utilizarse el servicio de registración itinerante previsto en el apartado 3-2-1-3-2, el procedimiento mencionado podrá efectuarse en forma remota por el Responsable de la Autoridad de Registración local o el OAR.
b) El RAR ingresa al sistema, verificando la lista de certificados cuya emisión ha sido aprobada y aún no han sido firmados. A continuación habilita la clave privada de la ACSTJ ingresando su dispositivo de firma y procede a firmar los certificados.
c) El solicitante recibirá un mensaje de correo electrónico que le informará acerca de la emisión de su certificado.
d) Por último, se cierran todos los servicios. Se entiende que el solicitante acepta la totalidad de las obligaciones establecidas por la Política de Certificación de la ACSTJ y por este Manual de Procedimientos a partir de la fecha y hora de inicio de validez del certificado emitido. En consecuencia, asume la absoluta y exclusiva responsabilidad por su utilización, y por los daños emergentes que la no observancia de la regulación pudiera implicar.

5- Contenido del certificado

El certificado de clave pública debe contener como mínimo los siguientes datos:
a) Número de versión X.509 del certificado
b) Nombre y apellido del suscriptor del certificado.
c) Localidad, provincia y país de residencia habitual.
d) Dirección de correo electrónico.
e) Clave pública del suscriptor.
f) Algoritmos de firma de la clave pública.
g) Número de serie del certificado.
h) Período de validez del certificado.
i) Nombre de la Autoridad Certificante emisora del certificado.
j) Dirección de consulta de la lista de certificados revocados (CRL).
k) URL donde se encuentra disponible esta Política de Certificación.

6- Revocación del Certificado

6-1- Clases de revocación

6-1-1- Revocación voluntaria:

El suscriptor de un certificado puede solicitar su revocación por cualquier motivo y en cualquier momento, para lo cual debe comunicarlo a la ACSTJ siguiendo el procedimiento que establece este manual.

6-1-2- Revocación obligatoria:

Un suscriptor debe obligatoriamente pedir la revocación de su certificado cuando:
a) Se produzcan cambios en la información que el certificado contiene o ésta se desactualice.

b) La clave privada asociada al certificado de clave pública, o el medio en que se encuentre almacenada se encuentren comprometidos o corran peligro de estarlo.
c) Se produzca el cese de su relación laboral con el organismo, dependencia o institución, sin perjuicio de la obligación que le corresponde al responsable del área de Recursos Humanos del organismo donde desempeña sus funciones.
La ACSTJ debe obligatoriamente revocar el certificado de un suscriptor en las siguientes situaciones:
a) A solicitud del suscriptor cuando se verifiquen los procedimientos de recepción y validación establecidos en los apartados 6.3.1 y 6.3.2 de este manual.
b) A solicitud del responsable del área de recursos humanos o de la máxima autoridad del organismo o dependencia cuando se verifiquen los procedimientos de recepción y validación establecidos en los apartados 6.3.1 y 6.3.2 de este manual.
c) Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en la ley 25506 y normativa reglamentaria, por la Política de Certificación de la ACSTJ, por este Manual de Procedimientos o cualquier otro acuerdo, regulación o ley aplicable al certificado.
d) Si toma conocimiento que existe sospecha que la clave privada del suscriptor se encuentra comprometida.
e) Si la ACSTJ determina que el certificado no fue emitido de acuerdo a los lineamientos de la ley 25506 y normativa reglamentaria, de la Política de Certificación, de este Manual de Procedimientos o de los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional.
En caso que el suscriptor cese en su vinculación laboral, el responsable del área de Recursos Humanos del organismo, dependencia o institución donde se desempeñara, o en su caso, el funcionario que administre el registro de personal, está obligado a informar de inmediato a la ACSTJ acerca de tal situación, a fin de efectuar la correspondiente revocación.

6-2- Autorizados a pedir revocación

Sólo pueden pedir la revocación de un certificado:
a) El suscriptor, si se da alguno de los supuestos de revocación indicados en el apartado 6-1-2.
b) La máxima autoridad del organismo o dependencia donde se desempeñe el suscriptor o bien el responsable del área de Recursos Humanos o el funcionario que administre el registro de personal.

6-3- Revocación a solicitud del suscriptor o de funcionario autorizado

6-3-1- Recepción e identificación

Producida una causa de revocación del certificado, el suscriptor del certificado, o bien alguno de los responsables indicados en el apartado 6-2-b deben comunicarlo a la ACSTJ.
Son aceptados los pedidos de revocación que se efectúen por los siguientes medios:
a) A través del sitio web de la ACSTJ.
b) Por correo electrónico firmado digitalmente por el suscriptor, el responsable del área de Recursos Humanos o la máxima autoridad del organismo o dependencia donde aquel desempeñe sus funciones. El texto del mensaje debe incluir los datos personales del suscriptor y la causa que origina el pedido de revocación y se dirigirá al Responsable de la Autoridad de Registración de la ACSTJ, quien revocará el certificado.
c) Personalmente, presentándose alguno de los funcionarios mencionados ante el Responsable de la Autoridad de Registración de la ACSTJ. Si quien concurre es el suscriptor, se dará curso al pedido de revocación en forma inmediata, previa verificación de su documento de identidad. Si quien concurre es un funcionario autorizado, debe acreditar su identidad mediante presentación de su documento de identidad y copia de su nombramiento o nota de autorización firmada por la máxima autoridad del organismo o dependencia. Se acompañará una nota de solicitud de revocación firmada por la máxima autoridad del organismo o dependencia o por el responsable del área de Recursos Humanos.
d) Dada la urgencia del caso, el Responsable de la Autoridad de Registración de la ACSTJ puede autorizar la revocación obviando la presentación del pedido de revocación y efectuando una confirmación telefónica de la solicitud.

6-3-2- Recepción por otros medios

El Responsable de la Autoridad de Registración se encuentra facultado para aceptar las solicitudes de revocación de certificados que reciba por otros medios (teléfono o fax). En estos casos debe verificar telefónicamente la identidad de quien efectuara el pedido de revocación, solicitando su número de documento de identidad y verificándolo con los datos del solicitante del certificado que figuran en sus archivos. De no ser posible dicha verificación, podrá aceptar la solicitud de revocación si a su juicio la urgencia de la situación lo justifica, debiendo efectuar las verificaciones que estime necesarias para validar la identidad del solicitante.
En caso de constituirse Autoridades de Registración remotas, los procedimientos de recepción de solicitudes de revocación indicados serán cumplidos por el Responsable de la Autoridad de Registración remota (RARR).

6-3-3- Procedimientos complementarios

En todos los casos en que se efectúe una revocación se labrará un acta en la que conste lo actuado en el proceso mencionado, firmada por el Responsable de la Autoridad de Registración y el Oficial Certificador. Un ejemplar del acta quedará a disposición del solicitante de la revocación; el otro ejemplar del acta quedará en poder del Responsable de la Autoridad de Registración para su archivo.

6-3-4- Actualización de repositorios de certificados revocados

Recibida y aceptada una solicitud de revocación el certificado será revocado automáticamente. El repositorio con el estado de los certificados se actualizará de inmediato.

6-3-5- Emisión de listas de certificados revocados (CRLs)

Toda vez que se produzca una revocación, la ACSTJ emite una lista de certificados revocados actualizada en un plazo máximo de VEINTICUATRO (24) horas de aceptada la solicitud. Dicha lista indica claramente la fecha y la hora de la última actualización.
El RAR de la ACSTJ es responsable de firmar digitalmente la lista de certificados revocados, pudiendo utilizar el mismo par de claves utilizado para firmar certificados.
El acceso a las listas de certificados revocados es público, no pudiendo establecerse ninguna clase de restricción. Se encuentra disponible en el sitio web de la ACSTJ, en el siguiente URL: http://ca.juschubut.gov.ar/updateCRL.htm

6-4- Revocación decidida por la AC-STJ

Si la ACSTJ toma conocimiento, por cualquier medio que fuera, acerca de irregularidades cometidas por el suscriptor de un certificado, las cuales, a su juicio, impliquen un posible incumplimiento de sus obligaciones que puedan originar causales de revocación, debe iniciar de inmediato la investigación pertinente.
En caso de confirmar dicho incumplimiento, la ACSTJ procede a revocar de inmediato el certificado comprometido.
De toda denuncia o notificación que se reciba e investigación que se inicie, así como sus resultados, debe dejarse documentación respaldatoria asentada en archivos que estarán a disposición del Organismo Auditante. Lo mismo debe hacerse con los incumplimientos que se detecten y que motiven revocación de certificados.

7- Expiración del certificado

Todos los certificados emitidos por la ACSTJ a favor de suscriptores tienen un período de vigencia de UN (1) año, contados a partir de la fecha de emisión. Esta información consta expresamente en el certificado.
Transcurrido el plazo mencionado, el certificado expirará automáticamente, perdiendo toda validez.

En tal caso, el suscriptor debe gestionar uno nuevo, para lo cual iniciará el correspondiente proceso de solicitud de emisión.

7-1- Renovación de certificados

Un suscriptor puede solicitar la renovación de su certificado dentro de los TREINTA (30) días anteriores a la fecha de su vencimiento. La utilización de este procedimiento de renovación evitará que aquella deba presentar nuevamente la documentación necesaria para emitir un certificado nuevo. El período de validez del certificado renovado se extenderá por UN (1) año a partir de la fecha de la renovación. El suscriptor efectuará su solicitud de renovación vía interfaz web, identificándose con su certificado vigente. El Responsable de la Autoridad de Registración recibe las solicitudes de renovación, verificando que el certificado a renovar se encuentra vigente. Efectuado el control mencionado, aprobará la renovación, autorizando la emisión del nuevo certificado que tendrá la misma clave pública que el certificado vencido.
En caso de constituirse Autoridades de Registración remotas, los procedimientos de recepción de solicitudes de renovación indicados serán cumplidos por el Responsable de la Autoridad de Registración remota (RARR).

8- Responsabilidades

8-1- Responsabilidad de la ACSTJ:

En el cumplimiento de sus funciones relativas a la emisión y administración de certificados, la ACSTJ garantiza:
a) Que el certificado ha sido emitido siguiendo las pautas establecidas en el Manual de Procedimientos para la validación de los datos en él incluidos.
b) Que el certificado satisface todos los requisitos exigidos por la ley 25506, normativa reglamentaria y demás normativa que se dicte.
c) Que los algoritmos y longitudes de claves utilizados cumplen con la última versión aprobada por la Autoridad de Aplicación en relación a los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional.
d) Que el certificado será publicado de acuerdo a lo dispuesto en la Política de Certificación.

8-2- Responsabilidad de las Autoridades de Registración Local y Remotas

a) ?Dar cumplimiento a los procedimientos establecidos en la Política de Certificación de la ACSTJ, de este Manual de Procedimientos y de las normas reglamentarias sobre firma digital.
b) Mantener el control de su clave privada e impedir su divulgación.
c) Solicitar la inmediata revocación de su certificado en caso de compromiso de la clave privada.
d) Resguardar el secreto de su clave privada aún en caso de que el certificado se encuentre expirado.
e) Solicitar la inmediata revocación de su certificado en caso de producirse algún cambio en su situación laboral que implique la discontinuidad de su función como Responsable de las Autoridades de Registración Local (RAL) o Remota (RARR).
f) Mantener actualizados los certificados emitidos
g) Permitir las auditorías y controles necesarios para garantizar la seguridad de la operatoria del sistema.
h) Mantener el archivo y resguardo de la información
i) Mantener la debida confidencialidad respecto a toda información recibida durante el desempeño de su función, cumpliendo las previsiones establecidas en el apartado 9.

8-3- Responsabilidad de los Suscriptores

Es responsabilidad de los suscriptores de certificados mantener informada a la ACSTJ acerca de cualquier cambio en la información que se incluya en los mismos. En particular el suscriptor es responsable de informar a la ACSTJ acerca del cese de su relación laboral con el organismo o

dependencia del que dependiera al momento de efectuar la solicitud del certificado. Las responsabilidades mencionadas se hacen extensivas al responsable del área de Recursos Humanos del organismo o dependencia del que dependiera el suscriptor o al funcionario que administre el registro de personal.

9- Confidencialidad

La información referida a los suscriptores recibida o generada por la ACSTJ puede clasificarse en:
a) No confidencial: la información que obligatoriamente debe figurar en el certificado según lo indicado en la Política de Certificación.
b) Confidencial: toda otra información recibida o generada por la ACSTJ en el proceso de identificación, emisión y administración del certificado, no incluida en el mismo, así como cualquier otra información vinculada a la operatoria de la ACSTJ.
La información considerada confidencial no puede ser revelada por la ACSTJ a terceros bajo ninguna circunstancia, excepto que se dé alguno de los siguientes supuestos:
a) Que exista consentimiento previo del suscriptor para su divulgación.
b) Esta autorización debe otorgarse a través de un mensaje de correo electrónico firmado digitalmente por el suscriptor o bien personalmente por éste, debiendo validar su identidad siguiendo los procedimientos previstos en el apartado 3-2-1-1 en cuanto sean pertinentes.
c) Que la información sea requerida legalmente, por orden judicial emanada de juez competente.
Toda solicitud de información confidencial que se reciba es archivada por el Responsable de la Autoridad de Registración en las condiciones establecidas en el apartado 12.
La información acerca de las causas de la revocación de un certificado es considerada confidencial y sujeta a las mencionadas restricciones informativas.
El deber de confidencialidad debe notificarse por escrito a todo el personal, como requisito de su designación.

10- Interpretación y obligatoriedad

La interpretación de toda la documentación técnica emitida por la ACSTJ se encuentra sometida a lo dispuesto en la ley Nro. 25506 y toda la reglamentación que al respecto se dicte y sus resoluciones reglamentarias.
Las disposiciones contenidas en los documentos indicados emitidos en acuerdo a la normativa mencionada son de aplicación obligatoria para los sujetos involucrados. Se considera que éstos se han notificado de tal circunstancia a partir de la fecha y hora de inicio de validez del certificado emitido.
Toda discrepancia respecto de la interpretación y/o aplicación de las políticas y procedimientos, así como los conflictos que pudieran suscitarse entre la ACSTJ y el suscriptor del certificado, serán resueltos por la Autoridad de Aplicación

11- Auditorías

Según lo establecido por el Art. 81 de la Ley 11.672 y el Art.61 de la Ley 25.237, la Sindicatura General de la Nación cumple funciones de Organismo Auditante de las Autoridades Certificantes que conforman la Infraestructura de Firma Digital del Sector Público Nacional. El propósito de las auditorías es verificar que las Autoridades Certificantes implementen un sistema que asegure la calidad de los servicios de certificación, cumpliendo con los lineamientos establecidos en su documentación técnica.

11-1- Archivos de Auditoría

La ACSTJ mantiene un sistema de archivos de transacciones de auditoría que permita mantener en un entorno de seguridad toda la información considerada relevante que pueda ser requerida por la Sindicatura General de la Nación en el desarrollo de su función de Organismo Auditante.
El sistema prevé la generación de:
a) Logs del sistema

Se mantiene un registro de logs que incluye información sobre los siguientes eventos:
1. Encendido y apagado del equipo
2. Ingreso y salida del sistema de cada usuario
3. Programas ejecutados
4. Acceso a los objetos del sistema (base de passwords, base de datos de certificados)
5. Cambios en los archivos o políticas de definición de logs
Para cada uno de estos eventos, se conserva la siguiente información mínima:
I. Usuario
II. Fecha y hora
III. Tipo de evento
IV. Datos particulares del evento
6. Registros de transacciones de auditoría que permitan el seguimiento de las distintas etapas del ciclo de vida de los certificados.
b) Copia de la documentación respaldatoria del proceso de validación de identidad de los suscriptores.
Todos los archivos (digitales o en soporte papel) que respalden las transacciones deben encontrarse actualizados en forma permanente y a disposición del Organismo Auditante.
Los archivos de auditoría son generados por el Operador Técnico de la ACSTJ. Se conservan bajo llave bajo la responsabilidad del Responsable de Seguridad Informática. Este tendrá en su poder un juego de llaves, junto al Operador Técnico y su sustituto. Una copia de la misma se encuentra en poder del responsable de la ACSTJ. Debe quedar constancia de los datos de quienes poseen una copia de las llaves Los archivos de transacciones de auditoría solo pueden ser visualizados por representantes de dicho organismo.
Los archivos deben conservarse en un espacio físico acondicionado dentro del ámbito de la ACSTJ por un plazo mínimo de DIEZ (10) años. Aquellos con antigüedad mayor a un año pueden trasladarse a un archivo secundario en un lugar físico protegido manteniendo las mismas medidas de seguridad.
De utilizarse un esquema de registración descentralizada, los Responsables de la Autoridades de Registración remotas (RARR) están obligados a mantener a disposición del Organismo Auditante archivo de copias de toda la documentación que reciban o generen como respaldo del proceso de validación de la identidad de los suscriptores. El mencionado archivo se conservará bajo la responsabilidad del RARR y su sustituto, en lugar físico seguro y por el plazo establecido en el presente apartado. Esta obligación se extiende a los auxiliares de los RARR que se hubieran designado.
La ACSTJ efectuará auditorías periódicas sobre las Autoridades de Registración remotas con el fin de verificar el cumplimiento por parte de estas de los procedimientos de validación y la revisión de su documentación respaldatoria.
Asimismo, el Responsable de una Autoridad de Registración remota está obligado a efectuar una auditoría semestral sobre sus auxiliares y en aquellos casos en los que se hubiera aplicado el procedimiento opcional indicado en el apartado 3-2-2-3-3. A tal fin efectuará una revisión de la documentación respaldatoria de dicho proceso, así como de los procedimientos de validación utilizados.

11-2-- Copias de resguardo de Archivos de transacciones de Auditoría

Las copias de resguardo de los archivos de transacciones de auditoría se mantienen a disposición del Organismo Auditante. El procedimiento para su generación y mantenimiento se encuentra especificado en el Manual de Procedimientos de Seguridad.

12- Archivos

La ACSTJ mantiene un sistema de archivos que permita la conservación, en condiciones adecuadas de seguridad, de toda la información referida a los procesos de emisión y administración de los certificados.
La información mínima a conservar es la siguiente:
a) Solicitudes de emisión de certificados, incluyendo documentación de respaldo del proceso de

identificación
b) Solicitudes de revocación de certificados.
c) Notificaciones de compromiso de claves.
d) Emisión de certificados.
e) Revocación de certificados.
f) Emisión de listas de certificados revocados.
g) Cambios de claves.
h) Nombramiento de personal en roles confiables.
i) Actas de actividades efectuadas por dicho personal
j) Nombramiento de Responsables de Autoridades de Registración remotas y de sus auxiliares
k) Toda comunicación entre la ACSTJ y el Organismo Licenciante.
Los archivos se conservarán bajo llave. Es función del Responsable de la Autoridad de Registración local su mantenimiento y resguardo. En caso de ausencia, su función será cubierta por su sustituto. Cada uno de los responsables mencionados tendrá en su poder un juego de llaves. Una copia de la misma se encuentra en poder del responsable de la ACSTJ. Debe quedar constancia escrita de los datos de quienes poseen una copia de las llaves.
Los archivos deben conservarse en un espacio físico acondicionado dentro del ámbito de la ACSTJ por un plazo mínimo de DIEZ (10) años. Aquellos con antigüedad mayor a un año pueden trasladarse a un archivo secundario en un lugar físico protegido, manteniendo las mismas medidas de seguridad.
De utilizarse un esquema de registración descentralizada, los Responsables de la Autoridades de Registración remotas (RARR) están obligados a mantener archivo de toda la documentación que reciban o generen como respaldo del proceso de validación de la identidad de sus auxiliares. El mencionado archivo se conservará bajo la responsabilidad del RARR y su sustituto, en lugar físico seguro y por el plazo establecido en el presente apartado. Esta obligación se extiende a los auxiliares de los RARR que se hubieran designado respecto a la documentación respaldatoria del proceso de validación de identidad de los suscriptores que hubieran solicitado sus certificados por su intermedio. En caso que se optara por centralizar el archivo de dicha información bajo la responsabilidad del RARR, su auxiliar le remitirá la documentación recibida, conservando copia de la misma en su poder.

12-1- Copias de resguardo

Se mantendrán copias de resguardo de todos los archivos referidos a los procesos de emisión y administración de certificados que se encuentren en el servidor de la ACSTJ. El procedimiento para su generación y mantenimiento se encuentra especificado en el Manual de Procedimientos de Seguridad.

13- Planes de emergencia

La ACSTJ posee un plan de contingencias que permite garantizar el mantenimiento mínimo de la operatoria y la recuperación de los recursos comprometidos dentro de las VEINTICUATRO (24) horas de producida una emergencia.
Los procedimientos detallados a cumplir se encuentran descriptos en el Plan de Contingencias.

14- Controles de Seguridad

14-1- Controles de Seguridad Física y Personal

La ACSTJ implementa controles de seguridad físicos y personales a fin de dotar de un adecuado marco de seguridad a las funciones que desarrolla (generación de claves, autenticación, emisión y revocación de certificados, archivos, etc.).
Estos controles son críticos para otorgar confiabilidad a los certificados, ya que su ausencia comprometerá todas las instancias del sistema.
Los controles de seguridad física y personal se detallan en el Manual deProcedimientos de Seguridad

14-2- Controles de Seguridad Lógica:

La ACSTJ define en el Manual de Procedimientos de Seguridad:
a) Las medidas de seguridad a fin de proteger sus claves criptográficas pública y privada y todos los demás datos críticos necesarios para operar con módulos criptográficos (números pin, passwords, claves manuales compartidas o no por el personal, etc.).
b) Otros controles de seguridad lógica que garantizan las funciones de generación de claves, identificación de usuarios, emisión y renovación de certificados, auditoría y archivos.

14-3- Controles de Seguridad del Computador:

Son aplicables los controles indicados en los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional (Resolución N° 194/98 de la ex Secretaría de la Función Pública).

15- Certificados y listas de certificados revocados - Características

Se emplean certificados en formato x509 versión 3 o superior y listas de certificados revocados en formato x509 versión 2.
La información a incluir en los certificados se encuentra detallada en los Estándares sobre Tecnología de Firma Digital para la Administración Pública Nacional (Resolución N° 194/98 de la ex Secretaría de la Función Pública) y en el apartado 5 del presente manual.

16- Administración de la documentación técnica emitida por la ACSTJ

En este capítulo se incluyen disposiciones acerca del mantenimiento de la documentación técnica emitida por la ACSTJ sus eventuales modificaciones y notificaciones.

16-1- Cambios a la documentación técnica:

La ACSTJ informará a sus suscriptores acerca de todos aquellos cambios significativos que se efectúen a la documentación técnica pública mencionada en el presente manual. Las modificaciones indicadas serán publicadas en el sitio web de la ACSTJ
Toda modificación debe ser aprobada por Resolución emitida por la Autoridad de Aplicación.

16-2- Publicación y Notificación:

El Manual de Procedimientos y demás documentación técnica pública emitida por la ACSTJ, así como sus versiones anteriores se encuentran disponibles en su sitio web en el siguiente URL: http://ca.juschubut.gov.ar/