POLÍTICAS
DE LA
AUTORIDAD DE REGISTRO (AR)

Características de cumplimiento de Autoridades de Registro

(AR)

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, S.A.

INDICE

1. MARCO LEGAL

1.1. Base Legal

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento; Ley Orgánica de Defensa del consumidor, Ley Orgánica de Transparencia de la Información y Acreditación de CONATEL.

1.2. Vigencia

El presente documento entrará en vigencia a partir de la fecha de su aprobación.

1.3. Soporte Legal

a) Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial No. 577 de 17 de abril de 2002.

b) De conformidad con lo dispuesto en el Art. 37 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, el Consejo Nacional de Telecomunicaciones es el Organismo de autorización, registro y regulación de las Entidades de Certificación de Información y Servicios Relacionados Acreditados.

c) Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedido mediante Decreto Ejecutivo No. 3496 publicado en el Registro Oficial 735 de 31 de diciembre de 2002, y reformas constantes en Decreto Ejecutivo 1356 de 29 de septiembre de 2008, publicadas en el Registro Oficial No. 440 de 6 de octubre de 2008.

d) Que, el segundo artículo enumerado agregado por el artículo 4 del Decreto Ejecutivo No. 1356 a continuación del artículo 17 del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, dispone que la acreditación como entidad de certificación de información y servicios relacionados, consistirá en un acto administrativo emitido por el CONATEL a través de una resolución que será inscrita en el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados.

e) Resolución 477-20-CONATEL-2008 de 08 de octubre de 2008, se aprobó el modelo de resolución para la Acreditación como Entidad de Certificación de Información y Servicios Relacionados.

f) Resolución No. TEL-640-21-CONATEL-2010 de 22 de octubre de 2010, aprobó la petición de Acreditación de la Compañía SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A. como Entidad de Certificación de Información y Servicios Relacionados, para los cual la SENATEL suscribió el respectivo acto administrativo, conforme el modelo aprobado por el Consejo Nacional de Telecomunicaciones.

2. INTRODUCCIÓN

2.1. Presentación

Este documento regula la operación y procedimientos mínimos adoptados por las Autoridades de Registro (AR) que gestionan los certificados para la Entidad de Certificación de Información (ECI) SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

La Autoridad de Registro es la entidad responsable de la comunicación entre el usuario y la autoridad certificadora. Está vinculada a una AC y tiene por objetivo recibir, validar, verificar y gestionar las solicitudes de emisión o revocación de los certificados de firma electrónica, cumpliendo con lo establecido en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y en concordancia con las políticas y procedimientos definidos por la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

2.2. Nombre del Documento

2.2.1. Identificación

Nombre:	Políticas de la Autoridad de Registro (PAR).
Versión:	3.1
Descripción:	Políticas de la Autoridad de Registro.
Fecha de Emisión:	29 de Noviembre 2012

2.2.2. Publicación

Este documento puede obtenerse libremente en la dirección electrónica https://www.securitydata.net.ec.

2.3. Definiciones y Acrónimos

2.3.1. Definiciones

- **Certificado Electrónico:** Es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

- **Certificado Reconocido:** Certificado expedido por una Entidad Acreditada que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

- **Clave Pública y Clave Privada:** La criptografía asimétrica en la que se basa la PKI emplea un par de claves (podrían ser dos pares de claves), lo que se cifra con una de ellas sólo se puede descifrar con la otra y viceversa. A una de esas claves se la denomina pública y se la incluye en el certificado electrónico, mientras que a la otra se la denomina privada y únicamente es conocida por el titular del certificado.

- **Datos de Creación de Firma (Clave Privada):** Son datos únicos, como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear la firma electrónica.

- **Datos de Verificación de Firma (Clave Pública**): Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

- **Dispositivo Seguro de Creación de Firma (DSCF):** Instrumento que sirve para aplicar los datos de creación de firma.

- **Firma Electrónica**: Es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

- **Firma Electrónica Avanzada:** Es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.

- **Función Hash:** Es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

- **Listas de Certificados Revocados (CRL):** Lista donde figuran las relaciones de certificados revocados o suspendidos.

- **Módulo Criptográfico Hardware (HSM):** Módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

- **Sellado de tiempo:** Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

- **Autoridad de Sellado de Tiempo (TSA):** Entidad de confianza que emite sellos de tiempo.

- **Autoridad de Validación (VA**): Entidad de confianza que proporciona información sobre la validez de los certificados y de las firmas electrónicas.

2.3.2.Acrónimos

AC:	Autoridad de Certificación
AC Sub:	Autoridad de Certificación Subordinada
AR:	Autoridad de Registro
PC:	Política de Certificación

DPC:	Declaración de Prácticas de Certificación
CRL:	Lista de Certificados Revocados (Certificate Revocation List)
HSM:	Módulo de seguridad criptográfico (Hardware Security Module)
LDAP:	Lightweight Directory Access Protocol
OCSP:	Online Certificate Status Protocol.
PKI:	Infraestructura de Clave Public (Public Key Infrastructure)
PSC:	Prestador de Servicios de Certificación
TSA:	Autoridad de sellado de tiempo (Time Stamp Authority)
VA:	Autoridad de validación (Validation Authority)
ECI:	Entidad de Certificación de Información
OID:	Identificador de objeto único (Object identifier)
DN:	Nombre Distintivo (Dinstinguished Name)
C:	País (Country), Atributo del Nombre Distintivo
CN:	Nombre Común (Common Name), Atributo del Nombre Distintivo
O:	Organización (Organization), Atributo del Nombre Distintivo
OU:	Unidad Organizacional (Organizational Unit), Atributo del Nombre Distintivo
SN:	Apellido (SurName), Atributo del Nombre Distintivo
ISO:	International Organizational for Standarization
PKCS:	Public Key Cryptography Standars, Estándares PKI
UTF8:	Unicode Transformation Format – 8 bits.

3. Disposiciones Generales

Para el presente documento se deben aclarar los siguientes conceptos:

a) **Operador de la AR**: Persona responsable de la ejecución de las actividades propias de la AR. Esta persona debe realizar las validaciones y verificaciones definidas en la política del certificado que corresponda.
b) **Confirmar la identidad del solicitante**: proceso para comprobar que el solicitante es la persona con autoridad para solicitar el certificado, de acuerdo a la política asociada al certificado.
c) **Suspensión de un operador**: Es cuando un funcionario que tiene el rol de agente de registro deja de ejercer sus labores temporalmente, alterándosele sus permisos dentro del sistema de la AC.

d) **Desvincular a un operador**: Es el proceso de separar a un agente de registro de sus funciones, eliminándole los permisos dentro del sistema de la AC. Este proceso ocurre cuando:

1. El funcionario ha renunciado a su cargo en la organización
2. El funcionario es cesado de sus funciones o de su organización
3. El funcionario que ha recibido la función de agente de registro la deja de ejercer, aunque continúa trabajando en otros puestos de la organización.
4. El funcionario sancionado mediante un proceso administrativo, o por un procedimiento disciplinario, que impidan continuar en su cargo.

e) **Encargado de la AR**: Persona responsable de la supervisión de las funciones de los agentes de registro, y la coordinación con la AC.
f) **Expediente del operador:** Es el conjunto de documentos relativos a un agente de registro.
g) **Expediente de instalación:** Es el conjunto de documentos relativo a las instalaciones de la AR, tales como plan de continuidad de negocio, análisis de riesgos, reglamento de sanciones, inventario de activos y un plan de terminación de la AR.
h) **Instalaciones:** Es el ambiente físico de una AR, cuyo funcionamiento es debidamente autorizado para realizar las actividades de validación y verificación de las solicitudes de certificado.
i) **Validación del solicitante del certificado:** Es la verificación de la identidad del individuo o la organización que se presente ante una AR para solicitar un certificado. Esta validación requiere de la presencia física del solicitante y de la evidencia que permita determinar su autoridad para la solicitud de su certificado respectivo.

4. Funciones de la AR

Las áreas y actividades ejecutadas por la AR incluyen:

- Verificar y validar los documentos de identidad
- Registrar a los suscriptores
- Entregar códigos para la emisión de los certificados de firma electrónica
- Gestionar la aceptación del certificado por parte del suscriptor
- Gestionar revocaciones de certificados
- Registrar los eventos en las bitácoras
- Controlar y supervisar a los agentes de registro
- Controlar los reportes de incidentes
- La AR debe establecer los procedimientos y guías para asegurar el cumplimiento de la política de certificados y de este documento, además de tomar las acciones que prevengan alguna deficiencia de la AR, incluyendo la terminación o suspensión de sus deberes.

Para cada agente de registro, de acuerdo a las Políticas de Certificado de cada tipo de certificado la AR debe requerir de los solicitantes:

Certificado de Persona Natural:

a) Original de cédula de ciudadanía o pasaporte en casos de extranjeros,
b) Original de papeleta de votación actualizada, (para militares la libreta militar).
c) Original de la planilla de un servicio básico, que certifique la dirección que conste en el RUC (luz, agua, teléfono, celular, Tvcable, gas o internet) de cualquiera de los últimos tres meses, a nombre de la persona que solicita el certificado. – (Si la planilla no está a su nombre o no es de la dirección del RUC NO se podrá tramitar la solicitud). Se puede aceptar también el contrato de arrendamiento del local o vivienda en el cual conste la dirección del RUC y que este a nombre de la persona que solicita el certificado. El contrato debe tener los sellos del juzgado del inquilinato + las tres últimas facturas del pago hecho
d) Original o copia certificada del Registro único de contribuyentes (RUC) en caso de disponerlo
e) Original o copia certificada del Registro único de proveedores (RUP) en caso de disponerlo
f) Ser persona física y mayor de edad.
g) Formulario de solicitud lleno y firmado
h) Contrato lleno y firmado
i) Presentarse físicamente en la entidad que emitirá el certificado para firmar el contrato y validar la identidad.
j) Hacer una foto instantánea del solicitante el momento en que se presente físicamente en la entidad y almacenarla conjuntamente con los demás documentos digitalizados.

Certificado de Persona Jurídica-Empresa:

a) Original o copia certificada Registro único de contribuyentes (RUC) de la empresa
b) Original o copia certificada Registro único de proveedores (RUP) en caso de disponerlo
c) Original o copia certificada y legible del nombramiento del representante legal adjuntando copia clara de la cédula de ciudadanía del mismo.
d) Original o copia certificada de constitución de la Empresa solicitante en la cual conste el nombre de la persona o las personas que llevarán la representación legal de la misma (notariada)
e) Autorización firmada por el representante legal
f) Formulario de solicitud lleno y firmado
g) Presentarse físicamente en la entidad que emitirá el certificado para firmar el contrato y validar la identidad.
h) Hacer una foto instantánea del solicitante el momento en que se presente físicamente en la entidad y almacenarla conjuntamente con los demás documentos digitalizados.

Certificado de Funcionario Público:

a) Original de cédula de ciudadanía o pasaporte en casos de extranjeros,
b) Papeleta de votación actualizada, (para militares la libreta militar).
c) Original o copia certificada y legible del nombramiento o "Acción de Personal" del solicitante o a su vez un certificado laboral que certifique el cargo del funcionario público,

actualizado, firmado por el representante legal o emitida por el departamento de recursos humanos de la institución.

d) Original o copia certificada del Registro único de contribuyentes (RUC) de la institución
e) Original o copia certificada del Registro único de proveedores (RUP) en caso de disponerlo
f) Original o copia certificada y legible del nombramiento del representante legal adjuntando copia clara de la cédula de ciudadanía del mismo.
g) Autorización firmada por el representante legal, donde conste el número de solicitudes, nombre y cargo de todos los solicitantes de la Empresa para emisión de certificado de Firma Electrónica.
h) Formulario de solicitud lleno y firmado
i) Presentarse físicamente en la entidad que emitirá el certificado para firmar el contrato y validar la identidad.
j) Hacer una foto instantánea del solicitante el momento en que se presente físicamente en la entidad y almacenarla conjuntamente con los demás documentos digitalizados.

Certificado de Miembro de empresa:

a) Original de cédula de ciudadanía o pasaporte en casos de extranjeros,
b) Original de papeleta de votación actualizada.
c) Original o copia certificada del Registro único de contribuyentes (RUC) de la empresa
d) Original o copia certificada del Registro único de proveedores (RUP) en caso de disponerlo
e) Original o copia certificada y legible del nombramiento del representante legal adjuntando copia clara de la cédula de ciudadanía del mismo.
f) Original o copia certificada de constitución de la Empresa solicitante en la cual conste el nombre de la persona o las personas que llevarán la representación legal de la misma (notariada)
g) Autorización firmada por el representante legal, donde conste el número, nombre y cargo del o de los solicitante(s) de la Empresa para emisión de certificado de Firma Electrónica.
h) Formulario de solicitud lleno y firmado
i) Presentarse físicamente en la entidad que emitirá el certificado para firmar el contrato y validar la identidad.
j) Hacer una foto instantánea del solicitante el momento en que se presente físicamente en la entidad y almacenarla conjuntamente con los demás documentos digitalizados.

Certificado de Representante Legal:

a) Original de cédula de ciudadanía o pasaporte en casos de extranjeros,
b) Original de papeleta de votación actualizada.
c) Original o copia certificada del Registro único de contribuyentes (RUC) de la empresa
d) Original o copia certificada del Registro único de proveedores (RUP) en caso de disponerlo
e) Original o copia certificada y legible del nombramiento del representante legal adjuntando copia clara de la cédula de ciudadanía del mismo.

f) Original o copia certificada de constitución de la Empresa solicitante en la cual conste el nombre de la persona o las personas que llevarán la representación legal de la misma (notariada)
g) Formulario de Solicitud lleno y firmado
h) Presentarse físicamente en la entidad que emitirá el certificado para firmar el contrato y validar la identidad.
i) Hacer una foto instantánea del solicitante el momento en que se presente físicamente en la entidad y almacenarla conjuntamente con los demás documentos digitalizados.

4.1. Autenticación de la AR

En la constitución de una nueva AR, se realizarán las siguientes acciones:

- Security Data Seguridad en Datos y Firma Digital verificará la existencia de la entidad mediante sus propias fuentes de información.
- Un representante autorizado de la organización deberá firmar un contrato con Security Data Seguridad en Datos y Firma Digital, donde se especificarán los aspectos concretos de la delegación y las responsabilidades de cada agente.
- Además se exigirá a la AR el cumplimiento de lo siguiente respecto de los operadores de AR:
    - Verificar y validar la identidad de los nuevos operadores de la AR. La AR deberá enviar a Security Data Seguridad en Datos y Firma Digital la documentación correspondiente al nuevo operador, así como su autorización para que actúe como operador de AR.
    - Asegurar que los operadores de la AR hayan recibido formación suficiente para el desempeño de sus funciones, asistiendo como mínimo a una sesión de formación de operador.
    - Asegurar que la comunicación entre la AR y Security Data Seguridad en Datos y Firma Digital se realiza de forma segura mediante el uso de certificados de firma electrónica de operador.

5. Controles del Personal

5.1. Disposiciones generales

La autoridad de registro es la responsable administrativa de su operación y debe enviar a la AC la información actualizada de los operadores de la AR activos, sus perfiles, cualidades y necesidades de acceso a la información

Los agentes de registro deben ser funcionarios de la organización que opera como Autoridad de Registro.

5.2. Requerimientos de documentación del Operador de la AR

Para cada operador de la AR, en concordancia con los roles de responsables en la sección 6.2.1 y 6.2.3 de las DPC de Security Data Seguridad en Datos y Firma Digital, la AR correspondiente debe poseer un expediente con:

a) Un contrato de trabajo o documento que permita comprobar su situación laboral.
b) Comprobante de verificación de antecedentes criminales.
c) Comprobante de verificación de empleos anteriores. Incluyendo empleos en otras RA y las sanciones aplicadas, en caso de que existan.
d) Comprobante de aprobación de las capacitaciones recibidas referentes a las actividades propias de un Agente de Registro.
e) Declaración en que afirma conocer las atribuciones que asume y el deber de cumplir con la política nacional de certificación, y de mantener confidencialidad y privacidad de los datos disponibles en la AC o AR.
f) Resultados de las evaluaciones periódicas
g) Registro que lo compromete a ejecutar labores de agente de registro en la AR.
h) Registro en la AC o AR del momento en que fue incluido el rol de agente en el sistema de certificación.

Cuando un operador es desvinculado o suspendido de sus actividades en la AR entonces el expediente de la persona debe indicar:

- Registro de la solicitud para deshabilitar al agente de registro del sistema de certificación
- Registro en la AC del momento en que el agente de registro es deshabilitado o suspendido del sistema de certificación

5.3. Requerimientos Capacitación

Todo agente de registro, y personal involucrado de su administración, debe recibir capacitación y documentación en los siguientes temas:

a) Concepto básico de certificados de firma electrónica y Tokens
b) Principios y mecanismos de seguridad de la AR
c) Procedimientos de recuperación de desastres y de continuidad del negocio
d) Procedimientos para la validación y verificación de identidad

Esto deberá constar en el expediente de agente de registro. Cuando se presenten cambios significativos en las operaciones de la AR, el personal involucrado debe recibir capacitación al respecto.

5.4. Procedimiento de suspensión o desvinculación

Cuando un operador sea suspendido o desvinculado de sus actividades, el encargado de la AR debe gestionar inmediatamente con la AC la suspensión o revocación de sus permisos de acceso a los sistemas de la AC y de las labores inherentes a las actividades de la AR. Estos procesos deben ser documentados.

6. Controles físicos

6.1. Exigencias mínimas de seguridad física

Todas las Autoridades de Registro deben cumplir con las siguientes exigencias mínimas de seguridad:

a) Dispositivos para la detección de incendios
b) Gabinetes o armarios con llave, de uso exclusivo de la AR
c) Los equipos de la AR deben estar protegidos contra fallas del fluido eléctrico y otras anomalías en la energía
d) Vigilancia y monitoreo del ambiente de la AR durante su horario de operación
e) Un perímetro de seguridad en el edificio donde se encuentran las instalaciones de la AR, con un guarda asignado durante el horario de operación.
f) Controles contra coacción para cada agente de registro
g) Iluminación de emergencia

7. Controles lógicos

7.1. Controles de seguridad de las estaciones de trabajo

Las estaciones de trabajo de la AR, incluyendo los equipos portátiles, deben estar protegidas contra amenazas y acciones no autorizadas.

Las estaciones de trabajo de la AR, deben cumplir las siguientes directivas de seguridad:

a) Control de acceso lógico al sistema operacional
b) Control de acceso con contraseña a la estación de trabajo
c) Enlace dedicado con acceso a internet

En las estaciones de la AR debe contarse con un perfil de administrador de los equipos, que sea el responsable de administrar la configuración de la máquina y esta labor debe ser segregada de las funciones del agente de registro de la AR.

8. Controles de seguridad de la información

8.1. General

Toda la información y documentos relacionados con la instalación y puesta en operación de la AR deben ser clasificados y almacenados de acuerdo a lo establecido en la sección 6 de DPC de Security Data Seguridad en Datos y Firma Digital y en la sección 6.1 del presente documento que garantizan privacidad y confidencialidad de la información.

La AR debe mantener en documentación privada y confidencial, la siguiente información:

a) Contrato de la AR con Security Data Seguridad en Datos y Firma Digital.
b) Inventario de Activos de la AR

Adicionalmente, debe tener disponible los siguientes documentos para uso de los agentes de registro:

- Copia de la Declaración de Prácticas de Certificación.
- Copia de las políticas de certificación.

8.2. Procedimientos de almacenamiento, manipulación y destrucción de documentos

Los documentos electrónicos que componen los expedientes de los solicitantes de certificado deben ser guardados en el repositorio de Security Data firmados con un certificado emitido la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

Almacenar de forma segura y por un periodo nunca inferior a 15 años la documentación aportada en el proceso de emisión del Certificado y en proceso de suspensión / revocación del mismo, en los términos y condiciones que se establezcan en esta DPC, en la PC de cada tipo de certificado y, en su caso, en el acuerdo para la Autoridad de Registro

La AR permitirá a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL el acceso a los archivos y a los procedimientos de conservación de los archivos asumidos por la AR y le dará el derecho a investigar cualquier sospecha de infracción de la DPC y/o de las PC por parte de la AR o cualquier poseedor de un Certificado. La AR y los poseedores de cualquier Certificado deberán informar a la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL inmediatamente de cualquier sospecha de infracción

9. Controles del ciclo de vida del certificado

La AR debe respetar el ciclo de vida del certificado definido en la sección 5.2 de las DPC de Security Data Seguridad en Datos y Firma Digital.

10. Acuerdos operacionales

La AC debe celebrar un acuerdo operacional para que la AR ejecute las actividades de validación y verificación de las solicitudes de certificado. Este acuerdo debe contener al menos:

a) La identificación y calidades de los celebrantes del acuerdo de la AR
b) La identificación de los deberes que competen a la AR en función del acuerdo
c) La identificación de los responsables de la AR
d) Compromiso de la AR de cumplir con las normas y procedimientos definidos
e) Plazo por medio del cual el acuerdo es celebrado
f) Obligaciones de la AR para verificar los procesos que ejecuta

11. Revisiones

Documento: Políticas de la AR					
Revisión	**1**	**2**	**3**	**4**	**5**
Publicado	**24/01/2011**	**24/01/2011**	**06/01/2012**	**29/11/2012**	
Autor(es)	**LV/XC**	**LV/XC**	**XC**	**XC**	
Fecha de revisión	**18/02/2011**	**14/03/2011**			
Revisado por	**XC**	**XC**			
Fecha aprobado	**02/03/2011**	**16/03/2011**	**06/01/2012**	**29/11/2012**	
Aprobado por	**CS**	**CS**	**CS**	**CS**	