# DECLARACIÓN DE PRÁCTICAS DE SEGURIDAD (DPS)

# DE

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

**Versión 1.0**

# 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 EJectr6nico, 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

El presente documento contempla la Declaración de Políticas de Seguridad (DPS) de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL.

Esta DPS específica y contempla lo establecido en la DPC de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL estableciendo un conjunto de reglas que indican los procedimientos seguidos por la Entidad de Certificación en cuanto a la seguridad en su infraestructura.

Esta Declaración de Políticas de Seguridad (DPS), junto con la DPC de la ECI SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, están dirigidas a cualquiera que confíe en esta ECI.

### 2.2. Nombre del Documento

#### 2.2.1.Identificación

| | |
|---|---|
| Nombre: | Declaración de Políticas de Seguridad (DPS) |
| Versión: | 1.0 |
| Descripción: | Declaración de Políticas de Seguridad de Security Data Seguridad en Datos y Firma Digital S.A. |
| Fecha de Emisión: | 11 de Febrero 2011 |

#### 2.2.2.Publicación

Este documento puede obtenerse libremente en la dirección electrónica 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 digitales 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 Pública (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. ENTIDADES PARTICIPANTES

## 3.1. Entidad Acreditada (EA)

Security Data Seguridad en Datos y Firma Digital es un Entidad Acreditada (EA) que emite certificados reconocidos según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Security Data Seguridad en Datos y Firma Digital es la entidad emisora de los certificados y responsable de las operaciones del ciclo de vida de los certificados. Las funciones de autorización, registro, emisión y revocación respecto de los certificados personales de entidad final, pueden ser realizadas por otras entidades por delegación soportada contractualmente con Security Data Seguridad en Datos y Firma Digital, que actuarán como intermediarios. Security Data Seguridad en Datos y Firma Digital también ofrece servicios de validación de firmas electrónicas y de sellado de tiempo, regidos por sus políticas particulares, no incluidas en este documento.

## 3.2. Autoridad de Certificación (AC)

El sistema de certificación de Security Data Seguridad en Datos y Firma Digital está compuesto por diversas Autoridades de Certificación (en inglés CA o Certificate Authority) organizadas bajo una Jerarquía de Certificación.

### 3.2.1. Autoridad de Certificación Raíz

Se denomina Autoridad de Certificación Raíz (AC Root) a la entidad dentro de la jerarquía que emite certificados a otras autoridades de certificación, y cuyo certificado de clave pública ha sido autofirmado. Su función es firmar el certificado de las otras ACs pertenecientes a la Jerarquía de Certificación.

## 3.3. Autoridad de Registro (AR)

Una Autoridad de Registro (en inglés RA o Registration Authority) de Security Data Seguridad en Datos y Firma Digital, es la entidad encargada de:

1. Tramitar las solicitudes de certificados.
2. Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
3. Validar las circunstancias personales de la persona que constará como firmante del certificado
4. Gestionar la generación de claves y la emisión del certificado
5. Hacer entrega del certificado al suscriptor.

Podrán actuar como AR de Security Data Seguridad en Datos y Firma Digital:

6. Cualquier Corporación que sea cliente de Security Data Seguridad en Datos y Firma Digital, para la emisión de certificados a nombre de la corporación o a miembros de la corporación.

7. Cualquier entidad de confianza que llegue a un acuerdo con Security Data Seguridad en Datos y Firma Digital para actuar como intermediario en nombre de Security Data Seguridad en Datos y Firma Digital.
8. La propia Security Data Seguridad en Datos y Firma Digital directamente.

Security Data Seguridad en Datos y Firma Digital formalizará contractualmente las relaciones entre ella y cada una de las entidades que actúen como AR de Security Data Seguridad en Datos y Firma Digital.

La entidad que actúe como AR de Security Data Seguridad en Datos y Firma Digital podrá autorizar a una o varias personas como Operador de la AR para operar con el sistema informático de emisión de certificados de Security Data Seguridad en Datos y Firma Digital en nombre de la AR.

Allí donde la ubicación geográfica de los suscriptores represente un problema logístico para la identificación del suscriptor y en la solicitud y entrega de certificados, la AR podrá delegar estas funciones a otra entidad de confianza. Dicha entidad deberá tener una especial vinculación con la AR y una relación de proximidad con los suscriptores de los certificados que justifique la delegación. La entidad de confianza deberá firmar un acuerdo de colaboración con la AR en el que se acepte la delegación de estas funciones. Security Data Seguridad en Datos y Firma Digital deberá conocer y autorizar de manera expresa el acuerdo.

### 3.4. Solicitante

Solicitante es la persona natural que, en nombre propio o en representación de un tercero, solicita la emisión de un certificado a Security Data Seguridad en Datos y Firma Digital. Los requisitos que debe reunir un solicitante dependerán del tipo de certificado solicitado y estarán recogidos en la "Política de Certificación" de cada tipo de certificado concreto.

### 3.5. Suscriptor

El Suscriptor es la persona natural o jurídica que ha contratado los servicios de certificación de Security Data Seguridad en Datos y Firma Digital. Por lo tanto será el propietario del certificado. En general, el suscriptor de un certificado de Security Data Seguridad en Datos y Firma Digital será una Corporación (empresa privada, entidad pública, persona natural), la identidad de la cual aparecerá en el propio certificado.

### 3.6. Firmante

El Firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona jurídica a la que representa.

El Firmante será responsable de custodiar los datos de creación de firma, es decir, la clave privada asociada al certificado.

### 3.7. Custodio de las Claves

La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona natural solicitante, cuya identificación se incluirá en el certificado electrónico

### 3.8. Tercero que confía en los Certificados

Se entiende como tercero que confía en los certificados (en inglés, relaying party) a toda persona u organización que voluntariamente confía en un certificado emitido por Security Data Seguridad en Datos y Firma Digital.

Los certificados reconocidos emitidos por Security Data Seguridad en Datos y Firma Digital tienen carácter universal y están aceptados por los organismos públicos del estado ecuatoriano, como Ministerios, Secretarías, etc.

Las obligaciones y responsabilidades de Security Data Seguridad en Datos y Firma Digital con terceros que voluntariamente confíen en los certificados se limitarán a las recogidas en la DPC de Security Data Seguridad en Datos y Firma Digital.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

## 4. DECLARACIÓN DE PRÁCTICAS DE SEGURIDAD

### 4.1. Generación e Instalación del Par de Claves

#### 4.1.1. Generación del Par de Claves

Se distinguirán dos casos en la generación de claves para certificados reconocidos:

a) En hardware (soporte físico)

La generación de la clave de las ACs se realiza, de acuerdo con el proceso documentado de ceremonia de claves, dentro de la sala de seguridad del la Entidad Acreditada, en dispositivos criptográficos hardware (HSM), por personal adecuado según los roles de confianza y, al menos con un control dual y testigos de Security Data Seguridad en Datos y Firma Digital, de la organización titular de la AC y del auditor externo.

Para los certificados de entidad final, el par de claves será creado en el mismo dispositivo utilizando el sistema proporcionado por la AR. Este proceso está vinculado de forma segura al proceso de generación del certificado, garantizando la confidencialidad de la clave privada durante el proceso de generación y la complementariedad entre los datos de creación y verificación de firma.

b) En software/Roaming

El suscriptor recibirá una invitación para conectarse al servicio de generación de certificados de Security Data Seguridad en Datos y Firma Digital. El suscriptor generará el par de claves en su sistema y enviará la clave pública a la AC en formato PKCS10 u otro equivalente.

En otros casos, la generación de claves del suscriptor se realizará en dispositivos que aseguran razonablemente que la clave privada será protegida por el suscriptor contra la utilización por otros, bien por medios físicos, bien estableciendo el suscriptor los controles y medidas de seguridad adecuadas.

### 4.1.2.Entrega de la Clave Privada al Suscriptor

a) En hardware (soporte físico)

La clave privada será entregada junto al certificado en el dispositivo de creación de firma. La AR será responsable de garantizar la entrega del dispositivo al suscriptor, asegurándose así que éste último está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

El dispositivo criptográfico utiliza una clave de activación para el acceso a las claves privadas.

b) En software

El suscriptor generará el par de claves directamente en su sistema y se guardará en el CAPI del computador.

c) Roaming

El suscriptor generará el par de claves directamente en su sistema y se almacena en los servidores de Security Data.

### 4.1.3.Entrega de la Clave Pública al Emisor del Certificado

El envío de la clave pública a la AC para la generación del certificado se realiza mediante un formato estándar preferiblemente en formato PKCS#10 o X.509 autofirmado, utilizando un canal seguro para la transmisión.

### 4.1.4.Entrega de la Clave Pública de la AC a los Terceros que Confían en los Certificados

El certificado de las ACs de la cadena de certificación y su fingerprint (huella digital) estarán a disposición de los usuarios en la página web de Security Data Seguridad en Datos y Firma Digital.

### 4.1.5.Usos Admitidos de la Clave (campo KeyUsage de X.509v3)

Todos los certificados incluyen la extensión Key Usage y Extended Key Usage, indicando los usos habilitados de la claves.

Los usos admitidos de la clave para cada certificado están definidos en la Política de Certificación correspondiente.

### 4.2. Protección de la Clave Privada y Controles de Ingeniería de los Módulos Criptográficos

#### 4.2.1. Estándares para los Módulos Criptográficos

Los módulos criptográficos empleados para generar y almacenar las claves de las Autoridades de Certificación están certificados con la norma FIPS-140-2 nivel 3.

Las claves de los suscriptores de certificados reconocidos con DSCF y de operadores y administradores son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico CC EAL4+, FIPS 140-1 nivel 3, ITSEC E4 High u otro de nivel equivalente.

Los dispositivos criptográficos de custodia de la clave privada del suscriptor de certificados reconocidos con DSCF y del operador o administrador aportan un nivel de seguridad

#### 4.2.2. Control Multipersona (k de n) de la Clave Privada

El acceso a las claves privadas de las AC requiere el concurso simultáneo de tres dispositivos criptográficos diferentes de cinco posibles, protegidos por una clave de acceso.

### 4.3. Custodia de la Clave Privada

La clave privada de la AC raíz está custodiada por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multipersona detallado anteriormente. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

Las claves privadas de las AC Subordinadas están custodiadas en dispositivos criptográficos seguros certificados con la norma FIPS 140-2 nivel 3.

### 4.4. Copia de Seguridad de la Clave Privada

Existen unos dispositivos que permiten la restauración de la clave privada de la AC, que son almacenados de forma segura y sólo accesibles por personal autorizado según los roles de confianza, usando al menos un control dual en un medio físico seguro.

Las claves de la AC Raíz y AC Subordinada se pueden restaurar por un proceso que requiere la utilización simultánea de 3 de 5 dispositivos criptográficos (tarjetas).

Este procedimiento se describe en detalle en las políticas de seguridad de Security Data Seguridad en Datos y Firma Digital.

### 4.5. Archivo de la Clave Privada

La AC no archivará la clave privada de firma de certificados después de la expiración del periodo de validez de la misma.

Las claves privadas de los certificados internos que usan los distintos componentes del sistema de la AC para comunicarse entre sí, firmar y cifrar la información serán archivadas por un periodo de al menos 10 años, después de la emisión del último certificado.

Las claves privadas de los suscriptores pueden ser archivadas por ellos mismos, mediante la conservación del dispositivo de creación de firma u otros métodos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la clave pública, siempre que el dispositivo de custodia permita la operación.

### 4.6. Transferencia de la Clave Privada a o desde el Módulo Criptográfico

Existe un documento de ceremonia de claves de la AC donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

En otros casos, se podrá utilizar un fichero en formato PKCS12 para transferir la clave privada al módulo criptográfico. En todo caso el fichero estará protegido por un código de activación.

### 4.7. Método de Activación de la Clave Privada

Las claves de la AC Raíz se activan por un proceso que requiere la utilización simultánea de 3 de 5 dispositivos criptográficos (tarjetas). Las claves de las AC Subordinadas se activan por un proceso que requiere la utilización de 1 de 4 dispositivos criptográficos (tarjetas).

El acceso a la clave privada del suscriptor se realiza por medio de un PIN o de ser el caso por medio de la huella digital. El dispositivo con PIN tiene un sistema de protección contra intentos de acceso que lo bloquean cuando se introducen más de seis veces un código de acceso erróneo.

### 4.8. Método de Desactivación de la Clave Privada

La clave privada del suscriptor de certificados con DSCF quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura.

### 4.9. Método de Destrucción de la Clave Privada

Se destruirán físicamente o reinicializarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de la clave privada de firma de certificados de las ACs, o de los datos de activación de las mismas.

## 4.10. Otros Aspectos de la Gestión del Par de Claves

### 4.10.1. Archivo de la Clave Pública

La AC conservará todas las claves públicas durante el periodo exigido por la legislación vigente, cuando sea aplicable, o mientras el servicio de certificación este activo y 6 meses más como mínimo, en otro caso.

### 4.10.2. Periodos Operativos de los Certificados y Periodo de uso para el Par de Claves

El periodo de uso de un certificado será determinado por la validez temporal del mismo.

Un certificado no debe ser usado después del periodo de validez del mismo aunque la parte confiante pueda usarlo para verificar datos históricos teniendo en cuenta que no existirá un servicio de verificación en línea válido para ese certificado.

## 4.11. Datos de Activación

### 4.11.1. Generación e Instalación de los Datos de Activación

Los datos de activación son generados en el momento de inicialización del dispositivo criptográfico.

Si la inicialización se produce en una entidad externa, los datos de activación le serán entregados al suscriptor mediante un proceso que asegure la confidencialidad de los mismos ante terceros.

### 4.11.2. Protección de los Datos de Activación

Sólo el personal autorizado tiene conocimiento de los datos de activación de las claves privadas de la AC raíz y AC subordinadas.

Para los certificados de entidad final, una vez se ha hecho entrega del dispositivo y de los datos de activación, es responsabilidad del suscriptor de mantener la confidencialidad de estos datos.

## 4.12. Controles de Seguridad informática

La AC emplea sistemas fiables y productos comerciales para ofrecer sus servicios de certificación.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de Security Data Seguridad en Datos y Firma Digital en los siguientes aspectos:

1. Configuración de seguridad del sistema operativo.
2. Configuración de seguridad de las aplicaciones.
3. Dimensionamiento correcto del sistema.
4. Configuración de Usuarios y permisos.

5. Configuración de eventos de log.
6. Plan de backup y recuperación.
7. Configuración antivirus.
8. Requerimientos de tráfico de red.

La documentación técnica y de configuración de Security Data Seguridad en Datos y Firma Digital detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

#### 4.12.1. Requerimientos Técnicos de Seguridad Específicos

Cada servidor de la AC incluye las siguientes funcionalidades:

1. Control de acceso a los servicios de AC y gestión de privilegios.
2. Imposición de separación de tareas para la gestión de privilegios.
3. Identificación y autenticación de roles asociados a identidades.
4. Archivo del historial del suscriptor y la AC y datos de auditoría.
5. Auditoria de eventos relativos a la seguridad.
6. Auto-diagnóstico de seguridad relacionado con los servicios de la AC.
7. Mecanismos de recuperación de claves y del sistema de AC.

Las funcionalidades expuestas son provistas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

#### 4.12.2. Evaluación de la Seguridad Informática

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal es fácil debido al reducido número de personas que realizan sus trabajos en el centro de datos de Security Data Seguridad en Datos y Firma Digital.

### 4.13. Controles de Seguridad del Ciclo de vida

#### 4.13.1. Controles de Desarrollo de Sistemas

La AC posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

## 4.14. Controles de Gestión de Seguridad

### 4.14.1. Gestión de Seguridad

La AC desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un foro para la gestión de la seguridad.

La AC exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

### 4.14.2. Clasificación y Gestión de Información y Bienes

La AC mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de la AC detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, INTERNO y CONFIDENCIAL.

#### 4.14.2.1. Operaciones de Gestión

La AC dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En la documentación técnica de la AC y de procedimientos del CPD se desarrolla en detalle el proceso de gestión de incidencias.

La AC dispone de cajas de seguridad ignífugas para el almacenamiento de soportes físicos.

La AC tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

#### 4.14.2.2. Tratamiento de los Soportes y Seguridad

Todos los soportes serán tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

#### 4.14.2.3. Planning del Sistema

El departamento técnico de la AC mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

4.14.2.4. Reportes de Incidencias y Respuesta

La AC dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

4.14.2.5. Procedimientos Operacionales y Responsabilidades

La AC define actividades asignadas a personas con un rol de confianza distinto a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

4.14.2.6. Gestión del Sistema de Acceso

La AC realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el acceso al sistema está limitado a las personas autorizadas. En particular:

a) Gestión general de la AC:

1. Se dispone de controles basados en firewalls de alta disponibilidad.
2. Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.
3. La AC dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
4. La AC dispone de un procedimiento para asegurar que las operaciones se realizan respetando la política de roles.
5. Cada persona tiene asociado su identificador para realizar las operaciones de certificación según su rol.
6. El personal de la AC será responsable de sus actos, por ejemplo, por retener logs de eventos.

b) Generación del certificado:

1. Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.
2. La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la AC.

c) Gestión de la revocación:

1. Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular al sistema de revocaciones.
2. La revocación se refiere a la perdida de efectividad de un certificado digital de forma Permanente. La revocación se realizara mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de AC.

d) Estado de la revocación

1. La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

4.14.2.7. Gestión del Ciclo de Vida del Hardware Criptográfico

1. La AC se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.
2. El Hardware criptográfico está construido sobre soportes preparados para evitar cualquier manipulación.
3. La AC registra toda la información pertinente del dispositivo para añadir al catálogo de activos de Security Data Seguridad en Datos y Firma Digital, S.A.
4. El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.
5. Security Data Seguridad en Datos y Firma Digital realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.
6. El dispositivo criptográfico solo es manipulado por personal confiable.
7. La clave privada de firma de la AC almacenada en el hardware criptográfico se eliminará una vez se haya retirado el dispositivo.
8. La configuración del sistema de la AC así como sus modificaciones y actualizaciones son documentadas y controladas.
9. La AC posee un contrato de mantenimiento del dispositivo para su correcto mantenimiento. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

### 4.15. Controles de Seguridad de la Red

La AC protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma encriptada.

## 5. CAMBIO DE CLAVES DE LA CA

### 5.1. AC Raíz

Antes de que el certificado de la AC Raíz expire se realizará un cambio de claves (rekeying) y, en su caso, se introducirán cambios en el contenido del certificado que se ajusten mejor a la legislación vigente y la realidad de Security Data Seguridad en Datos y Firma Digital y del mercado. La AC antigua y su clave privada sólo se usarán para la firma de CRL's mientras existan certificados activos emitidos por la AC antigua. Se generará una nueva AC con una clave privada nueva.

La documentación técnica y de seguridad de la AC detalla el proceso de cambio de claves de la AC.

#### 5.1.1. AC Subordinada

En el caso de las AC subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves. Sólo cuando se realice el cambio se aplicará lo descrito en el punto anterior.

### 5.2. Plan de Recuperación de Desastres

#### 5.2.1. Procedimientos de Gestión de Incidentes y Vulnerabilidades

La AC ha desarrollado un plan de contingencias, detallado en el documento "Política de Seguridad", para recuperar todos los sistemas en menos de 48 horas, aunque se asegura la revocación y publicación de información del estado de los certificados en menos de 24 horas.

Cualquier fallo en la consecución de las metas marcadas por este plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

#### 5.2.2. Alteración de los Recursos Hardware, Software y/o Datos

En el caso de que tuviera lugar un incidente que alterara o corrompiera tanto recursos de hardware, software como datos, Security Data Seguridad en Datos y Firma Digital procederá según lo estipulado en el documento "Política de seguridad".

#### 5.2.3. Procedimiento de Actuación ante la Vulnerabilidad de la Clave Privada de una Autoridad de Certificación

El plan de contingencias de la jerarquía de Security Data Seguridad en Datos y Firma Digital trata el compromiso de la clave privada de la AC como un desastre.

En caso de compromiso de la clave privada de la AC, Security Data Seguridad en Datos y Firma Digital:

1. Informará a todos los suscriptores, usuarios y otras AC's con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web de la AC.
2. Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

#### 5.2.4. Continuidad del Negocio después de un desastre

La AC restablecerá los servicios críticos (Revocación y publicación de certificados revocados) de acuerdo con esta DPC dentro de las 24 horas posteriores a un desastre o emergencia imprevista tomando como base el plan de contingencias y continuidad de negocio existente.

La AC dispone de un centro alternativo, en caso de ser necesario, para la puesta en funcionamiento de los sistemas de certificación.

### 5.3. Cese de Actividad

#### 5.3.1. Autoridad de Certificación

Antes del cese de su actividad la AC realizará las siguientes actuaciones:

1. Proveerá de los fondos necesarios (para continuar la finalización de las actividades de revocación hasta el cese definitivo de la actividad, si es el caso).
2. Informará a todos los suscriptores, solicitantes, usuarios, otras AC's o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.
3. Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el
4. Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los certificados, especificando, en su caso, si se va a transferir la gestión y a quien.

#### 5.3.2. Autoridad de Registro

Ante el cese de una autoridad de registro de un colectivo específico, Security Data Seguridad en Datos y Firma Digital:

1. Dejará de emitir y renovar certificados de esa AR.
2. Revocará los certificados de operador de esa AR.
3. Revocará los certificados de suscriptor emitidos por esa AR salvo que expresamente se decida lo contrario.

## 6. REVISIONES

| **Documento:** **Declaración de Prácticas de Seguridad** | | | | | |
|---|---|---|---|---|---|
| **Revisión** | **1** | **2** | **3** | **4** | **5** |
| **Publicado** | **11/02/2011** | | | | |
| **Autor(es)** | **LV/XC** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **Fecha de revisión** | **23/08/2011** | | | | |
| **Revisado por** | **XC** | | | | |
| **Fecha aprobado** | **23/08/2011** | | | | |
| **Aprobado por** | **CS** | | | | |