ENTIDAD DE CERTIFICACIÓN DEL CONSEJO DE LA JUDICATURA ICERT-EC

DECLARACIÓN DE POLÍTICA DE SEGURIDAD

ICERT - EC ENTIDAD DE CERTIFICACIÓN Consejo de la Judicatura	***DECLARACIÓN DE POLÍTICA DE SEGURIDAD***	*Versión: 2.0*
		Fecha: 17-10-2014

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.0-3Declaración de Política de Seguridad	Declaración de Política de Seguridad Versión 1.0	Junio 2014	Octubre 2014

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
2014-06-04	1.0	**CONSEJO DE LA JUDICATURA**	
2014-10-17	2.0	**CONSEJO DE LA JUDICATURA** David Moncayo Flor Chancay	Se realizó actualización de la documentación presentada ante SENATEL para obtener la acreditación.

Firmas de responsabilidad

	Nombre	Cargo	Firma
Creado por:	David Moncayo	Experto en Proyectos DNTICs	
Creado por:	Flor Chancay	Analista 4 DNTICs	
Revisado por:	José Luis Medina	Subgerente de Proyectos DNTICs	
Aprobado por:	Vladimir Rodríguez	Subdirector Nacional de Infraestructuras, Servicios y Telecomunicaciones Administrador del Contrato 133-2013	

Código	Sustituye a:	Fecha de emisión:	Fecha de revisión:
00-14-A.05-DEC2.0-3Declaración de Política de Seguridad	Declaración de Política de Seguridad Versión 1.0	Junio 2014	Octubre 2014

Contenido

1. INTRODUCCIÓN

1.1 Objeto

La presente Declaración de Política de Seguridad ha sido desarrollada para especificar las condiciones y procedimientos relativos a los requisitos de seguridad de la infraestructura física y tecnológica y sobre la prestación de servicios que dispone Entidad de Certificación del Consejo de la Judicatura.

Se establece en el documento su ámbito de aplicación y los participantes de este proceso especificando sus responsabilidades.

1.2 Administración de la Declaración de Política de Seguridad

La Subdirección Nacional de Seguridad de la Información del Consejo de la Judicatura es la instancia que administra la presente Declaración de Política de Seguridad, encargada también de la elaboración, registro, mantenimiento y actualización de la DPC y las PC.

1.3 Procedimientos de aprobación de la Declaración de Política de Seguridad

La Declaración de Política de Seguridad es administrada por la Subdirección Nacional de Seguridad de la Información del Consejo de la Judicatura y aprobada por el Consejo de la Judicatura.

2. REFERENCIAS

La presente Declaración de Política de Seguridad (DPS) está fundamentada en las normas y en las recomendaciones contenidas en los siguientes documentos:

[DPC]	Declaración de Prácticas de Certificación de la ICERT-EC
[X.509]	Norma de la UIT que regula la interconexión de los sistemas de procesamiento de información con el fin de proporcionar servicios de directorio. Para su aplicación en Infraestructura de Clave Pública la norma desarrolla el marco al que deben regirse las Prácticas de Certificación y las Políticas de Certificado.
[RFC2560]	RFC 2560. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. June 1999.
[RFC3161]	RFC 3161. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). August 2001.
[RFC3629]	RFC 3629. UTF-8, a trasformation format of ISO 10646. November 2003.
[RFC5280]	RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. May 2008.
[CWA14167-1]	CWA 14167-1. Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. June 2003.
[LEY2002-67]	Ley No. 2002-67. Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Dada en la ciudad de San Francisco de Quito, Distrito Metropolitano, en la sala de sesiones del Pleno del Congreso Nacional del Ecuador, a 10 de abril de 2002.
[DECRETO3496]	Decreto No. 3496. Reglamento a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Dado en el Palacio Nacional, en Quito, a 12 de diciembre de 2002.
[DECRETO1356]	Decreto Nº 1356. Reformas al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Dado en el Palacio Nacional, en San Francisco de Quito, el día de 29 de septiembre de 2008.
[DECRETO867]	Decreto Nº 867. Reforma al Reglamento general a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos. Registro Oficial Nº 532. Quito, Lunes 12 de Septiembre de 2011.
[MINTEL181]	Ministerio de Telecomunicaciones y de la Sociedad de la Información. Acuerdo Nº 181. Dado en Quito, Distrito Metropolitano, a 15 de septiembre de 2011.
[P-CERT]	Firma Electrónica CJ Ecuador - Perfiles de certificado y CRL - versión 2.0. 17/10/2014.

3. DEFINICIONES Y SIGLAS

3.1 Definiciones

En el desarrollo de la presente DPS los términos empleados son los siguientes:

Suscriptor: Persona o entidad que solicita los servicios proporcionados por la Autoridad de Sellado de Tiempo del ICERT-EC.

Autoridad de Certificación (AC): Entidad encargada de emitir y revocar certificados digitales utilizados en firma electrónica y cuya clave pública está incluida en el.

Autoridad de Registro (AR): Entidad encarga de receptar las solicitudes de certificados, identificar y autenticar la información de los solicitantes de certificados, aprobar o rechazar las solicitudes de certificados, revocar o suspender certificados o en determinadas circunstancias, y aprobar o rechazar las solicitudes para renovar o volver a introducir su certificados.

CRL (Certificate Revocation List): Lista de certificados que han sido revocados.

Clave privada: En un criptosistema de claves públicas es la clave, de un par de claves de un usuario, que es conocida solamente por el usuario o titular del certificado.

Clave pública: En un criptosistema de claves públicas es la clave, de un par de claves de un usuario, que se conoce públicamente y aparece en un directorio público. La clave pública pertenece a la CA, se incluye en el certificado digital.

HSM (Hardware Security Module): Es el componente o dispositivo criptográfico utilizado para generar, almacenar y proteger claves criptográficas.

PKI (Public Key Infrastructure): La Infraestructura de Clave Pública es el conjunto de elementos informáticos (hardware y software), políticas y procedimientos necesarios para brindar servicios de certificación digital.

Cadena de confianza: También conocida como Jerarquía de Confianza la constituyen las autoridades de certificación relacionadas por la confiabilidad en la emisión de certificados digitales entre diferentes niveles jerárquicos. En el caso de la ICERT-EC existen la Autoridad de Certificación Raíz y la Autoridad de Certificación Subordinada.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de la Ley 2002 - 67.

Datos Personales Autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, hecho que debe constar expresamente señalado y ser aceptado por dicho titular.

OCSP (Online Certificate Status Protocol): Protocolo informático utilizado para comprobar el estado de un certificado digital en el momento en que es utilizado. Proporciona información actualizada y complementaria del estatus de certificados revocados.

OID (Object Identifier): El Identificador de Objetos constituye el valor de una secuencia de componentes variables utilizado para nombrar a casi cualquier tipo de objeto en los certificados digitales, tales como los componentes de los nombres distinguidos, DPC, etc.

PKCS (Public Key Cryptography Standard): Estándares de criptografía de claves públicas.

PKCS #10: Estándar de criptografía de clave pública utilizado para procesar la petición de un certificado y solicitar la generación de una clave.

PKCS #12: Estándar de criptografía de clave pública que define un formato de fichero utilizado para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

Política de Certificados: Documento que complementa la Declaración de Prácticas de Certificación y que contiene un conjunto de reglas que norman las condiciones de uso y los procedimientos seguidos por la ICERT-EC para la emisión de certificados, determinando la aplicabilidad de un certificado a una grupo o comunidad en particular y/o a una clase de aplicaciones con requisitos comunes de seguridad.

RFC (Request for comments): Publicaciones de *Internet Engineering Task Force* que en forma de memorandos contienen protocolos y procedimientos para regular el funcionamiento de Internet.

X.509: Estándar desarrollado por la UIT-T para infraestructuras de claves públicas que especifica entre otros temas, los formatos estándar para certificados de claves públicas y para la implementación de listas de certificados en revocación.

3.2 Siglas

AC: Autoridad de Certificación

AR: Autoridad de Registro

AV: Autoridad de Validación

C (Country) País: Atributo del DN de un objeto dentro de la estructura de directorio X.500.

CN (Common Name) Nombre Común: Atributo del DN de un objeto dentro de la estructura de directorio X.500.

CRL (Certificate Revocation List): Lista de Certificados Revocados

DN (Distinguished Name) Nombre distintivo: Identificación unívoca de una entrada dentro de un directorio X.500.

DNTIC'S: Dirección Nacional de Tecnologías de la Información y Comunicación

DPC: Declaración de Prácticas de Certificación

DPS: Declaración de Política de Seguridad

ICERT-EC: Entidad de Certificación Consejo de la Judicatura

HSM (Hardware Security Module): Módulo de Seguridad Criptográfica

LDAP: Lightweight Directory Access Protocol

O (Organization) Organización: Atributo del DN de un objeto dentro de la estructura de directorio X.500.

OCSP (Online Certificate Status Protocol): Protocolo de Estatus de Certificados en Línea

OID (Object Identifier): Identificador de Objetos

OU (Organizational Unit) Unidad Organizativa: Atributo del DN de un objeto dentro de la estructura de directorio X.500.

PC: Política de Certificado

PKCS (Public Key Cryptography Standard): Estándares de Criptografía de Clave Pública

PKI (Public Key Infrastructure): Infraestructura de Clave Pública

RFC (Request for Comments): Petición de comentarios

4. DECLARACIÓN DE POLÍTICAS DE SEGURIDAD

La ICERT-EC mantiene un control efectivo sobre la infraestructura PKI de manera que se proporciona la seguridad integral que garantiza los siguientes aspectos:

- El acceso físico y lógico a los sistemas y datos de la ICERT-EC restringido a personal autorizado.
- La continuidad de las claves y el manejo de las emisiones y operación de certificados.
- El desarrollo de los sistemas, mantenimiento y operaciones de la ICERT-EC que es manejado previo sistemas de autenticación y desarrollado para mantener la integridad de los sistemas de la ICERT-EC.
- La supervisión del funcionamiento del hardware y software de todos los equipos de la solución a través de un sistema de monitorización centralizado.

4.1 Seguridad de la clave privada de la ICERT-EC

La clave privada de la AC de la ICERT-EC se guarda en dispositivos HSM por personal autorizado según los roles de confianza y su recuperación es posible en caso de compromiso o desastre.

4.1.1 Procedimiento ante el compromiso de la clave privada

En el supuesto de revocación del certificado de la AC si la clave privada ha sido comprometida se procederá de acuerdo a lo siguiente:

- Informar al Organismo de Control y las entidades de confianza.
- Notificar a los suscriptores de certificados.
- Generar y publicar la correspondiente CRL.
- Suspender el funcionamiento de la entidad hasta el momento de generar un nuevo par de claves.
- Emitir nuevos certificados para los suscriptores.
- Destruir las claves pública y privada del certificado comprometido.

El certificado revocado permanecerá accesible en el repositorio de la ICERT-EC con el objeto de permitir la verificación de los certificados emitidos durante su período de funcionamiento.

4.2 Ataques externos

Los servicios de las interfaces web administración y operación y de operadores en los equipos de todos los componentes de la PKI y de la interfaz web de usuarios en los equipos de la AR aplican filtros a todas las páginas que puedan recibir parámetros a través del método GET, incluidos en la URL, para impedir que puedan contener código intruso, que pudiese producir, por ejemplo, un ataque de inyección SQL.

4.3 Sistemas de contingencia

La infraestructura de la ICERT-EC cuenta con equipos y mecanismos que permiten detectar y corregir fallas que afecten a su normal funcionamiento.

4.3.1 Tolerancia a fallos

El hardware de todos los equipos es tolerante a fallos en lo relativo a la fuente de alimentación, los discos duros y la interfaz de red, ya que cuenta sistemas redundantes de sus unidades, fuente de alimentación, discos duros e interfaces de red Ethernet con la misma dirección IP.

Cuenta también con equipos que serán utilizados en caso de falla de los equipos correspondientes en el entorno de producción mientras estos se reparan o sustituyen, así como para realizar tareas de mantenimiento y de verificación de funcionamiento.

4.3.2 HSM

Los HSM utilizados están certificados FIPS 140-2 Level 3 y/o Common Criteria EAL4+ y por lo tanto implementan todas las medidas de seguridad requeridas.

4.3.3 Protección de acceso al Sistema Operativo

La interfaz web de operadores de cada equipo incorpora funcionalidades de monitorización de su hardware y su software, y de configuración, administración y de actualización de su software, que evitan el acceso a su sistema operativo.

4.4 Seguridad en la Entidad

La seguridad de la ICERT-EC está sujeta a rigurosos procedimientos que norman la seguridad física, operacional y de procedimientos, para lo cual se dispone de un Manual de Seguridad de uso interno.

Los controles relativos a la seguridad en la operación y gestión de la ICERT-EC se rigen a lo establecido en la DPC y que tienen relación con:

- Control de riesgos
- Seguridad física
- Procedimientos
- Gestión de acceso a los sistemas
- Seguridad del personal

4.5 Seguridad del personal

Con el objeto de garantizar la idoneidad del personal que labora en la ICERT-EC así como la seguridad de las funciones encomendadas, se establecen las siguientes condiciones:

4.5.1 Requisitos

Los requisitos de calificación que cumple el personal que desempeña las distintas actividades en el proceso de certificación de la ICERT-EC son los siguientes:

- Título profesional o experiencia equivalente.
- Conocimiento y experiencia en certificados digitales y firma digital.
- Capacitación específica para la función desempeñada.

4.5.2 Verificación de antecedentes

El personal que desempeña las funciones operativas en el funcionamiento de la ICERT-EC deberá demostrar documentadamente su formación académica, su experiencia profesional y sus conocimientos y experiencia en el desarrollo de las funciones técnicas encomendadas.

4.5.3 Capacitación y entrenamiento

Adicionalmente al conocimiento de los documentos DPC y PC de la Entidad, los conocimientos de que dispone el personal se ajustan pero no se limitan a:

- Conceptos acerca de PKI
- Servicios prestados por la ICERT-EC
- Aspectos legales relativos a la prestación de servicios de certificación digital
- Seguridades física y lógica de las tareas y roles
- Procedimientos para la operación, administración y mantenimiento de acuerdo a cada rol específico.
- Gestión de incidencias
- Procedimientos para la operación en caso de desastre

4.6 Procedimientos para administrar incidentes

En caso de que se produjese un incidente que implique la indisponibilidad de la ICERT-EC se procederá a la ejecución del Plan de Continuación del Servicio, el mismo que garantiza que los servicios considerados como críticos por su requerimiento de disponibilidad estén disponibles en menos de 72 horas.

4.7 Recursos informáticos, software y datos corruptos

Si los componentes de la PKI (hardware), el software y/o los datos son alterados o se sospecha que son corruptos se suspenderá el funcionamiento de los servicios de la ICERT-EC hasta que sea restablecido el entorno seguro determinando cuáles certificados serán revocados. Si la

clave de la AC debe ser revocada, la nueva clave pública será suministrada nuevamente a los usuarios y los suscriptores serán nuevamente registrados.

4.8 Procedimientos ante compromiso de la clave privada de la AC

En el supuesto de revocación del certificado de la AC si la clave privada ha sido comprometida se generará y publicará la correspondiente CRL, se suspenderá el funcionamiento de la entidad y se procederá a generar una nueva entidad con un nuevo par de claves.

El certificado revocado permanecerá accesible en el repositorio de la ICERT-EC con el objeto de permitir la verificación de los certificados emitidos durante su período de funcionamiento.

Se informará a las entidades correspondientes.

4.9 Medidas para la corrección de vulnerabilidades detectadas

Los servicios de las interfaces web de administración y operación de todos los componentes de la infraestructura PKI y de la interfaz web de usuarios de la AR aplican filtros para impedir que puedan contener código intruso, que pudiese, por ejemplo, vulnerar la base de datos.

4.10 Capacidad de continuidad del negocio ante un desastre

La ICERT-EC garantiza su capacidad para asegurar la continuidad de sus operaciones si se produjera un desastre natural, como un terremoto que destruya las instalaciones, o desastre de cualquier tipo que comprometa su funcionamiento. Una infraestructura redundante existe para esta garantizar las operaciones.

4.11 Terminación o disolución de las autoridades de certificación y de registro

Las causas que pueden producir el cese de la actividad de la ICERT-EC son:

- Compromiso de la clave privada de la AC.
- Decisión propia de la ICERT-EC.

En el supuesto no consentido y muy remoto de disolución de la Entidad de Certificación ICERT-EC el procedimiento a seguir será determinado por la Subdirección Nacional de Seguridad de la Información.