ENTIDAD DE CERTIFICACIÓN DEL CONSEJO DE LA JUDICATURA ICERT-EC

DECLARACIÓN DE POLÍTICAS DE SEGURIDAD

SUBDIRECCIÓN NACIONAL DE SEGURIDAD DE LA INFORMACIÓN

JEFATURA DE FIRMA ELECTRÓNICA

FECHA: 29/04/2024

Código:	JFE-SNS-2024-014-AP
Versión:	3.0
Fecha de elaboración	29/04/2024
Creado por:	Alberto Pazmiño
Nivel de confidencialidad:	PÚBLICO

Historial de versiones:

Fecha	Versión	Creado por:	Descripción de la modificación
04/06/2014	1.0	CONSEJO DE LA JUDICATURA	Creación del documento.
17/10/2014	2.0	David Moncayo Flor Chancay	Se realizó actualización de la documentación presentada ante SENATEL para obtener acreditación.
29/04/2024	3.0	Alberto Pazmiño	Se realizó la actualización previa a la renovación de la acreditación de la entidad de certificación.

CONTENIDO

1 INTRODUCCIÓN

1.1. Objeto

La presente Declaración de Políticas 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.

Este documento es el compendio de los documentos relativos a los procesos que precautelan la seguridad de la información y seguridad informática de la Entidad de Certificación de Firma Electrónica

1.2. Administración de la Declaración de Políticas 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 Declaración de Prácticas de Certificación y las Políticas de Certificación.

1.3. Procedimientos de aprobación de la Declaración de Política de Seguridad

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

CWA14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. June 2003.

P-CERT: Perfiles de Certificado y CRL

RFC (Request for Comments) 2560: Internet *Public Key Infrastructure Online Certificate Status Protocol – OCSP. Protocolo de consulta en línea de Estado de Certificados OCSP. Junio 1999*.

RFC (Request for Comments) 3161: Internet X.509 v3 *Public Key Infrastructure – Time- StampProtocol (TSP)*. Agosto 2001.

RFC (Request for Comments) 3629: UTF-8 a transformation format of ISO 10646. Noviembre 2003.

RFC (Request for Comments) 3647: Internet X.509 *Public Key Infrastructure - Certificate Policy and Certification Practices Framework*, y constituye el marco que una Autoridad de Certificación (AC) emplea en la elaboración de la Declaración de las Prácticas y Políticas de Certificado relativas al ciclo de vida de los certificados para su emisión, suspensión, reactivación, revocación y renovación.

RFC (Request for Comments) 5280: Internet X.509 v3 *Public Key Infrastructure - Certificate Policy and Certification Practices Framework*, que regula el formato de los certificados emitidos por las AC Raíz y Subordinada y permite personalizar los campos y extensiones de cada tipo de certificado.

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.

Base Legal

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos publicada en el suplemento del RO No. 577 de 17 de abril de 2002 [Ley 2002 – 67].

- Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedido mediante Decreto 3496 publicado en el RO No. 735 de 31 de diciembre de 2002.

- Reformas al Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedidas mediante Decreto No. 1356 de 29 de septiembre de 2008, publicado en RO No. 440 de 6 de octubre de 2008.Reforma al

- Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expedida mediante Decreto No. 867 de 1 de septiembre de 2011.

- Acuerdo Ministerial No. 181 del Ministerio de Telecomunicaciones y de la Sociedad de la Información, de 15 de septiembre de 2011.

- Acuerdo Ministerial No. 12 del Ministerio de Telecomunicaciones y de la Sociedad de la Información, de 23 de mayo de 2016.

- Norma CGE, Suplemento Nº 257 - Registro Oficial febrero 2023

- Ley Orgánica de Transformación Digital y Audiovisual, Artículo 22.- Implementación de la firma electrónica, artículo 63 entre otras. LOTDA

3 DEFINICIONES Y SIGLAS

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

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

Autoridad de registro (RA): Encargada 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 digitales en determinadas circunstancias, y aprobar o rechazar las solicitudes para renovar certificados digitales.

CRL (En idioma inglés Certification 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 usuario que es conocida únicamente por el usuario o titular del certificado.

Clave pública: En un criptosistema de claves públicas, es la clave, de un par de claves de usuario, que se conoce públicamente y aparece en un directorio público. La clave pública pertenece a la Autoridad de Certificación (CA).

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

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

WAF (Firewall de aplicaciones web): Un firewall de aplicaciones web es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web.

Balanceador de carga: Hardware o software utilizado para la administración de sistemas informáticos cuyo principio es distribuir el trabajo entre varios servidores, procesos, discos u otros recursos informáticos.

Antivirus: Programas informáticos cuyo objetivo es detectar y eliminar virus informáticos.

Ataques DDoS: Ataque de denegación de servicio que causa que un servicio informático sea inaccesible a los usuarios legítimos del sistema.

Ataques MitM: Ataque informático por el cual un usuario no autorizado adquiere la capacidad de leer, insertar y modificar datos en tránsito de un servicio informático.

Ataque de Inyección SQL: Ataques orientados a realizar consultas no autorizadas en las Bases de datos de los sistemas informáticos.

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 se encuentra restringido a únicamente 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 del ICERT-EC que es manejado mediante 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 ICERT-EC

La clave privada de la Autoridad de registro de ICERT-EC se guarda en dispositivos HSM por personal autorizado según los roles de confianza y su recuperación es posible en caso de que haya sido comprometida o en situación de desastre.

4.1.1. Procedimiento en el caso de que se haya comprometido la clave privada

En el supuesto de revocación del certificado de la Autoridad de Certificación, si la clave privada ha sido comprometida se procederá de acuerdo de la siguiente forma:

- 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 la clave pública y privada del certificado comprometido.

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

4.2. Ataques externos

Los servicios de las interfaces web de administración y de operación de los equipos de todos los componentes de la PKI y de la interfaz web de usuarios en los equipos de la Autoridad de Registro están protegidos mediante procedimientos de gestión de usuarios y equipos como el WAF (Firewall de aplicaciones web), Firewall de red que cuenta con sistemas IPS, Anti-Bot, Application control, URL filtering, antivirus, Balanceador de carga para mejorar el rendimiento y disponibilidad de los servicios web; infraestructura que en conjunto impiden ataques como DoS, DDoS, ataques MitM e inyecciones SQL.

4.3. Sistemas de contingencia para continuidad del negocio ante un desastre

El ICERT-EC cuenta con un centro de datos de contingencia de similares características del centro de datos principal ubicado geográficamente en una posición estratégica en el caso de fallo total. Además, se cuenta con procedimientos de réplicas y respaldos que precautelan los datos de los usuarios y de la entidad de certificación. De esta manera ICERT-EC garantiza su capacidad para asegurar la continuidad de sus operaciones si se produjera un desastre natural que destruya las instalaciones del centro de datos principal y comprometa su funcionamiento.

En caso de que se produjese un incidente que implique la indisponibilidad de la entidad de certificación ICERT-EC se procederá con la ejecución del Plan de contingencias, el mismo que prevé que los servicios considerados como críticos por su requerimiento de disponibilidad estén habilitados en menos de 72 horas.

4.3.1. Tolerancia a Fallos

El hardware de todos los equipos está conectado en alta disponibilidad, según las políticas del Centro de Datos del Consejo de la Judicatura; esto permite que si un equipo falla en el entorno de producción otro equipo de similares características entra en operación hasta que el equipo sea reparado o sustituido; lo cual además facilita las tareas de mantenimiento y verificación de funcionamiento.

Por otra parte, todos los equipos son tolerante a fallos mediante sistemas redundantes en lo relativo a la fuente de alimentación, los discos duros y la interfaz de red.

4.3.2. HSM

Los HSM utilizados en la infraestructura PKI del ICERT-EC están certificados FIPS 140-2 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

El sistema operativo de los componentes de la infraestructura PKI están hardenizados según las mejores prácticas del mercado, además la interfaz web de operadores de cada equipo incorpora funcionalidades de monitorización de su hardware y software y se cuenta con un servicio de antivirus institucional que evitan el acceso a su sistema operativo.

4.4. Procedimiento ante un incidente de seguridad informático

Si los componentes de la PKI (hardware), software y/o los datos son alterados o se sospecha que han sido corrompidos, se suspenderá el funcionamiento de los servicios de ICERT-EC hasta que el servicio sea restablecido en un entorno seguro determinando cuales certificados serán revocados. Si la clave de la autoridad de registro debe ser revocada, la nueva clave pública será suministrada a los usuarios, y los suscriptores serán nuevamente registrados.

4.5. Seguridad física, operacional y de procedimientos de la Entidad de Certificación ICERT-EC

La seguridad de la entidad de certificación 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 Políticas 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 Declaración de Prácticas de Certificación y que tiene relación con:

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

4.6. Seguridad del personal que trabaja en ICERT-EC

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

4.6.1. 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 la gestión del ciclo de vida de certificados digitales y firma electrónica.
- Capacitación específica para la función desempeñada.

4.6.2. Verificación de antecedentes

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

4.6.3. Capacitación y entrenamiento

Además del conocimiento de los documentos de la Declaración de Prácticas de Certificación y de Políticas de certificación, los conocimientos que dispone el personal se ajustan, pero no se limitan a:

- Conceptos y definiciones acerca de la infraestructura PKI

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

4.7. Termino 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 la disolución de la Entidad de Certificación ICERT-EC, el procedimiento a seguir será determinado por la Subdirección Nacional de Seguridad de la Información de la Dirección Nacional de Tecnologías de la Información y Comunicaciones del Consejo de la Judicatura.

Firmas de Responsabilidad:

	Nombre	Cargo	Firma
Elaborado por:	Washington Alberto Pazmiño Vivanco	Analista 2	ALBERTO PAZMIÑO VIVANCO Firmado digitalmente por WASHINGTON ALBERTO PAZMIÑO VIVANCO
Revisado por:	Manuel Alejandro Pineda Serrano	Jefe Departamental de Seguridad de la Información	MANUEL ALEJANDRO PINEDA SERRANO Firmado digitalmente por MANUEL ALEJANDRO PINEDA SERRANO Fecha: 2024.04.29 12:32:39 -05'00'
Aprobado por:	Peter Antonio Cabrera Zambrano	Subdirector Nacional de Seguridad de la Información	PETER ANTONIO CABRERA ZAMBRANO Firmado digitalmente por PETER ANTONIO CABRERA ZAMBRANO Fecha: 2024.04.29 16:40:45 -05'00'

Fin del documento