DECLARACIÓN

DIRECCIÓN GENERAL DE REGISTRO CIVIL,
IDENTIFICACIÓN Y CEDULACIÓN

Políticas de Seguridad para la prestación de Servicios de Certificación de Información y Servicios Relacionados.

Dirección General de Registro Civil, Identificación y Cedulación
Versión 1.0
Enero 2021

	VERSIÓN1.0

Políticas de Seguridad para la prestación de Servicios de Certificación de Información y Servicios Relacionados

RUBRO	CARGO	FIRMA	FECHA
APROBADO POR:	Eco. Rodrigo Avilés **DIRECTOR GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN**		26/01/2021
REVISADO POR:	Ing. Adolfo Salcedo Gluckstadt **SUBDIRECTOR GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN**		26/01/2021
	Mgs. Jorge Trujillo Salazar. **COORDINADOR GENERAL DE PLANIFICACIÓN Y GESTIÓN ESTRATÉGICA**	Firmado electrónicamente por: JORGE REMIGIO TRUJILLO SALAZAR	26/01/2021
	Ing. Andrés Muñetón Achi. **COORDINADOR GENERAL DE SERVICIOS**	Firmado electrónicamente por: HOLBACH ANDRES MUNETON ACHI	26/01/2021
	Dra. Lucía Rosero Araujo. **COORDINADORA GENERAL DE ASESORÍA JURÍDICA**		26/01/2021
	Ing. Juan José Villota Holguín. **COORDINADOR GENERAL DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACION**		26/01/2021

	VERSIÓN1.0

Políticas de Seguridad para la prestación de Servicios de Certificación de Información y Servicios Relacionados

RUBRO	CARGO	FIRMA	FECHA
	Ing. Javier Jara **DIRECTOR DE SOPORTE E INTEROPERABILIDAD**	Firmado electrónicamente por: **RAUL JAVIER JARA**	26/01/2021
	Ing. Carlos Almeida **DIRECTOR DE INFRAESTRUCTURA Y OPERACIONES DE TI**		26/01/2021
	Ing. Gabriel Ruales **DIRECTOR DE GESTIÓN DE TI**		26/01/2021
	Ing. Ernie Donoso **DIRECTOR DE SERVICIOS DE IDENTIFICACIÓN Y CEDULACIÓN**	Firmado electrónicamente por: **ERNIE GUILLERMO DONOSO ORDONEZ**	26/01/2021
	Ing. Cesar Burneo **DIRECTOR DE SERVICIOS ELECTRÓNICOS**	Firmado electrónicamente por: **CESAR AUGUSTO BURNEO RIOFRIO**	26/01/2021
	Ing. Jacqueline Verdesoto **DIRECTORA DE SERVICIOS, PROCESOS Y CALIDAD**	Firmado electrónicamente por: **MARCIA JACQUELINE VERDESOTO BOLANOS**	26/01/2021
	Abg. Felipe Abarca **DIRECTOR DE ASESORÍA JURÍDICA**		26/01/2021

REGISTRO DE VERSIONES

Versión	**Descripción de la versión** (motivos y cambios)	**Realizado / Aprobado por**	**Fecha de elaboración**	**Documentos que se dan de baja con la vigencia de este documento**
1.0	Creación:	Elaborado por: Fausto Tabango **Analista de la Coordinación General de Servicios** Adrian Freire Diana Torres **Analistas Coordinación General de Tecnología de la Información y Comunicación** **Aprobado por** Eco. Rodrigo Avilés ***Director General de Registro Civil, Identificación y Cedulación***	Enero 2021	

ÍNDICE Y CONTENIDO

1. OBJETIVO

Especificar las condiciones y procedimientos relativos a la seguridad de la infraestructura de la Entidad de Certificación de Información y seguridad en la prestación de servicios de certificación de información y servicios relacionados con el certificado de firma electrónica.

2. MARCO NORMATIVO

2.1. DOCUMENTOS EXTERNOS

- Constitución de la República del Ecuador
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos, vigente.
- Reglamento a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos vigente.
- Resolución Arcotel-2021-0013, con la que la Agencia de Regulación y Control de las Telecomunicaciones Otorga la Acreditación como Entidad de Certificación de Información y Servicios Relacionados, a favor de la Dirección General De Registro Civil, Identificación Y Cedulación
- Esquema Gubernamental de Seguridad de la Información EGSI

2.2. DOCUMENTOS INTERNOS

- Procedimiento de servicios de Identificación y Cedulación
- Procedimiento de back de servicios de certificado de firma electrónica
- Declaración de Prácticas de Certificación

3. DECLARACIÓN DE POLÍTICAS DE SEGURIDAD

3.1. Procedimientos de Seguridad para el manejo de posibles eventos

3.1.1. Cuando la seguridad de la clave privada de la Entidad de Certificación de Información y Servicios Relacionados Acreditada se vea comprometida.

La Dirección General de Registro Civil, Identificación y Cedulación, cumple con controles físicos, lógicos, así como con procedimientos para fortalecer la seguridad en el resguardo de su clave privada. La descripción de estos controles y procedimientos se incluye a lo largo del presente DPS.

Los controles con los que cuenta la Infraestructura de Clave Pública la Entidad de Certificación de Información y Servicios Relacionados, están previstos desde el propio acceso al centro de datos donde se albergan los servidores y servicios, es decir que para acceder y llegar de manera presencial a los servidores y módulos HSM, una persona debe pasar varios filtros de seguridad, que se listan a continuación:

- **Controles Físicos.**
  - Controles de validación biométrica
  - Controles con tarjetas de proximidad
  - Controles a través de exclusas.
  - Control de acceso a la jaula de servidores mediante llaves.
  - Cámaras de video, el centro de datos como parte de la seguridad asociada a los servicios que provee, realiza grabaciones de las personas que acceden al centro de datos en distintos lugares y momentos.
  - El centro de datos registra la información del visitante, fotografía de la persona, fecha, hora de entrada, fecha hora de salida.

- **Controles lógicos**
  - Las credenciales de acceso a los servidores es información que administra y gestiona el personal de la DIGERCIC.
  - El esquema de direccionamiento es información que la DIGERCIC administra.

- **Procedimientos para acceder al centro de datos y servidores de la DIGERCIC**

    - Solicitar el acceso de manera explícita al área, rack y servidores de la infraestructura.
    - Las solicitudes son realizadas al centro de datos únicamente por personas registradas y autorizadas para este efecto.
    - La solicitud debe ser autorizada por personal de la DIGERCIC y personal del centro de datos.
    - Para el acceso al centro de datos se realiza una validación de la identificación de la persona a través de documentos aceptados para efectos de identificación.
    - El acceso es exclusivamente al espacio, área o equipos solicitados.
    - En todo momento la persona que accede es acompañada por personal del centro de datos.

La clave privada de la Entidad de Certificación de Información y Servicios Relacionados de la DIGERCIC se encuentra almacenada de manera segura mediante el uso de un módulo de seguridad de hardware (Hardware Security Module – HSM), que es un criptoprocesador seguro y resistente a la manipulación, diseñado específicamente para proteger el ciclo de vida de las claves criptográficas y ejecutar rutinas de encriptación y desencriptación, proporcionando un alto nivel de seguridad en términos de confidencialidad, integridad y disponibilidad de claves criptográficas y de cualquier dato sensible procesado.

El HSM que contiene la clave privada de la Entidad de Certificación de la DIGERCIC permanece fuera de línea, solo se pone en línea cuando es necesario realizar tareas específicas, generalmente limitadas a la emisión o reemisión de certificados, de esa manera se mantiene a salvo del acceso no autorizado y la administración se realiza exclusivamente por personal autorizado y capacitado de la DIGERCIC.

Asumiendo que los filtros de Seguridad mencionados líneas arriba, hubieran sido vulnerados y el atacante se encuentra frente a los servidores entonces, ¿Qué sucede con la Clave privada de la AC?

Ante este eventual escenario, no existe manera de obtener la clave o llave privada de la AC, porque se encuentra dentro del módulo de Seguridad HSM que tiene las siguientes características:

- Cumple con el FIPS 140-2 nivel 3, que entre sus principales características indica que las claves asociadas a una AC se generan dentro del HSM, se usan dentro del módulo y se desechan también en el mismo, dicho de manera simple la información de la Clave privada no saldrá del HSM.
- El acceso a esta clave o clave privada está protegido bajo un esquema de secreto compartido o mancomunado, es decir que cuando se crea la clave privada se define en ese momento un esquema de protección N/K donde N es el número requerido de (personas + Tarjeta inteligente) para autorizar el uso de la clave privada y por otro lado K es el total de (personas + Tarjeta inteligente) definido para proteger la clave privada.

Existe segregación de funciones entre el nivel de operadores y el nivel de Administradores, esta segregación es excluyente es decir que cada grupo de usuarios tiene capacidades específicas en el entorno de seguridad y ninguno tiene el control total de la información.

En el caso de que la clave privada de la Autoridad de Certificación de la DIGERCIC sea comprometida, se define el siguiente procedimiento:

- Suspender el funcionamiento de la Autoridad,
- Revocar los certificados que pudieran verse afectados,
- Generar y publicar la correspondiente CRL,

- Generar una nueva Autoridad con un nuevo par de claves,
- El certificado revocado permanecerá accesible en el repositorio de la DIGERCIC con el objeto de permitir la verificación de los certificados emitidos durante su período de funcionamiento.
- Finalmente, informar de los hechos a las partes afectadas que correspondan.

3.1.2. Cuando el sistema de seguridad de la Entidad de Certificación de Información y Servicios Relacionados Acreditada ha sido vulnerado.

La Entidad de Certificación de Información y Servicios Relacionados ha sido implementada bajo un esquema seguro e incorpora sistemas confiables que cumplen con las medidas de seguridad y procesos de evaluación continua establecidos por la Dirección General de Registro Civil, Identificación y Cedulación.

La infraestructura de red y comunicaciones utilizada por los sistemas de la AC está dotada de todos los mecanismos de seguridad necesarios para garantizar el servicio de manera confiable e íntegra.

Las vulneraciones al sistema de seguridad de la Entidad de Certificación son tratadas como incidentes de seguridad. En el caso de que el sistema de seguridad de la Entidad de Certificación sea vulnerado se define el siguiente procedimiento:

- Notificar el incidente de seguridad a través de la mesa de soporte
- Clasificar y asignar el incidente a la unidad de seguridad informática
- Coordinar, investigar y ejecutar acciones para la resolución del incidente de seguridad en coordinación con actores internos (DIGERCIC) y externos (PROVEEDOR)
- Elaborar un reporte o documentar el incidente incluyendo el análisis de la causa raíz del incidente y de ser el caso las recomendaciones de mejora.
- Notificar la resolución (exitosa o no exitosa) a los interesados
- Cerrar el incidente

3.1.3. Cuando se presenten fallas en el sistema de la DIGERCIC como entidad de certificación que comprometan la seguridad, disponibilidad y prestación de los servicios

En este aspecto la plataforma ofrece una colección de elementos que permitan minimizar el riesgo ante posibles escenarios de falla en la prestación de los servicios de Certificación.

En términos de Seguridad
De acuerdo a la descripción que se realizó en el apartado de controles de seguridad, la posibilidad de comprometer la seguridad de la clave privada es realmente inexistente por el esquema de seguridad que se utiliza con la segregación de roles, el uso de cuentas mancomunadas y el uso de tarjetas inteligentes protegidas por contraseñas.

En términos de disponibilidad
Para este escenario el planteamiento de la solución implica tolerancia a fallas, es decir la solución estará desplegada en dos entornos, el ambiente productivo y un sitio alterno remoto, adicionalmente es importante tomar en cuenta que en el ambiente productivo se contará con dos nodos en un esquema activo pasivo lo cual refuerza la disponibilidad de los servicios.

Es importante mencionar que el ambiente con tolerancia a fallas incluye todos los módulos y componentes de la solución.

Para el caso de las bases de datos existe adicionalmente a la redundancia de los servicios la replicación de la información entre el centro de datos de Producción y un sitio alterno remoto.

Otro aspecto para mantener la disponibilidad y continuidad de las operaciones de la AC es efectuar respaldos periódicos de la base de datos de certificados digitales emitidos, así como de recursos como archivos de configuración y elementos críticos para la continuidad de los servicios.

El esquema de alta disponibilidad incluye un sitio alterno remoto al cual se replica la información del sitio principal, y ante una eventual falla del sitio principal se sigue el siguiente procedimiento:

- Notificar a todas las partes implicadas acerca de la falla del sitio principal
- Autorizar el cambio al sitio secundario
- Suspender las operaciones en el sitio principal
- Configurar el sitio secundario para operar
- Notificar e iniciar las operaciones en el sitio secundario
- Resolver la falla en el sitio principal
- Autorizar el regreso al sitio principal
- Reiniciar las operaciones en el sitio principal
- Notificar a todas las partes implicadas

3.2. Plan de contingencia para garantizar la continuidad y disponibilidad de los servicios de identificación

La infraestructura de la AC de la DIGERCIC utiliza sistemas y productos confiables, los cuales están protegidos contra toda alteración con el fin de garantizar la seguridad técnica y criptográfica de los procesos de certificación que dan soporte a la operación de la Autoridad Certificadora y en base al Plan de Contingencia que mantiene la Coordinación General de TIC se podrá dar continuidad a los servicios en caso de alguna eventual falla, el documento es de uso interno y por aspectos de seguridad no se incluyen en esta declaración, sin embargo, se puede revisar directamente con el área correspondiente en la DIGERCIC.

La DIGERCIC notificará a todas las partes implicadas la interrupción de todo lo relacionado con su labor certificadora en el menor tiempo posible. Cuando se tenga conocimiento del fallo y se lo haya solventado; se notificará a todas las partes implicadas la restauración de su servicio de certificación.

3.3. Procedimientos y mecanismos de seguridad para resguardo y conservación segura de la información relativa a la emisión de certificados e información proporcionada por los usuarios.

La información relacionada con la emisión de los certificados y los datos de los usuarios se resguardan en la plataforma bajo los siguientes mecanismos:

Respecto a los Certificados emitidos:

- Todos los certificados emitidos por la Entidad de Certificación de Información y Servicios Relacionados se almacenan en la base de datos única asociada al servicio principal de la AC.
- La base de datos no es de propósito común, en todo caso es accesible única y exclusivamente a través de los servicios.
- Uno de los servicios que se incluyen, es el de consulta y solo a través de este medio se podrá consultar el certificado de un suscriptor.
- Es importante mencionar que los certificados solo incluyen la clave pública del usuario, nunca la clave privada del mismo.

El usuario conoce los datos que son entregados como parte del uso del certificado electrónico y en tal sentido acepta que los mismos sean sometidos a un proceso de validación.

La información con la que se alimenta el proceso de emisión de Certificados de Firma Electrónica, proviene de los sistemas de la DIGERCIC.

Los módulos y servicios que intervienen en la emisión de Certificados de Firma Electrónica están contemplados y cubiertos bajo los esquemas de auditoria que la DIGERCIC tiene para los servicios y procesos sustantivos.

La DIGERCIC como mecanismos de conservación segura de la información relativa a la emisión de certificados e información proporcionada por los usuarios, mantiene controles de seguridad para:

- El manejo seguro de respaldos de las aplicaciones y bases de datos
- Controles físicos y lógicos de su infraestructura
- Conservación de registros de auditoría, etc.

La generación de los registros de auditoria se realiza de forma automática por cada transacción realizada por la Autoridad Certificadora Raíz y la Autoridad Certificadora Subordinada, el módulo funciona a través de la emisión de recibos criptográficos (bajo los estándares RFC3161, RFC5305 y RFC5816), esto garantiza la integridad de las operaciones y de la base de datos para todo el ciclo de vida de los certificados durante:

- Emisión
- Revocación
- Renovación