ABC
Declaración de Políticas y Prácticas (DPS) para las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC)

Versión más reciente: 17 de octubre de 2011

Este documento establece las políticas y prácticas de las DNSSEC, vigentes en las operaciones del Registro de ABC. En él se describen las prácticas y disposiciones que ABC utiliza en la prestación de servicios de gestión de llaves criptográficas y firmado de la zona.

Control de Documentos

Información y Seguridad de Documentos

Realizado por	Responsable de hechos	Responsable de documentos
Director de operaciones	Director de operaciones	Director de operaciones

Clasificación de seguridad	Nombre del archivo
Abierto	ABC_DPS.doc

Aprobado por

Fecha	Nombre	Función
16 de diciembre de 2010	Bert	Director de operaciones
8 de septiembre de 2011	Kathie	Director de operaciones
12 de septiembre de 2011	Kathie	Director de operaciones

Auditorías

Fecha	Versión	Nombre	Descripción
16 de diciembre de 2010	1.0	BK	Declaración de Políticas y Prácticas (DPS)
7 de febrero de 2011	1.0	KW	Ronda de Consulta Interna
1 de abril	1.0	KW	Edición menor
15 de julio de 2011	1.1	KW	Corrección de errores de traducción
3 de agosto de 2011	1.1	RL	Observaciones de EDG
8 de septiembre de 2011	1.1	RL	Versión final
12 de septiembre de	1.1	RL	Actualizaciones debido a los cambios en la política de ABC

2011			

Contenido

1 Introducción

Este documento ("DPS") es la declaración de políticas y prácticas de seguridad de ABC aplicables a sus operaciones de DNSSEC. Este documento se ajusta al borrador de la Solicitud de comentarios (RFC) sobre la versión 4 del Marco de Declaración de Políticas y Prácticas de DNSSEC, al momento de la última revisión de la DPS. La DPS es uno de los varios documentos relevantes para el funcionamiento de la zona de cc. Otros documentos relevantes son el estándar de seguridad de referencia de ABC, la política de seguridad de la información de ABC y el plan de contingencia de negocios de ABC. En algunos casos se hace referencia a estos documentos, que pueden no constituir información pública (sólo para uso interno).

1.1 Descripción general

DNSSEC constituye un conjunto de nuevos registros de DNS y modificaciones del protocolo que proporcionan autenticación del firmante de los datos del sistema de nombres de dominio (DNS), verificación de la integridad de los datos del DNS en caso de modificación, el no repudio de los datos del DNS que han sido firmados y la denegación autenticada de la existencia de registros de DNS. Los datos del DNS asegurados con DNSSEC son firmados criptográficamente e incorporan criptografía asimétrica en la jerarquía del DNS, por lo que la confianza sigue la misma cadena que el árbol del DNS, lo cual significa que la confianza se origina en la raíz y es delegada en la misma forma que el control de un dominio. Es importante notar que DNSSEC no mejora la disponibilidad de datos del DNS, ni proporciona ningún tipo de confidencialidad.

La DPS constituye sólo uno de una serie de documentos relacionados con las operaciones de DNSSEC de ABC. Otros documentos incluyen documentación auxiliar sobre seguridad y operaciones, que complementan a la DPS estableciendo requisitos más detallados, tal como la Guía de referencia para las ceremonias de gestión de las llaves criptográficas, que presenta detallados procedimientos operacionales de gestión de las llaves. En algunos casos, cuando la inclusión de detalles no es relevante para el propósito de la DPS, la DPS hace referencia a estos documentos auxiliares para prácticas detalladas y específicas de la implementación de las políticas de ABC.

1.2 Nombre e identificación del documento

Título del documento: Declaración de Prácticas (DPS)
Versión: 1.1
Creado: 15 de julio de 2011
Actualizado: 17 de octubre de 2011

1.3 Comunidad y aplicabilidad

A continuación se establecen las funciones y la delegación de responsabilidad. La relación entre el registro y un registrador está regulada en el Acuerdo entre registro-registrador, el cual puede encontrarse completo en <inserte URL>.

1.3.1 Registro

ABC (*ABC Incorporated*) es responsable por el dominio <TLD>. ABC administra los nombres de dominio que identifican zonas subyacentes en la zona de <TLD>. Esto significa que ABC gestiona todos los datos que están relacionados con un nombre de dominio.

El registro es responsable de generar pares de llaves y proteger la confidencialidad del componente privado de dichas llaves para la llave para la firma de llaves (KSK) y llave para la firma de zona (ZSK). El registro también es responsable de firmar de manera segura todos los registros del DNS autorizados en la zona de <TLD>.

Por último, el registro es responsable de asegurar la exportación segura y la publicación de los anclajes de confianza (TA) y el registro y mantenimiento de los registros firmantes de delegación (DS) en la zona padre.

1.3.2 Registradores

Un registrador es la parte responsable de la administración y gestión de los nombres de dominio, en nombre de los registrantes. El registrador se encarga del registro, mantenimiento y gestión de un nombre de dominio del registrante, y está acreditado por ABC.

El registrador es responsable por la identificación segura del registrante de un dominio. El registrador es responsable de agregar, eliminar y actualizar los registros DS especificados para cada dominio, a solicitud del registrante.

1.3.3 Registrante

Un registrante es la persona física o jurídica que posee el control de un nombre de dominio. Los registrantes son responsables de generar y proteger sus propias llaves, y de registrar y mantener los registros DS a través del registrador.

Los registrantes son responsables de renovar las llaves si sospechan que éstas no son ya mas confidenciales o se han perdido.

1.3.4 Usuario de confianza

El usuario de confianza (o parte que confía) es la entidad que depende de DNSSEC, tal como los servidores de DNS recursivos y otras aplicaciones que realizan la validación de firmas de DNSSEC. El usuario de confianza debe configurar y actualizar adecuadamente los anclajes de confianza, según corresponda. Los usuarios de confianza también deben estar informados de cualquier evento que esté relacionado con la gestión de DNSSEC en el dominio <TLD>.

1.3.5 Aplicabilidad

Cada registrante es responsable de determinar el nivel de protección pertinente para su dominio. Esta DPS es exclusivamente aplicable al dominio <TLD> y describe los procedimientos, controles de seguridad y las prácticas aplicables en la gestión y el empleo de llaves y firmas, para la firma de zona <TLD>.

Con el apoyo de esta DPS, el usuario de confianza debe evaluar su propio entorno y sus amenazas y vulnerabilidades asociadas para determinar el nivel de confianza que puede asignar a las TA del dominio <TLD>, así como el nivel de riesgo que está dispuesto a aceptar.

1.4) Administración de especificaciones

La presente DPS pueden ser ocasionalmente actualizado por la Autoridad de Gestión de Políticas (PMA) de DNSSEC de ABC, incluyendo, sin limitación, las revisiones que reflejen modificaciones en los sistemas o procedimientos que afectan al contenido de esta DPS o a las operaciones de las DNSSEC de ABC. La PMA es responsable por la gestión de la DPS y debe ser considerada como el punto de contacto para todos los asuntos relacionados con la DPS.

1.4.1 Gestión del documento

ABC Incorporated
PO Box 19036
Millbrae, California 94030 EE.UU.

1.4.2 Información de contacto

Autoridad de Gestión de Políticas de DNSSEC
ABC Incorporated
PO Box 19036
Millbrae, California 94030 EE.UU.
Teléfono: +1 202 709 5262
Fax: +1 707 885 1704
Reg. Corp. N º: 20-04712337
https://www.ABC
dnssec-pma@ABC

1.4.3 Procedimientos para cambios de especificación

Las enmiendas a la presente DPS son realizadas por la Autoridad de Gestión de Políticas (PMA) de DNSSEC de ABC. Las modificaciones son realizadas tanto en forma de enmiendas al documento existente como en forma de publicación de una nueva versión del documento. Esta DPS y sus modificaciones son publicados en <inserte URL>.

Sólo resulta aplicable la versión más reciente de esta DPS, y cualquier enmienda a la misma según lo publicado por ABC. ABC se reserva el derecho a ocasionalmente modificar o replantear la DPS y cualquiera de sus modificaciones, sin previo aviso. Todos los cambios son efectivos inmediatamente después de ser publicados por ABC. La decisión de designar a las enmiendas como materiales o no materiales queda a criterio exclusivo de PMA.

2 Publicación y Repositorios

2.1 Publicación del sitio

ABC publica la información relevante de las DNSSEC en el sitio web de ABC, en <inserte URL>. La versión electrónica de esta DPS en esta dirección específica constituye la versión oficial de dicho documento. Las notificaciones relevantes de DNSSEC en ABC son distribuidas por e-mail procedente de <inserte dirección de correo de la lista de anuncios de DNS de ABC>.

2.2 Publicación de llaves para la firma de llaves (KSK)

ABC publica las KSKs en la forma de una DNSKEY (llave del sistema de nombres de dominio) y DS, de la siguiente manera:

- Sitio web de ABC, https://www.ABC/dnssec/public-key-for-dnssec/
- En la zona padre de <TLD> (sólo DS)

La parte pública de la KSK de ABC podrá ser adicionalmente firmada con su clave PGP oficial.

2.3 Control de acceso

La información relativa a las DNSSEC publicada en https://www.ABC/dnssec está disponible para el público en general.

3 Requisitos Operacionales

3.1 Significado de nombres de dominio

Un nombre de dominio es un identificador único, que a menudo se asocia con servicios tales como web o correo electrónico. La solicitud de registro bajo el dominio <TLD> está abierta para todas las personas físicas y jurídicas que tengan un número de registro civil o corporativo, que puedan ser identificados a través de la lista del registro, en los registros de una autoridad u organización con una denominación similar a la de una autoridad. El enfoque de "por orden de llegada" se aplica al nuevo registro de nombres de dominio, lo cual significa que los nombres de dominio son asignados en el orden en que las solicitudes son recibidas por el registro ABC.

En otras palabras, no tiene que existir una correlación entre el nombre de dominio y el registrante de ese dominio.

3.2 Activación de las DNSSEC para una zona hija

DNSSEC es activado por la existencia de al menos un registro DS para la zona que está siendo enviada desde el registrador al registro, y por lo tanto está siendo publicada en el DNS, el cual estableció una cadena de confianza para la zona hija (dominio del registrante). El registro presume que el registro DS es correcto y no realizará ningún tipo de verificación.

3.3 Identificación y autenticación del administrador de una zona hija

El registrador es responsable de identificar en forma segura y de autentificar al registrante, a través de un mecanismo adecuado y en cumplimiento con el contrato entre ABC y el registrador.

3.4 Aprovisionamiento de registros DS (firmante de delegación)

El registro acepta los registros de DS a través de la interfaz EPP (protocolo de aprovisionamiento extensible) de cada registrador. El registro DS debe ser validado y enviado en el formato indicado en el RFC 5910. Se pueden registrar hasta <máximo de registros DS aceptados> registros DS por cada nombre de dominio.

3.5 Método para probar la posesión de la llave privada

El registro no realiza ningún tipo de control con el objetivo de validar al registrante como administrador de una llave privada. El registrador es responsable de realizar los controles que sean requeridos o considerados como necesarios.

3.6 Eliminación de registros DS

Un registro DS es dado de baja a través de una solicitud de eliminación transmitida del registrante al registrador y luego al registro. La eliminación de todos los registros DS asociados con una zona hija desactiva el mecanismo de seguridad de DNSSEC para esa zona hija.

3.6.1 Autoridad para solicitar eliminaciones

Sólo el registrante —o la parte formalmente designada por el registrante mediante la asignación del rol Contacto Técnico o Contacto Administrativo—, tiene la facultad de solicitar la eliminación de los registros DS.

3.6.2 Procedimiento de eliminación

El registrante —o el representante del registrante en la forma de contacto técnico o administrativo—, es quien solicita al registrador la eliminación del registro DS. El registrador sólo puede hacer esto en nombre del registrante. Desde que la solicitud de eliminación del registro DS es recibida por ABC, la ejecución del cambio en la zona no toma más que hasta la siguiente generación de zona. Posteriormente, toma hasta dos veces el TTL (tiempo de vida), más el tiempo de distribución antes de que los cambios sean desplegados. Todo el procedimiento puede tomar un máximo de <inserte el cálculo aplicable a TLD> para completarse.

3.6.3 Procedimiento de emergencia para eliminaciones

Si el registrante se encuentra en una situación en la cual no puede contactarse con el registrador, ABC puede eliminar el registro DS, siempre que dicho registrante cuente con una identificación segura.

4 Controles de Instalaciones, Administración y Funcionamiento

4.1 Controles físicos

ABC ha implementado controles de seguridad física para cumplir con los requisitos especificados en esta DPS.

4.1.1 Ubicación y construcción de las instalaciones

ABC ha establecido dos centros de operaciones en pleno funcionamiento y geográficamente dispersos: uno primario y uno de respaldo, separados por al menos 5 kilómetros de distancia.

La instalación de respaldo contiene un conjunto completo de sistemas críticos del registro, cuya información es continuamente actualizada a través de la réplica automática de las operaciones de la instalación primaria. Todos los componentes del sistema están protegidos dentro de un perímetro físico con un control de acceso y sistema de alarma operados por ABC.

La instalación de operaciones de respaldo cumple con los estándares mínimos aplicados a la instalación principal en términos de seguridad física, alimentación de energía, medio ambiente y protección contra incendios y agua.

4.1.2 Acceso físico

El acceso físico al entorno protegido está limitado al personal autorizado. Todas las entradas son registradas y el ambiente es monitoreado en forma permanente.

4.1.3 Energía y aire acondicionado

La energía es proporcionada a las instalaciones operativas a través de varias fuentes separadas. En el caso de cortes de energía, la energía es proporcionada por UPS hasta que los sistemas de energía de respaldo comiencen a generar electricidad. Los sistemas de energía de respaldo tienen la capacidad de suministrar electricidad para los recursos críticos, durante al menos cuatro días.

4.1.4 Exposición al agua

Las instalaciones implementan mecanismos de detección y protección ante inundaciones.

4.1.5 Prevención y protección contra incendios

Las instalaciones están equipadas con sistemas de detección y extinción de incendios. Las instalaciones están equipadas con extintores automáticos de extinción seca y suelos ignífugos. Cada habitación constituye una celda de incendios independiente.

4.1.6 Medios de almacenamiento

Las directrices del Registro ABC para la clasificación de la información definen los requisitos impuestos para el almacenamiento de datos sensibles.

4.1.7 Eliminación de residuos

El desecho de medios de almacenamiento y otros materiales que pueden contener información confidencial se realiza mediante eliminación segura, ya sea por parte del Registro ABC como de un tercero contratado.

4.1.8 Respaldo remoto

Ciertos datos críticos también se almacenan de forma segura utilizando una instalación de almacenamiento de terceros. El acceso físico a las instalaciones de almacenamiento está limitado al personal autorizado. La instalación de almacenamiento está geográfica y administrativamente separada de las otras instalaciones de ABC.

4.2 Controles Procedimentales

4.2.1 Posiciones de confianza

Las posiciones de confianza están en manos de personas que son capaces de afectar el contenido del archivo de zona, la entrega de los anclajes de confianza o la generación o el uso de llaves privadas. Las posiciones de confianza son:

1. Administrador de sistemas (SA)
2. Oficial de seguridad (SO)
3. Controlador de seguridad (SC)

4.2.2 Cantidad de personas requeridas por tarea

En un momento dado, como respaldo, debe haber al menos dos personas dentro de la organización por cada posición de confianza indicada en el punto 4.2.1.

La activación del HSM (módulo de seguridad del hardware) requiere la presencia de tres personas; una de cada posición.

La generación de llaves requiere la presencia de tres personas; una de cada posición.

La exportación y el control de los anclajes de la confianza requieren la presencia de tres personas; una de cada posición.

Ninguna de las operaciones anteriormente mencionadas podrá desarrollarse en la presencia de personas no autorizadas.

4.2.3 Identificación y autenticación para cada posición

Sólo las personas que han firmado un acuerdo de confidencialidad y un acuerdo de reconocimiento de sus responsabilidades para con el Registro, pueden ocupar posiciones de confianza. Antes de que una persona reciba sus credenciales para acceder al sistema, se debe presentar una identificación válida. Refiérase a
4.3.2.

4.2.4 Separación de responsabilidades

Las posiciones de confianza mencionadas en 4.2.1 no podrán ser ocupadas simultáneamente por una misma persona. La separación de responsabilidades se ve forzada debido a que el Oficial de Seguridad no tiene acceso físico exclusivo a las instalaciones operativas, y a que el Administrador de sistema o el Controlador de seguridad no tienen acceso al material de activación de la tarjeta inteligente del HSM.

4.2.5 Otras personas autorizadas

Otras personas autorizadas incluyen:

- Testigo interno, IW
- Testigo externo, EW
- Administrador de ceremonia, CA
- Maestro de ceremonias, MC

4.3 Controles del personal

4.3.1 Requisitos de calificaciones, experiencia y antecedentes

Los aspirantes a cubrir cualquiera de las posiciones de confianza deben ser capaces de presentar pruebas en cumplimiento de los requisitos de antecedentes y calificaciones.

4.3.2 Procedimientos de verificación de antecedentes

La evaluación de los antecedentes es realizada por la posición de Recursos humanos (HR) de ABC. El control de los antecedentes y calificaciones incluye la revisión de:

- Currículum vitae de los candidatos,
- Empleos anteriores,
- Referencias (no confidencial y otras),
- Documentación acreditativa de la educación pertinente y completa,
- Situación financiera a través de una verificación de crédito.

Para calificar para cualquiera de las posiciones de confianza, estos controles no pueden revelar ninguna discrepancia que indique la falta de idoneidad, conforme lo determinado por la cadena ABC.

4.3.3 Requisitos de capacitación

El Registro proporciona la capacitación pertinente y necesaria en relación a los procedimientos, administración y sistemas técnicos asociados a cada posición de confianza. La formación incluye:

- Funcionamiento de .cc (equivalente al programa de capacitación para la certificación de registradores).
- El alcance, las áreas de responsabilidad y autoridad de la posición.
- Concepto de la separación estructural de las posiciones y el acceso
- Competencia técnica básica en el DNS y las DNSSEC (para el SO y el SC)
- Competencia técnica avanzada en el DNS y las DNSSEC (para SA)
- Conocimientos básicos de seguridad de la información
- Administración, procedimientos y listas de verificación.
- Procedimientos para la gestión de incidentes
- Procedimientos para la gestión de crisis.

El conocimiento del titular de la posición de confianza es evaluado por la posición de HR de ABC.

4.3.4 Frecuencia y requisitos de reentrenamiento

Las personas que ocupan posiciones de confianza están sujetas a la evaluación continua y sometidas al requisito de llevar a cabo capacitaciones complementarias, de forma periódica o en caso de grandes cambios, conforme lo determinado por ABC.

4.3.5 Frecuencia y secuencia de rotación de posiciones

Ocasionalmente, algunas responsabilidades operativas específicas rotan entre las personas que ocupan posiciones de confianza, conforme al criterio exclusivo de ABC. ABC puede reemplazar a cualquier persona de confianza, en cualquier momento.

4.3.6 Sanciones por acciones no autorizadas

Las acciones disciplinarias derivadas de actividades no autorizadas están reguladas en el acuerdo de responsabilidad. La negligencia grave puede llevar a la rescisión y a la responsabilidad por daños y perjuicios.

4.3.7 Requisitos para el personal contratado

En ciertas circunstancias, ABC podrá necesitar el uso de contratistas como un suplemento de los empleados de tiempo completo. Estos contratistas firman los mismos acuerdos de responsabilidad que los empleados de tiempo completo. Los contratistas que no han sido objeto de una verificación de antecedentes y capacitación, y por lo tanto no están cualificados para una posición de confianza, no podrán participar en las actividades indicadas en el punto 4.2.2.

4.3.8 Documentación proporcionada al personal

Las operaciones de IT (tecnología de la información) de ABC proporcionan la documentación necesaria para que todo el personal lleve a cabo su tarea de trabajo de una manera segura y satisfactoria.

4.4 Procedimientos de bitácora para auditorías

La información relativa a las actividades que toman lugar y al estado de funcionamiento y de seguridad del sistema es recolectada de forma automática y continua. Esta información de registro en bitácora se utiliza en el monitoreo del desempeño, la disponibilidad y el correcto funcionamiento del sistema, con fines estadísticos y para la investigación de presuntas infracciones de las políticas, procedimientos y normas de ABC.

Además de los sensores automáticamente recolectados y la información del estatus del proceso, los registros de bitácora también incluyen anotaciones diarias, listas de comprobación y demás documentos que sean necesarios para reconstruir una imagen completa del estado del sistema o de un calendario de eventos.

El objetivo final del registro de bitácora es permitir el entendimiento completo por parte del auditor investigador y poder atribuir cualquier fallo que pudiese producirse, después del hecho. A tal fin, la información de registro de bitácora identifica a los individuos, componentes y procesos y ofrece tanta información como sea posible acerca de lo que ocurrió, cuándo y con qué propósito.

4.4.1 Tipos de eventos registrados en bitácora.

Los siguientes eventos están incluidos en el registro de bitácora:

- Todos los tipos de actividades que involucran al HSM, tal como la generación de llaves, activación de llaves y la firma y exportación de llaves.
- Acceso remoto, exitoso y no exitoso.
- Operaciones privilegiadas.
- Ingreso a las instalaciones o acceso al equipo.
- Sensor de entrada que indica la actividad o un cambio de estado.

Las entradas del sensor que indican la inactividad o continuidad del estado podrán ser publicadas en tiempo real, aunque pueden, a discreción de ABC, ser suprimidas del archivo a largo plazo.

4.4.2 Frecuencia del registro de procesos en bitácora.

Los registros en bitácora se analizan en forma continua a través de controles manuales y automatizados. En los procesos que incluyen la generación de llaves, reinicios del sistema y anormalidades detectadas, se realizan controles específicos.

4.4.3 Período de retención para la información de bitácora para auditoría

La información de la bitácora se archiva por no menos por diez años.

4.4.4 Protección de bitácora para auditoría

Toda la información de registro electrónico se almacena en al menos dos instalaciones de ABC. El sistema de bitácora está protegido contra accesos y manipulación no autorizada de la información.

4.4.5 Procedimientos de respaldo de bitácora para auditoría

Toda la información de bitácora electrónica está respaldada de manera segura, en forma separada del sistema y en un lugar seguro. Toda la información de bitácora en papel es escaneada y transferida electrónicamente a al menos dos instalaciones de ABC.

4.4.6 Sistema de recolección para auditoría

La información de bitácora eléctronica es transferida a través de un sistema de recolección externa al sistema de generación de llaves. Los registros manuales son registrados en papel, escaneados y transferidos manualmente al sistema de recolección. Los documentos originales son archivados en una caja de seguridad a prueba de fuego.

4.4.7 Notificación sobre el registro en bitácora a las partes involucradas

Al personal involucrado se le notifica que el registro en bitácora está siendo realizado. No se requiere aviso alguno que deba darse a ningún individuo, organización, dispositivo o aplicación por causar o aparecer en un evento de registro, ni ninguna de dichas partes tiene ningún derecho especial para ver los registros.

4.4.8 Evaluaciones de vulnerabilidad

Todas las anomalías en la información de registro del bitácora son investigadas, a fin de analizar las posibles vulnerabilidades.

4.5 Compromiso y recuperación en caso de desastres

4.5.1 Procedimientos de gestión ante incidentes y compromisos

Se define como incidentes a todos los eventos de seguridad reales y percibidos que causen o pudiesen comprometer la integridad del sistema de DNSSEC o causar interrupciones o defectos en el servicio.

Los incidentes se manejan de acuerdo con los procedimientos de gestión de incidentes de ABC. El procedimiento de gestión de incidentes incluye la investigación de la causa del incidente, la

identificación de cualquier efecto del incidente, y la evaluación de las medidas para evitar que el incidente se repita.

En el caso de sospecharse que alguna llave privada está comprometida o siendo mal utilizada, la llave es inmediatamente renovada de conformidad con los procedimientos descriptos en la sección 4.5.3.

4.5.2 Recursos informáticos, software o datos dañados

En el caso de daño/corrupción, se inician los procedimientos de gestión de incidentes y se toman las medidas apropiadas conforme lo establecido en la presente DPS.

4.5.3 Procedimientos de compromiso de clave privada para entidades

La sospecha de que una llave privada ha sido comprometida o mal utilizada conduce a una renovación de llave controlada, de la siguiente manera:

- Si se sospecha que una ZSK está comprometida, se genera una nueva ZSK y una serie de registros de recursos (RRsets) de DNSKEY firmada. La vieja llave se programará para ser eliminada del conjunto de llaves, tan pronto como sea posible (por ejemplo, pasa el tiempo suficiente para el vencimiento de los cachés). Si se sospecha que una ZSK está comprometida o ha sido revelada a terceros no autorizados, esto será notificado a través de los canales indicados en el apartado 2.1.
- Si se sospecha que una KSK está comprometida, se generará y pondrá en uso inmediato una nueva llave, en forma paralela a la llave antigua. La antigua KSK permanecerá en su lugar y será utilizada para firmar conjuntos de llaves hasta el momento en que se pueda considerar lo suficientemente seguro eliminar la llave, teniendo en cuenta el riesgo de interrupciones del sistema en relación con el riesgo que presenta la llave comprometida. Una renovación de KSK en curso, siempre es notificada a través de los canales indicados en el apartado 2.1.
- Si se pierde una KSK, una KSK nueva será inmediatamente generada y se crearán RRsets de DNSKEY firmada a partir de la ZSK vigente. Los registros DS asociados a la nueva KSK son presentados a la Autoridad de números asignados en Internet (IANA) como una solicitud de emergencia para añadirse al conjunto de DS vigente. Tan pronto como ha sido publicado y propagado a través de los cachés, ABC comienza a utilizar los nuevos RRsets de DNSKEY. En ese momento, esto se dará a conocer a través de los canales indicados en el apartado 2.1. Los usuarios de confianza con una configuración estática del anclaje de confianza de ABC, deben agregar la nueva KSK como un anclaje de confianza extra, por adelantado. Durante el tiempo hasta que la renovación ocurre, el conjunto de llaves se mantendrá estático y cualquier renovación programada de la ZSK se pospondrá hasta después del cambio de la KSK.

4.5.4 Continuidad del negocio y capacidad de recuperación de IT en caso de desastres

El plan de contingencia del registro garantiza que la producción crítica y operativa pueda ser trasladada entre las dos instalaciones operativas en cuatro horas. Las instalaciones son equivalentes en términos de protección física y logística. La información se replica entre las

instalaciones. Los componentes auxiliares frecuentemente utilizados y los componentes críticos de hardware son almacenados *in situ*, en las instalaciones de cada operación.

El plan de contingencia y las rutinas son probados con regularidad. Las pruebas y ensayos realizados son registrados y posteriormente evaluados.

El plan de contingencia incluye:

- Quién decide sobre la activación de un procedimiento de recuperación de emergencia.
- Cómo y dónde se convocará la gestión de crisis.
- Activación de las operaciones de respaldo.
- Activación del plan de comunicación pública.
- Designación de un Gerente de tareas.
- Criterios para la restauración de las operaciones normales.

4.5.5 Rescisión de la entidad

Si por alguna razón el registro debe descontinuar las DNSSEC para la zona ABC y retornar a una posición sin firma, esto se llevará a cabo de manera ordenada en la cual el público será informado. Si las operaciones serán transferidas a otra parte, el registro participará en la transición, con el fin de que sea lo más suave posible.

5 Controles de seguridad técnica

5.1 Generación e instalación de pares de llaves

5.1.1 Generación de pares de llaves

La generación de llaves se realiza en un computador portátil sin disco duro y sin conexión a Internet, utilizando un generador de números aleatorios basado en hardware.

La llave resultante se almacena en varios módulos de seguridad basados en tarjetas inteligentes de hardware (HSM) que son administrados por personal capacitado y designado específicamente para posiciones de confianza.

La generación de llaves se lleva a cabo cuando sea necesario y debe ser realizada por tres personas (SA, SC y SO) mediante un trabajo al unísono. Estas personas están presentes durante toda la operación.

Todo el procedimiento de generación de llaves es registrado y grabado en video, parte de lo cual se realiza electrónicamente y otra parte manualmente, en papel y mediante el trabajo del Testigo interno (IW).

5.1.2 Entrega de llave pública

El componente público de cada KSK generada se exporta desde el sistema de firma y es verificado por el SO y el SA. El SO es responsable de la publicación del componente público de

la KSK, de una manera segura y conforme a lo establecido en el apartado 2.2. El SA es responsable de asegurar que las llaves publicadas son las mismas que las que se generaron.

5.1.3 Propósitos del uso de llaves

Las llaves generadas por las DNSSEC no se utilizan nunca para ningún otro propósito o fuera del sistema de firma. Una firma creada por una clave de DNSSEC, ya sea para una ZSK o KSK tiene un período de validez máximo de 15 días y las firmas se actualizan al menos 5 días antes de su vencimiento.

5.2 Protección de claves privadas y controles de ingeniería de los módulos criptográficos

La generación de llaves KSK y ZSK se realiza se realiza en un computador portátil sin disco duro y sin conexión a Internet, utilizando un generador de números aleatorios basado en hardware.

La llave privada KSK resultante es importada en múltiples tarjetas inteligentes FIPS (Estándar de procesamiento de información federal) 140-2, basadas en HSMs. La llave privada es posteriormente destruida.

Después de la generación, todas las operaciones de firma criptográfica de KSK se realizan en la tarjeta inteligente HSM y ninguna llave privada se encuentra desprotegida fuera de la tarjeta inteligente.

1. Después de la generación de la llave ZSK, las operaciones de firma criptográfica de ZSK se llevan a cabo utilizando la llave privada basada en software, en un servidor protegido física y lógicamente, fuera de la red.

5.2.1 Normas y controles del módulo criptográfico

El sistema utiliza una tarjeta inteligente HSM, conforme a los requisitos FIPS 140-2 nivel 3 (a través de la interfaz PKCS11) para la generación de números aleatorios de KSK y ZSK, el almacenamiento de KSK y las operaciones de firma. Las operaciones ZSK emplean el software OpenSSL y BIND.

5.2.2 Control multipersonal de llaves privadas (m-de-n)

Se requiere que un SO active el módulo, el cual a su vez requiere el acceso físico que únicamente puede ser realizado por el SA y el SC juntos.

5.2.3 Custodia de llaves privadas

El Registro no utiliza un sistema de custodia de llaves.

5.2.4 Respaldo de llaves privadas

Las KSKs se almacenan en forma de inextraíble en tres tarjetas inteligentes HSMs en envases a prueba de manipulación, guardadas en forma segura dentro de cajas de seguridad en cada centro de operaciones. Luego de generarse, las ZSKs son almacenadas y sincronizadas entre los sitios, de manera encriptada.

5.2.5 Archivo de llaves privadas
Las llaves privadas que ya no se utilizan no son archivadas de ninguna otra manera que como copias de seguridad.

5.2.6 Método para la activación de llaves privadas
Las llaves privadas son activadas mediante el desbloqueo de la tarjeta inteligente HSM. Un SA y SC proporcionan al SO con el acceso al HSM. El SO ingresa un PIN para la tarjeta inteligente HSM, a través de una consola.

5.2.7 Método de desactivación de llaves privadas
El HSM se bloquea si el sistema de firma es apagado o reiniciado.

5.2.8 Método de destrucción de llaves privadas
Las llaves privadas no se destruyen. Después de su vida útil, se retiran del sistema de firma.

5.3 Otros aspectos de la gestión de pares de llaves

5.3.1 Archivo de llaves públicas
Las llaves públicas son archivadas junto con la información pertinente para la trazabilidad en el sistema, tal como los datos de bitácora.

5.3.2 Períodos de uso de las llaves
Las llaves dejan de ser válidas a medida que son retiradas de la producción. Las llaves viejas no se reutilizan.

5.4 Datos de activación
Los datos de activación toman la forma de un PIN personal controlado por cada SO y utilizado para activar la tarjeta inteligente HSM.

5.4.1 Generación de datos e instalación de activación
Cada SO es responsable de crear sus propios datos de activación de conformidad con los requisitos aplicables de ocho caracteres de distinta naturaleza.

5.4.2 Protección de los datos de activación
Cada SO es responsable de proteger sus datos de activación de la mejor manera posible. En caso de sospecha de que los datos de activación estuviesen comprometidos, el SO debe cambiarlos inmediatamente.

5.5 Controles de seguridad informática
Todos los componentes críticos de los sistemas del registro se colocan en las instalaciones de seguridad de la organización, conforme a lo establecido en el apartado 4.1. El acceso al sistema operativo del servidor se limita a las personas que así lo requieran para su trabajo, es decir, los administradores del sistema. Todos los accesos son registrados y trazables a nivel individual.

5.6 Controles de seguridad de red

El Registro cuenta con redes lógicamente seccionada que se dividen en varias zonas de seguridad con comunicaciones seguras entre ellas. El registro se realiza en los servidores de seguridad. Toda la información confidencial que es transferida a través de la red de comunicaciones, está siempre protegida por una fuerte encriptación.

5.7 Sello de tiempo

ABC obtiene la hora que es atribuible a los servidores horarios del Instituto Nacional de Normas y Tecnologías de los EE.UU. Los sellos de tiempo son registrados en hora UTC y están estandarizados para toda la información de registro y el tiempo de validez de las firmas.

5.8 Controles técnicos del ciclo de vida

5.8.1 Controles del desarrollo del sistema

Todo el código fuente es almacenado en un sistema de control de versiones. El archivo del código fuente es regularmente respaldado y las copias se almacenan por separado, en una caja fuerte a prueba de fuego.

El modelo de desarrollo de ABC está basado en estándares de la industria, e incluye:

- Requisitos de especificación funcional completa y seguridad documentada,
- Diseño arquitectónico documentado, en base a un diseño modular natural del sistema,
- Búsqueda continua de minimizar la complejidad,
- Prueba sistemática y automatizada y pruebas de regresión,
- Emisión de distintas versiones del software,
- Constantes seguimientos de calidad para los defectos detectados.

5.8.2 Controles de gestión de seguridad

Los registros de autorización se mantienen y corroboran regularmente. El registro también lleva a cabo auditorías regulares de la seguridad del sistema. El registro se prepara y mantiene un plan de seguridad del sistema, el cual está basado en el análisis de riesgos recurrentes.

5.8.3 Controles de seguridad del ciclo de vida

El sistema firmante está diseñado para requerir un mantenimiento mínimo. Las actualizaciones críticas para la seguridad y las operaciones del sistema firmante se aplican después de la prueba y aprobación formales. El origen de todo el software y el firmware está bien autenticado por los medios disponibles.

Los componentes críticos del hardware del sistema firmante se adquieren directamente del fabricante y se transportan en bolsas a prueba de manipulación, hasta su destino en las instalaciones de seguridad. Todo el hardware es retirado de servicio dentro de la expectativa especificada para su ciclo de vida.

6 Firma de zona

6.1 Longitud y algoritmos de las llaves

La longitud y algoritmos de las llaves deben ser lo suficientemente largas para su propósito designado durante la vida útil de cada llave.

Los algoritmos deben ser estandarizados por la IETF (Fuerza de trabajo en ingeniería de Internet), y estar a disposición del público.

Para la KSK se utiliza el algoritmo RSA con una longitud de llave de 2048 bits, y de 1024 bits para la ZSK.

6.2 Denegación de existencia autenticada

El registro utiliza los archivos de salida NSEC3, conforme lo especificado en la RFC 5155.

6.3 Formato de la firma

Las firmas son generadas utilizando la operación RSA en una función hash criptográfica con SHA256.

6.4 Renovación de clave para la firma de zona (ZSK)

La renovación de ZSK se realiza cada XX días.

6.5 Renovación de clave para la firma de clave (KSK)

La renovación de KSK se realiza cuando sea necesario.

6.6 Tiempo de vida de la firma y frecuencia de nueva firma

Las RRsets son firmadas con ZSKs que tienen un período de validez de XX días. La nueva firma toma lugar al menos cada XX días. Las firmas KSK son actualizadas cada XX días, de acuerdo con una programación predefinida.

6.7 Verificación del conjunto de llaves de firma de la zona

Antes de la publicación de información de la zona en Internet y a fin de garantizar la firma y el período de validez de las claves, se realizan controles con la DNSKEY.

6.8 Verificación de los registros de recursos

El Registro comprueba que todos los registros de recursos (RR) sean válidos, conforme a las normas vigentes antes de su distribución.

6.9 Tiempo de vida (TTL) de los registros de recursos

DNSKEY = 3.600 segundos. SOA = 172,800 segundos. RRSIG hereda el TTL de la serie RRset que lo firma.

7 Auditoría de Cumplimiento

En una auditoría se pueden utilizar documentos auditados (políticas, procedimientos y requisitos) así como cualquier otra información pertinente y verificable.

7.1 Frecuencia de las auditorías de cumplimiento de la entidad

La necesidad de auditorías es decidida por ABC. Algunas de las circunstancias que puedan suponer un requisito de auditoría son:

- Anomalías recurrentes.
- Cambios significativos hechos a nivel de gestión, en la organización o en los procesos.
- Otras circunstancias, tal como la competencia entre el personal, equipo nuevo u otros cambios importantes.

7.2 Identidad/calificación del auditor

El auditor debe ser capaz de demostrar su competencia en la seguridad de IT, el DNS y las DNSSEC.

7.3 Relación del auditor con la parte auditada

Para la auditoría se designa a un gerente de auditoría externa. Cuando sea necesario, el gerente de auditoría podrá ser contratar expertos con conocimientos especializados específicos. El gerente de auditoría es responsable de la implementación durante toda la auditoría.

7.4 Temas cubiertos por la auditoría

Las tareas asignadas al gerente de auditoría, incluyen garantizar lo siguiente:

- Que ABC posee las competencias adecuadas.
- Que los auditados estén informados acerca del tema de la auditoría y estén preparados antes de la auditoría.
- Que los procedimientos de seguimiento de los resultados estén en orden.

7.5 Acciones tomadas como resultado de una deficiencia

El gerente de auditoría informa inmediatamente a la gerencia de ABC acerca de cualquier anomalía.

7.6 Comunicación de los resultados

El gerente de auditoría presenta un informe escrito de los resultados de la auditoría a la gerencia de ABC, a más tardar 30 días naturales después de la concluida dicha auditoría.

8 Asuntos Legales

8.1 Tarifas

Actualmente, el registro ABC no cobra a los registradores ninguna tarifa por los registros DNSSEC.

8.2 Confidencialidad de la información personal

La información personal será tratada de acuerdo con la <hacer referencia a la ley de protección de datos, si aplica> y en virtud de otros acuerdos.

8.2.1 Responsabilidad de Proteger la Información Personal

Esto está regulado por los términos de registración de ABC y por las condiciones del acuerdo entre el registro y el registrador.

8.2.2 DIVULGACIÓN DE INFORMACIÓN PERSONAL A LAS AUTORIDADES JUDICIALES

En caso de petición directa, se podrá tomar decisiones relativas a la divulgación de información personal a las autoridades judiciales. La cuestión de divulgación se decide sobre una base de caso por caso, de conformidad con la Ley de seguridad y privacidad de datos personales de los EE.UU. Las decisiones son tomadas por el departamento legal de ABC.

8.3 Limitación de responsabilidad

La responsabilidad de los daños entre el registro y el registrador está regulada por <hacer referencia al acuerdo o contrato entre el Registro y el Registrador>

La responsabilidad de ABC ante daños a registrantes está regulada por <hacer referencia al acuerdo o contrato del Registro>, aplicables al dominio ABC.

---------- O ----------

TODOS LOS SERVICIOS PRESTADOS POR O EN NOMBRE DE ABC DE O EN CONEXION CON ESTA DPS (colectivamente, "Servicios") SE PROPORCIONAN "TAL CUAL", "DONDE ESTÁN" Y "COMO ESTÁN DISPONIBLES" CON TODOS LOS RIESGOS Y FALLOS QUE PUEDAN ESTAR ASOCIADOS EN RELACIÓN CON LOS MISMOS. SIN PERJUICIO DE CUALQUIER DISPOSICIÓN CONTRARIA, ABC NO HACE NINGUNA REPRESENTACIÓN, GARANTÍA NI CONVENIO DE NINGÚN TIPO CON RESPECTO A CUALQUIER SERVICIO, YA SEA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITACIONES, A CUALQUIER GARANTÍA DE COMERCIALIZACIÓN, IDONEIDAD PARA UN PROPÓSITO PARTICULAR O NO INFRACCIÓN. POR LA PRESENTE ABC RENUNCIA A TODAS Y CADA UNA DE LAS REPRESENTACIONES, GARANTÍAS Y CONVENIOS, RESPONSABILIDAD DE CADA PERSONA QUE UTILIZA, DEPENDE O SE BENEFICIA A PARTIR DE CUALQUIER SERVICIO.

SIN PERJUICIO DE CUALQUIER DISPOSICIÓN CONTRARIA, ABC NO SE RESPONSABILIZA DE NINGUNA MANERA, YA SEA EN LA LEY Y/O EN EQUIDAD, POR NINGÚN RECLAMO Y/O DAÑO, INCLUYENDO, SIN LIMITACIONES, CONSECUENTE, INCIDENTAL, INDIRECTO, PUNITIVO, EJEMPLAR O DAÑO ESPECIAL (INCLUYENDO, SIN LIMITACIÓN, RESPONSABILIDADES POR DAÑOS RELACIONADOS CON LA PÉRDIDA DE BENEFICIOS, PÉRDIDA DE DATOS O PÉRDIDA DE BUENA VOLUNTAD) DERIVADOS, EN RELACIÓN CON, O DE CUALQUIER OTRA MANERA RELACIONADO CON CUALQUIER SERVICIO, YA SEA POR CONTRATO, RESPONSABILIDAD CIVIL EXTRACONTRACTUAL O CUALQUIER OTRA CAUSA DE ACCIÓN DE CUALQUIER TIPO.

8.4 Vigencia y rescisión

8.4.1 Período de validez

Esta DPS se aplica hasta nuevo aviso.

8.4.2 Vencimiento de validez

Esta DPS es válida hasta que sea reemplazada por una versión actualizada o nueva, conforme lo establecido en el apartado
1.4.3.

8.4.3 Resolución de disputas

Cualquier disputa o conflicto que resulte del presente Acuerdo, debe ser presentada ante el <tribunal competente de aplicación en cada país>

8.4.4 Legislación aplicable

Esta DPS estará regida por las leyes <país de aplicación>, excluyendo sus principios de conflictos jurídicos.

- FIN -