

Declaración de prácticas de DNSSEC para la zona TLD/GTLD de VeriSign

Declaración de prácticas de DNSSEC para la zona TLD/GTLD de VeriSign.

**Versión 1.0**

**Fecha de entrada en vigor: 28 de julio de 2011**

Resumen

El presente documento es la declaración de prácticas de DNSSEC de VeriSign para la zona TLD/GTLD. Declara las prácticas y disposiciones que se tienen en cuenta para la prestación de servicios de firma y distribución para la zona TLD/GTLD que incluyen entre otros, a modo ejemplificativo, la emisión, gestión, modificación y distribución de claves del DNS. VeriSign es el operador de registro delegado para la zona TLD/GTLD en virtud del contrato con la Internet Corporation for Assigned Names and Numbers (Corporación de Internet para Nombres y Números Asignados, ICANN, en sus siglas en inglés).

Nota sobre derechos de autor

Derechos de autor (c) 2011 VeriSign Inc. Todos los derechos reservados. Nota sobre marcas comerciales VeriSign es una marca comercial registrada de VeriSign, Inc.

VeriSign, Inc.

21345 Ridgetop Circle Dulles, VA 20166 EE. UU.

+1 (703) 948-3200

[http://www.VeriSigninc.com](http://www.verisigninc.com/)

**Índice**

1. [INTRODUCCIÓN 7](#_bookmark0)
	1. [Consideraciones generales 7](#_bookmark1)
	2. [Nombre e identificación del documento 7](#_bookmark2)
	3. [Comunidad y aplicabilidad 8](#_bookmark3)
		1. [Jefe de la zona TLD/GTLD 8](#_bookmark4)
		2. [Administrador de la zona TLD/GTLD 8](#_bookmark5)
		3. [Mantenedor de la zona TLD/GTLD 8](#_bookmark6)
		4. [Operadores del servidor de TLD/GTLD 8](#_bookmark7)
		5. [Operador de claves de firma de claves de la zona TLD/GTLD 8](#_bookmark8)
		6. [Operador de claves de firma de zona TLD/GTLD 8](#_bookmark9)
		7. [Jefe de la zona subordinada 9](#_bookmark10)
	4. [Administración de especificaciones 9](#_bookmark11)
		1. [Organización de administración de especificaciones 9](#_bookmark12)
		2. [Información de contacto 9](#_bookmark13)
		3. [Procedimiento de especificación de cambios 10](#_bookmark14)
2. [PUBLICACIÓN Y ARCHIVOS 10](#_bookmark15)
	1. [Archivos 10](#_bookmark16)
	2. [Publicación de las claves de firma clave 10](#_bookmark17)
	3. [Controles de acceso a los archivos 10](#_bookmark18)
3. [REQUISITOS OPERATIVOS 11](#_bookmark19)
	1. [Significado de los nombres de dominio 11](#_bookmark20)
	2. [Activación de las DNSSEC para la zona subordinada 11](#_bookmark21)
	3. [Identificación y autenticación del jefe de la zona subordinada 11](#_bookmark22)
	4. [Inscripción de los registros del firmante por delegación (DS, en sus siglas en inglés) 11](#_bookmark23)
	5. [Eliminación del registro del DS 11](#_bookmark24)
		1. [Quién puede solicitar la eliminación 11](#_bookmark25)
4. [CONTROLES DE INSTALACIONES, DE GESTIÓN Y OPERATIVOS 12](#_bookmark26)
	1. [Controles físicos 12](#_bookmark27)
		1. [Ubicación del emplazamiento y construcción 12](#_bookmark28)
		2. [Acceso físico 12](#_bookmark29)
		3. [Electricidad y aire acondicionado 12](#_bookmark30)
		4. [Exposiciones al agua 12](#_bookmark31)
		5. [Prevención y protección contra incendios 13](#_bookmark32)
		6. [Medios de almacenamiento 13](#_bookmark33)
		7. [Eliminación de residuos 13](#_bookmark34)
		8. [Copia de seguridad ex situ 13](#_bookmark35)
	2. [Controles de procedimiento 13](#_bookmark36)
		1. [Funciones de confianza 13](#_bookmark37)
		2. [Número de personas necesarias por tarea 14](#_bookmark38)
		3. [Identificación y autenticación de cada función 14](#_bookmark39)
		4. [Tareas que requieren separación de funciones 14](#_bookmark40)
	3. [Controles de personal 14](#_bookmark41)
		1. [Requisitos de titulación, experiencia y de permisos de entrada 14](#_bookmark42)
		2. [Procedimientos de comprobación de los antecedentes 15](#_bookmark43)
		3. [Requisitos de formación 15](#_bookmark44)
		4. [Periodicidad de la retención y requisitos 16](#_bookmark45)
		5. [Periodicidad y secuencia de la rotación de puestos de trabajo 16](#_bookmark46)
		6. [Sanciones por actuaciones no autorizadas 16](#_bookmark47)
		7. [Requisitos de contratación del personal 16](#_bookmark48)
		8. [Documentación facilitada al personal 16](#_bookmark49)
	4. [Procedimientos de auditoría de inicio de sesión 16](#_bookmark50)
		1. [Tipos de sucesos registrados 16](#_bookmark51)
		2. [Periodicidad del registro de procesamiento 17](#_bookmark52)
		3. [Período de conservación del registro de auditoría 17](#_bookmark53)
		4. [Protección del registro de auditoría 17](#_bookmark54)
		5. [Procedimientos de copia de seguridad de los registros de auditoría 17](#_bookmark55)
		6. [Sistema de recopilación de auditorías 18](#_bookmark56)
		7. [Notificación a la persona que ha ocasionado un suceso 18](#_bookmark57)
		8. [Evaluación de la vulnerabilidad 18](#_bookmark58)
	5. [Compromiso y recuperación ante desastres 18](#_bookmark59)
		1. [Procedimientos de gestión de incidentes y compromisos 18](#_bookmark60)
		2. [Recursos informáticos, software y datos dañados 18](#_bookmark61)
		3. [Procedimientos de compromiso de clave privada de entidad 18](#_bookmark62)
		4. [Capacidad de recuperación ante desastres informáticos y continuidad de la actividad 19](#_bookmark63)
	6. [Terminación de la entidad 20](#_bookmark64)
5. [CONTROLES DE SEGURIDAD TÉCNICA 20](#_bookmark65)
	1. [Generación e instalación de par de claves 20](#_bookmark66)
		1. [Generación de par de claves 20](#_bookmark67)
		2. [Entrega de clave pública 20](#_bookmark68)
		3. [Generación y comprobación de la calidad de los parámetros de la clave pública 20](#_bookmark69)
	2. [Protección de la clave privada y controles de la ingeniería de los módulos criptográficos 21](#_bookmark70)
		1. [Normas y controles de los módulos criptográficos 21](#_bookmark71)
		2. [Control multipersonal de la clave privada (m-de-n) 21](#_bookmark72)
		3. [Depósito de la clave privada 21](#_bookmark73)
		4. [Copia de seguridad de la clave privada 21](#_bookmark74)
		5. [Almacenamiento de la clave privada en el módulo criptográfico 21](#_bookmark75)
		6. [Trabajo de archivo de las claves privadas 22](#_bookmark76)
		7. [Transmisión de la clave privada al o del módulo criptográfico 22](#_bookmark77)
		8. [Método de activación de la clave privada 22](#_bookmark78)
		9. [Método de desactivación de la clave privada 22](#_bookmark79)
		10. [Método de destrucción de la clave privada 22](#_bookmark80)
	3. [Otros aspectos de la gestión del par de claves 22](#_bookmark81)
		1. [Trabajo de archivo de las claves públicas 22](#_bookmark82)
		2. [Períodos de uso de las claves 22](#_bookmark83)
	4. [Datos de activación 23](#_bookmark84)
		1. [Generación e instalación de los datos de activación 23](#_bookmark85)
		2. [Activación de la protección de los datos 23](#_bookmark86)
	5. [Controles de seguridad informática 23](#_bookmark87)
	6. [Controles de seguridad de la red 23](#_bookmark88)
	7. [Sello de tiempo 24](#_bookmark89)
	8. [Controles técnicos del ciclo de vida 24](#_bookmark90)
		1. [Controles de desarrollo del sistema 24](#_bookmark91)
		2. [Controles de gestión de la seguridad 24](#_bookmark92)
		3. [Controles de seguridad del ciclo de vida 24](#_bookmark93)
6. [FIRMA DE LA ZONA 24](#_bookmark94)
	1. [Longitud y algoritmos de las claves 25](#_bookmark95)
	2. [Negación de existencia autenticada 25](#_bookmark96)
	3. [Formato de firma 25](#_bookmark97)
	4. [Transmisión de la clave de firma de la zona 25](#_bookmark98)
	5. [Transmisión de la clave de firma 25](#_bookmark99)
	6. [Duración de la firma y periodicidad de la firma 26](#_bookmark100)
	7. [Comprobación del conjunto de la clave de firma de la zona 27](#_bookmark101)
	8. [Comprobación de los registros de recursos 27](#_bookmark102)
	9. [Registros de duración de los recursos 27](#_bookmark103)
7. [AUDITORÍA DE CUMPLIMIENTO 28](#_bookmark104)
	1. [Periodicidad de la auditoría de cumplimiento de entidad 28](#_bookmark105)
	2. [Identidad y titulación del auditor 28](#_bookmark106)
	3. [Relación del auditor con el auditado 28](#_bookmark107)
	4. [Cuestiones analizadas en la auditoría 28](#_bookmark108)
	5. [Medidas adoptadas como consecuencia de deficiencias 28](#_bookmark109)
	6. [Comunicación de los resultados 29](#_bookmark110)
8. [TEMAS JURÍDICOS 29](#_bookmark111)
	1. [Honorarios 29](#_bookmark112)
	2. [Responsabilidad económica 29](#_bookmark113)
	3. [Confidencialidad de la información comercial 29](#_bookmark114)
		1. [Alcance de la información confidencial 29](#_bookmark115)
		2. [Tipos de información no considerada confidencial 29](#_bookmark116)
		3. [Responsabilidad de protección de la información confidencial 29](#_bookmark117)
	4. [Protección de la información de carácter personal 30](#_bookmark118)
		1. [Información tratada como privada 30](#_bookmark119)
		2. [Información no considerada privada 30](#_bookmark120)
		3. [Responsabilidad de protección de la información privada 30](#_bookmark121)
		4. [Divulgación en virtud de un proceso judicial o administrativo 30](#_bookmark122)
	5. [Limitaciones de la responsabilidad 30](#_bookmark123)
	6. [Vigencia y terminación 30](#_bookmark124)
		1. [*Vigencia 30*](#_bookmark125)
		2. [*Terminación 31*](#_bookmark126)
		3. [*Disposición sobre resolución de conflictos 31*](#_bookmark127)
		4. [*Legislación aplicable 31*](#_bookmark128)

[Anexo A. Tabla de acrónimos y definiciones 32](#_bookmark129)

* 1. [Acrónimos 32](#_bookmark130)
	2. [Definiciones 33](#_bookmark131)

[Anexo B. Histórico de modificaciones 34](#_bookmark132)

# INTRODUCCIÓN

El presente documento es la declaración de prácticas de DNSSEC de VeriSign (DPS, en sus siglas en inglés) para la zona TLD/GTLD. Declara las prácticas y disposiciones que VeriSign tiene en cuenta para la prestación de servicios de firma y distribución para la zona TLD/GTLD, que incluyen entre otros, a modo ejemplificativo, la emisión, gestión, modificación y distribución de claves del DNS.

## Consideraciones generales

Las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC, en sus siglas en inglés) es un conjunto de especificaciones IETF para dotar de autenticación de origen e integridad a los datos del Sistema de Nombres de Dominio (DNS, en sus siglas en inglés). Las DNSSEC sirven para que el software valide que los datos del DNS no se han modificado durante el tránsito por internet. Lo hacen incorporando criptografía de la clave pública a la jerarquía del DNS para formar una cadena de confianza que se origina en la raíz de internet.

El DNS no fue diseñado originariamente con mecanismos de seguridad sólidos para dotar de integridad y autenticidad a los datos del DNS. Con el paso del tiempo, se han detectado varias vulnerabilidades que amenazan la fiabilidad y confianza del sistema. Las DNSSEC abordan estas vulnerabilidades dotando al DNS de autenticación del origen de los datos, comprobación de la integridad de los datos y negación de existencia autenticada.

La presente DPS es aplicable en particular a todas las operaciones relacionadas con las DNSSEC realizadas por VeriSign para la zona TLD/GTLD. De forma más general, el presente documento establecerá las políticas y disposiciones que regirán la gestión, seguridad y especificaciones técnicas de la clave de firma de claves y la clave de firma de la zona TLD/GTLD. El presente documento estará bajo el control y gestión de VeriSign. La información contenida en este y posteriores documento se harán públicos en función de la necesidad.

La DPS es solo uno de un conjunto de documentos pertinentes para la gestión de VeriSign de las KSK (siglas en inglés de claves de firma clave) y ZSK (siglas en inglés de claves de firma de la zona). Entre otros documentos estarían: documentos auxiliares de seguridad confidencial y operativos que complementan la DPS indicando requisitos más pormenorizados, tales como:

* La Política de seguridad física de VeriSign - Establece los principios de seguridad que rigen la infraestructura de la DPS
* Las políticas de información y seguridad física de VeriSign describen los requisitos pormenorizados de VeriSign relativos a la seguridad personal, física de las telecomunicaciones y lógica.
* La guía de referencia de actos de claves - Presenta los requisitos operativos de gestión clave pormenorizados

En muchos casos, la DPS hace referencia a estos documentos para prácticas específicas y pormenorizadas de aplicación de las normas de titularidad de VeriSign, cuando incluir las especificidades de la DPS pueda comprometer la seguridad de la operación de firma de la zona TLD/GTLD.

## Nombre e identificación del documento

Declaración de prácticas de DNSSEC para la zona TLD/GTLD de VeriSign.

## Comunidad y aplicabilidad

### Jefe de la zona TLD/GTLD

El jefe de la zona TLD/GTLD es VeriSign

### Administrador de la zona TLD/GTLD

El administrador de la zona TLD/GTLD es VeriSign. Esta función difiere de los terceros auditores que llevan a cabo la auditoría de cumplimiento y elaboran el informe de auditoría.

### Mantenedor de la zona TLD/GTLD

El jefe de la zona TLD/GTLD es VeriSign, que lleva a cabo la función de recibir las solicitudes de modificación de la zona TLD/GTLD, aplicar los cambios, generar el nuevo archivo de la zona TLD/GTLD y publicar la zona TLD/GTLD.

### Operadores del servidor de TLD/GTLD

VeriSign actúa como el único operador para la zona TLD/GTLD.

### Operador de claves de firma de claves de la zona TLD/GTLD

El operador de claves de firma de claves de la zona TLD/GTLD es VeriSign, que lleva a cabo la función de generar la clave de firma de claves (KSK) de la zona TLD/GTLD y firmar el conjunto de claves TLD/GTLD mediante la KSK. El operador de claves de firma de claves de la zona TLD/GTLD también es responsable de generar de forma segura y de almacenar las claves privadas y de distribuir la parte pública de la clave de firma de claves a la zona principal.

El operador de KSK de la zona TLD/GTLD (KSK de TLD/GTLD) es responsable de:

1. Generar y proteger el componente privado de la KSK de TLD/GTLD.
2. Importar de forma segura los componentes de clave públicos del operador de clave de firma de la zona (ZSK) de la zona TLD/GTLD.
3. Autenticar y validar el conjunto de claves ZSK de TLD/GTLD público.
4. Firmar de manera segura los conjuntos de claves KSK y ZSK de TLD/GTLD (esto es, todos los registros DNSKEY).
5. Transmitir de manera segura el conjunto firmado de recurso-registro de DNSKEY de TLD/GTLD al operador de ZSK TLD/GTLD.
6. Exportar de forma segura los componentes de clave públicos de KSK de TLD/GTLD.
7. Crear un registro del DS de la clave pública KSK y prepararlo para el registro de los registros de TLD/GTLD.
8. El registro de los registros de TLD/GTLD lo enviará a IANA para que lo introduzca en la zona raíz.
9. Emitir una transmisión clave de emergencia en un plazo razonable si cualquier KSK asociada a la zona se pierde o se sospecha que puede verse comprometida.

### Operador de claves de firma de zona TLD/GTLD

El operador de claves de firma de claves de la zona TLD/GTLD es VeriSign, que lleva a cabo la función de generar la clave de firma de claves de la zona (ZSK) de la zona TLD/GTLD y de firmar el archivo de la zona TLD/GTLD mediante la ZSK.

El operador de clave de firma de la zona TLD/GTLD también es responsable de generar de forma segura y de almacenar las claves privadas y de distribuir la parte pública de la clave de firma de la zona al operador clave de firma de clave de la zona TLD/GTLD para que la firme.

El operador de ZSK de la zona TLD/GTLD (ZSK de TLD/GTLD) es responsable de:

1. Generar y proteger el componente privado de la ZSK de TLD/GTLD.
2. Exportar y transmitir de manera segura el componente público de ZSK de TLD/GTLD al operador de KSK de TLD/GTLD.
3. Importar de manera segura el conjunto firmado de recurso-registro de DNSKEY de TLD/GTLD del operador de KSK TLD/GTLD.
4. Firmar los registros de recurso acreditado de la zona TLD/GTLD omitiendo el registro de recurso DNSKEY.
5. Emitir una transmisión clave de emergencia en un plazo razonable si cualquier ZSK asociada a la zona se pierde o se sospecha que puede verse comprometida.

### Jefe de la zona subordinada

Los jefes de la zona subordinada (nombre de dominio TLD/GTLD) son fideicomisos del dominio delegado y como tales son responsables de prestar sus propios servicios de DNS y hacer funcionar servidores DNS subordinados. Respecto a las DNSSEC, el jefe de la zona subordinada también es responsable de:

1. Generar las claves asociadas a la zona mediante un método de confianza.
2. Registrar y conservar las representaciones abreviadas de la clave de firma de claves (en forma de un registro de recurso de firmante por delegación) en la zona principal para establecer la cadena de confianza.
3. Adoptar las precauciones razonables para evitar cualquier pérdida, divulgación o uso no autorizado de las claves asociadas a la zona.
4. Emitir una transmisión clave de emergencia en un plazo razonable si cualquier clave asociada a la zona se pierde o se sospecha que puede verse comprometida.

## Administración de especificaciones

La presente DPS se revisará y actualizará periódicamente, según corresponda, por la Autoridad de gestión de políticas (PMA, en sus siglas en inglés) de VeriSign. La PMA es responsable de la gestión de la DPS y tendrá la consideración de punto de contacto para todas las cuestiones relacionadas con ella.

### Organización de administración de especificaciones

VeriSign, Inc.

21345 Ridgetop Circle

Dulles, VA 20166 EE. UU.

### Información de contacto

Jefe de prácticas de la DPS

Autoridad de gestión de políticas de DNSSEC de VeriSign c/c a VeriSign, Inc.

21345 Ridgetop Circle

Dulles, VA 20166 EE. UU.

+1 (703) 948-3200 (teléfono)

+1 (703) 421-4873 (fax)

dnspractices@VeriSign.com

### Procedimiento de especificación de cambios

Las modificaciones de la presente DPS las realizará la autoridad de gestión de políticas (PMA) de DNSSEC de VeriSign. Las modificaciones tendrán la forma o bien de un documento que contenga una forma modificada de la DPS o una actualización. Las versiones modificadas y actualizaciones se vincularán a

la sección de actualizaciones y notificaciones de las prácticas de DNSSEC del archivo de VeriSign que se encuentra en: [http://www.VeriSigninc.com/en\_US/repository/index.xhtml.](http://www.verisigninc.com/en_US/repository/index.xhtml) Las actualizaciones sustituyen a cualquier disposición especificada o en conflicto de la versión de referencia de la DPS.

VeriSign y la PMA se reservan el derecho a modificar la DPS sin notificación de las modificaciones que no sean sustanciales, entre otras, a modo de ejemplo, las correcciones de errores tipográficos, cambios en las URL y cambios en la información de contacto. La decisión de la PMA de considerar modificaciones como sustanciales o no sustanciales queda a la exclusiva discreción de esta. Las modificaciones propuestas de la DPS aparecerán en la sección de actualizaciones y notificaciones de las prácticas de DNSSEC del archivo de VeriSign que se encuentra en: [http://www.VeriSigninc.com/en\_US/repository/index.xhtml.](http://www.verisigninc.com/en_US/repository/index.xhtml)

La PMA ofrece modificaciones propuestas de la DPS de otros participantes del subdominio de VeriSign. Si la PMA considera que dicha modificación es conveniente y propone su aplicación, notificará dicha modificación de conformidad con este apartado. No obstante cualquier disposición en contrario de la DPS, si la PMA considera que son necesarias modificaciones sustanciales de la DPS con carácter inmediato para detener o evitar una vulneración de la seguridad de parte de ella, VeriSign y la PMA podrán realizarlas mediante su publicación en el archivo de VeriSign. Tales modificaciones entrarán en vigor inmediatamente con su publicación.

# PUBLICACIÓN Y ARCHIVOS

## Archivos

VeriSign publica la DPS en la sección de archivo de su página web en [http://www.VeriSigninc.com/en\_US/repository/index.xhtml.](http://www.verisigninc.com/en_US/repository/index.xhtml)

## Publicación de las claves de firma clave

La parte pública de las KSK de TLD/GTLD se publicarán en la zona TLD/GTLD.

## Controles de acceso a los archivos

La información publicada en la parte del archivo de la página web de VeriSign es información de acceso público. El acceso de solo lectura a dicha información es ilimitado. VeriSign ha adoptado medidas de seguridad lógicas y físicas para evitar que personas no autorizadas añadan, eliminen o modifiquen entradas del archivo.

# REQUISITOS OPERATIVOS

## Significado de los nombres de dominio

Las DNSSEC ofrecen mecanismos para garantizar que el origen de los datos del DNS está en consonancia con la información del registro. NO establece ninguna manera para determinar la entidad jurídica que se encuentra detrás del nombre de dominio o la pertinencia del propio nombre de dominio.

## Activación de las DNSSEC para la zona subordinada

Las DNSSEC para una zona subordinada se activan al publicar en la zona TLD/GTLD un registro del DS firmado para esa zona subordinada. El registro del DS es una representación abreviada criptográfica o almohadilla de la clave de firma de claves de la zona subordinada generada y controlada. Establecerá una cadena de confianza desde la zona TLD/GTLD a la zona subordinada.

## Identificación y autenticación del jefe de la zona subordinada

VeriSign no lleva a cabo ninguna comprobación de la identidad y autoridad del jefe de la zona subordinada, dado que solo aplica los cambios recibidos de los registradores.

## Inscripción de los registros del firmante por delegación (DS, en sus siglas en inglés)

VeriSign aplica cambios al archivo de la zona TLD/GTLD atendiendo a las solicitudes de los registradores.

## Eliminación del registro del DS

### Quién puede solicitar la eliminación

La eliminación de los registros del DS (desactualizados o activos) solo la puede solicitar el jefe de la zona subordinada.

# CONTROLES DE INSTALACIONES, DE GESTIÓN Y OPERATIVOS

## Controles físicos

VeriSign ha puesto en marcha la Política de seguridad física de VeriSign, que respalda los requisitos de seguridad de la presente DPS. El cumplimiento de estas políticas está incluido en los requisitos de auditoría independiente de VeriSign descritos en el artículo 7. La Política de seguridad física de VeriSign contiene información de seguridad sensible y solo está disponible previo contrato con VeriSign. A continuación se describe un resumen de los requisitos.

### Ubicación del emplazamiento y construcción

Las operaciones de DNSSEC de VeriSign se llevan a cabo dentro de un entorno protegido físicamente que impide, evita y detecta el uso, el acceso o divulgación no autorizados de información y sistemas sensibles, ya sean abiertos o encubiertos. VeriSign también dispone de instalaciones de recuperación ante desastres para sus operaciones de DNSSEC. Las instalaciones de recuperación ante desastres de VeriSign están protegidas por múltiples niveles de seguridad física comparables a los de las instalaciones principales de VeriSign.

### Acceso físico

Los sistemas de DNSSEC de VeriSign están protegidos por un mínimo de cuatro niveles de seguridad física, siendo necesario acceder al nivel inferior antes de poder acceder al siguiente nivel superior. Con privilegios de acceso físico restrictivo progresivos para controlar el acceso a cada nivel. La actividad operativa de DNSSEC sensible, cualquier actividad relacionada con el ciclo de vida de las KSK y ZSK de TLD/GTLD tiene lugar dentro de niveles con grandes restricciones físicas. El acceso a cada nivel exige el uso de una tarjeta identificativa de proximidad de empleado. El acceso físico se registra automáticamente y se graba con vídeo. Los niveles adicionales exigen control de acceso individual a través del uso de dos factores de autenticación, que incluyen elementos de reconocimiento biométricos. El sistema de seguridad física incluye niveles adicionales para la seguridad de la gestión clave que sirve para proteger tanto el almacenamiento en línea como fuera de línea de HSM y material de claves. Las zonas utilizadas para crear y almacenar material criptográfico tienen doble control, cada uno a través del uso de dos factores de autenticación, que incluyen elementos de reconocimiento biométricos. Los HSM en línea se protegen mediante el uso de armarios cerrados con llave. Los HSM fuera de línea se protegen mediante el uso de cajas fuertes, armarios y contenedores cerrados con llave. El acceso a los HSM y material de claves está restringido de conformidad con los requisitos de separación de funciones de VeriSign. La apertura y cierre de los armarios o contenedores de estos niveles se registran a efectos de auditoría.

### Electricidad y aire acondicionado

Las instalaciones de seguridad de VeriSign están equipadas con sistemas de electricidad principales y de reserva para garantizar el acceso continuado e ininterrumpido a la electricidad y sistemas de calefacción, ventilación y aire acondicionado a fin de controlar la temperatura y humedad relativa.

### Exposiciones al agua

VeriSign ha adoptado precauciones razonables para reducir los efectos a la exposición al agua de sus sistemas.

### Prevención y protección contra incendios

VeriSign ha adoptado precauciones razonables para prevenir y extinguir incendios u otra exposición a llamas o humo dañina. Las medidas de prevención y protección contra incendios de VeriSign se han diseñado para cumplir las normas de seguridad ante incendios locales.

### Medios de almacenamiento

Todos los medios que contengan software de producción, así como medios que contengan datos, auditorías, archivos e información de respaldo se almacenan en las instalaciones de VeriSign o en instalaciones de almacenamiento fuera de las mismas con controles de acceso físico y lógico destinadas a limitar el acceso de personas no autorizadas y protegerlos contra daños accidentales (p. ej. agua, fuego y electromagnetismo).

### Eliminación de residuos

Los documentos y materiales sensibles se trituran antes de su eliminación. Los medios utilizados para recopilar o transmitir información sensible se hacen ilegibles antes de su eliminación. Los dispositivos criptográficos se destruyen o ponen a cero físicamente de conformidad con las directrices del fabricante antes de su eliminación. Otros residuos se eliminan de acuerdo con los requisitos de eliminación de residuos normales de VeriSign.

### Copia de seguridad ex situ

VeriSign realiza copias de respaldo rutinarias de datos de sistema esenciales, datos de registro de auditoría y otra información sensible. Los medios de respaldo ex situ se almacenan de forma físicamente segura haciendo uso de instalaciones de depósito de almacenamiento de terceros y en la instalación de recuperación ante desastres de la Costa Este de VeriSign.

## Controles de procedimiento

### Funciones de confianza

Las personas de confianza son, entre otras, los empleados, contratistas y consultores que tienen acceso o controlan operaciones criptográficas que pueden afectar sustancialmente:

* a la generación y protección del componente privado de la clave de firma de claves de la zona TLD/GTLD,
* a la exportación o importación segura de cualesquiera componentes públicos, y
* a la generación y firma de los datos del archivo de la zona. Entre las personas de confianza se encuentran, a modo ejemplificativo:
* personal de establecimiento de nombres y operaciones de resolución,
* personal de operaciones comerciales criptográficas,
* personal de seguridad,
* personal de administración de sistemas,
* personal de determinada ingeniería, y
* directivos nombrados para gestionar la fiabilidad infraestructural.

VeriSign considera las categorías de personal identificado en este apartado personas de confianza que ocupan una posición de confianza. Las personas que quieran ser personas de confianza ocupando un puesto de confianza deben cumplir los requisitos de prueba establecidos en la presente DPS.

### Número de personas necesarias por tarea

VeriSign ha establecido, mantiene y aplica procedimientos de control rigurosos para asegurarse de la separación de funciones atendiendo a la responsabilidad del puesto y para garantizar que son necesarias varias personas de confianza para llevar a cabo tareas sensibles. Los procedimientos de política y control se aplican para garantizar la separación de funciones atendiendo a las responsabilidades del puesto.

Las tareas más sensibles, tales como el acceso y gestión a hardware criptográfico (módulo de seguridad de hardware o HSM en sus siglas en inglés) y material de claves vinculado exigen varias personas de confianza. Estos procedimientos de control interno están destinados a garantizar que, como mínimo, dos personas de confianza deban acceder física o lógicamente al dispositivo.

El acceso al hardware criptográfico se lleva a cabo por varias personas de confianza a lo largo de su ciclo de vida desde la recepción de su entrada e inspección a su destrucción lógica y física definitiva. Una vez activado un módulo con claves operativas, se invocan posteriores controles de acceso para mantener un control separado sobre tanto el acceso físico como el lógico al dispositivo. Las personas con acceso físico a los módulos no tienen participaciones secreta y viceversa.

### Identificación y autenticación de cada función

Se comprueba la identidad de cualquier persona que quiera ser una persona de confianza a través de su presencia personal (física) ante las personas de confianza del Departamento de Recursos Humanos de VeriSign o posiciones de seguridad y la comprobación de formas de identificación reconocidas (p. ej. pasaportes y permisos de conducción). La identidad se confirma además a través de los procedimientos de comprobación de los antecedentes del apartado 4.3 de la DPS. VeriSign garantiza que el personal ha adquirido la condición de personal de confianza y que se ha contado con autorización departamental antes de que ese personal:

* reciba dispositivos de acceso y se le confiera acceso a las instalaciones requeridas
* reciba credenciales electrónicas para acceder y realizar determinadas funciones en los sistemas de TI de VeriSign

### Tareas que requieren separación de funciones

Entre las tareas que exigen la separación de funciones se encuentran, a modo de ejemplo, la generación, funcionamiento y destrucción del material de claves de DNSSEC de la zona TLD/GTLD.

El personal de auditoría nombrado no podrá participar en el control multipersonal para las ZSK o KSK de TLD/GTLD.

## Controles de personal

### Requisitos de titulación, experiencia y de permisos de entrada

VeriSign exige que el personal que quiera ser personal de confianza acredite sus antecedentes, titulación y experiencia necesarios para llevar a cabo las responsabilidades del posible puesto de trabajo de manera competente y satisfactoria, así como que presente las autorizaciones oficiales o prueba de nacionalidad, de ser necesarias para llevar a cabo operaciones en virtud de contratos públicos.

### Procedimientos de comprobación de los antecedentes

Todo el personal que tenga acceso a cualquier componente criptográfico utilizado en el proceso de firma de la zona TLD/GTLD tiene que someterse a una comprobación de sus antecedentes de al menos los 3 años anteriores.

Antes de empezar a desempeñar un puesto de confianza, VeriSign realiza comprobaciones de los antecedentes que incluyen:

* confirmación del trabajo anterior
* comprobación de referencias profesionales
* confirmación de la titulación más alta o más pertinente obtenida
* comprobación de los registros de crédito y financieros en la medida en que lo permitan las leyes nacionales para las personas físicas del país de residencia
* comprobación de los antecedentes penales (locales, estatales, provinciales y nacionales)
* comprobación de los registros de permiso de conducción
* comprobación de los registros de la administración de la Seguridad Social

En la medida en que cualquiera de los requisitos establecidos en este artículo no se cumplan como consecuencia de una prohibición o limitación de la legislación local u otras circunstancias, VeriSign utilizará una técnica de investigación sustituta que esté permitida por la ley y que proporcione información sustancialmente similar, incluido, entre otras cosas, la obtención de una comprobación de los antecedentes realizada por el organismo público aplicable.

Los factores revelados en una comprobación de los antecedentes que podrían considerarse motivos para rechazar a candidatos a posiciones de confianza o para adoptar medidas contra las personas que ya las ocupen son, entre otros:

* declaraciones falsas realizadas por el candidato o persona de confianza
* referencias profesionales muy desfavorables o poco fiables
* indicaciones de falta de responsabilidad económica
* determinadas condenas penales

Los informes que contengan dicha información se evaluarán por el personal de recursos humanos y seguridad de VeriSign, que decidirá las medidas oportunas a adoptar a la luz del tipo, magnitud y frecuencia de la conducta desvelada por la comprobación de los antecedentes.

Tales medidas podrían incluir la cancelación de ofertas de empleo realizadas a candidatos para posiciones de confianza o la terminación de los contratos de personas que ya ocupen puestos de esa naturaleza. El uso de información revelada en una comprobación de antecedentes para adoptar tales medidas estará sujeta a las leyes federales, estatales y locales.

### Requisitos de formación

VeriSign proporciona formación a su personal en el momento de su contratación, así como requisito de formación para el puesto necesaria para desempeñar las responsabilidades derivadas del mismo de forma competente y satisfactoria. VeriSign revisa y mejora periódicamente sus programas de formación según corresponda.

Los programas de formación de VeriSign se adaptan a las responsabilidades de las personas e incluyen lo siguiente, según corresponda:

* conceptos básicos de DNS/DNSSEC
* responsabilidades del puesto
* uso y funcionamiento de hardware y software utilizados
* políticas y procedimientos de seguridad y operativos
* elaboración de informes y gestión de incidentes y compromisos
* procedimientos de recuperación ante desastres y continuidad de la actividad

### Periodicidad de la retención y requisitos

VeriSign proporciona formación de actualización a su personal en la medida y con la frecuencia que sean necesarias para asegurarse de que ese personal mantiene el nivel exigido de competencia para desempeñar las responsabilidades derivadas de su puesto de trabajo de manera competente y satisfactoria.

### Periodicidad y secuencia de la rotación de puestos de trabajo

El personal rotará y será sustituido según proceda.

### Sanciones por actuaciones no autorizadas

Se adoptarán las medidas disciplinarias oportunas respecto a las actuaciones no autorizadas relativas a la presente DPS y otras vulneraciones de las políticas y procedimientos de VeriSign. Entre las acciones disciplinarias que se podrán adoptar se encuentra la terminación y serán proporcionales con la frecuencia y gravedad de las actuaciones no autorizadas.

### Requisitos de contratación del personal

En circunstancias limitadas, se podrá hacer uso de contratistas y consultores independientes para ocupar posiciones de confianza. Dichos contratistas o consultores estarán sujetos a los mismos criterios funcionales y de seguridad que se aplican a los empleados en posiciones comparables. Los contratistas o consultores independientes que no hayan completado o pasado los procedimientos de comprobación de antecedentes especificados en el apartado 4.3 de la DPS solo tendrán acceso a las instalaciones de seguridad de VeriSign en la medida en que vayan acompañados y sean supervisados directamente por personas de confianza en todo momento.

### Documentación facilitada al personal

VeriSign proporciona formación a sus empleados y toda la documentación que sea necesaria para desempeñar las responsabilidades derivadas de su puesto de trabajo de forma competente y satisfactoria.

## Procedimientos de auditoría de inicio de sesión

### Tipos de sucesos registrados

VeriSign registra manual o automáticamente los siguientes sucesos importantes: los sucesos de gestión del ciclo de vida de las KSK y ZSK de TLD/GTLD, entre otros:

* generación, copia de respaldo, almacenamiento, recuperación archivo y destrucción de claves
* exportación de componentes de clave públicos
* sucesos de gestión de ciclo de vida de dispositivos criptográficos

los sucesos de firma y gestión de las KSK y ZSK de TLD/GTLD, entre otros:

* activación de clave
* recepción y validación de material de clave público firmado
* solicitudes de firma correctas e incorrectas
* sucesos de transmisión de claves

sucesos relativos a la seguridad, entre otros:

* intentos de acceso al sistema exitosos y fallidos
* acciones de sistema de seguridad y de claves llevados a cabo por personal de confianza
* archivos y registros de seguridad sensibles leídos, escritos y eliminados
* cambios de perfil de seguridad
* caídas del sistema, fallos del hardware y otras anomalías
* actividad del router y cortafuegos
* entrada salida de los visitantes a las instalaciones
* cambios del sistema y actualizaciones de mantenimiento y del sistema
* gestión de la respuesta a incidentes

Las entradas de registro incluyen los elementos siguientes:

* fecha y hora de la entrada
* identidad de la entidad que realiza la entrada al diario
* número de serie o secuencia de la entrada para entradas automáticas del diario
* tipo de entrada
* otros sucesos, en su caso

Todos los tipos de información de auditoría contendrán información correcta de la hora y la fecha

### Periodicidad del registro de procesamiento

Los registros de auditoría analizados tras cada acto clave para sucesos importantes de seguridad y operativos. Asimismo, VeriSign revisa sus registros de auditoría para actividad sospechosa o extraordinaria como respuesta a las alertas generadas como consecuencia de irregularidades e incidentes dentro de los sistemas de firma de la zona de VeriSign. El procesamiento de registro de auditoría consiste en una revisión de los registros de auditoría y documentación para todos los sucesos importantes. Las revisiones de registro de auditoría incluyen una comprobación de que el registro no ha sido alterado con una investigación de cualquier alerta o irregularidad de los registros. Las acciones adoptadas en las revisiones de los registros de auditoría también se documentan

### Período de conservación del registro de auditoría

Todos los datos de auditoría recopilados conforme a lo establecido en el apartado 4.4.1 se conservarán in situ durante al menos un (1) año tras su creación y posteriormente se archivarán durante al menos 2 años.

Los medios que contengan los datos de auditoría y las aplicaciones necesarias para procesar la información se conservarán para garantizar que se pueda acceder a los datos almacenados durante el plazo establecido en esta DPS.

### Protección del registro de auditoría

Los registros de auditoría se protegerán con un sistema de registro de auditoría electrónico que incluye mecanismos para proteger los archivos de registro de visitas, modificaciones, borrado u otras alteraciones no autorizadas.

### Procedimientos de copia de seguridad de los registros de auditoría

VeriSign realiza copias de seguridad de forma progresiva de archivos electrónicos de su información de las ZSK y KSK de TLD/GTLD diariamente y lleva a cabo copias de seguridad completas cada semana. Las copias de cualquier registro en papel se conservarán en unas instalaciones de seguridad.

### Sistema de recopilación de auditorías

Los datos de auditoría automatizados se generan y graban en la aplicación, la red y el sistema operativo. El personal de VeriSign graba los datos de auditoría generados manualmente.

Se hacen copias de respaldo de la información electrónica de forma gradual y se hacen copias de los registros en papel a medida que se incluyen nuevos registros en el archivo. Estas copias de seguridad se conservan en instalaciones de seguridad.

### Notificación a la persona que ha ocasionado un suceso

Cuando se registra un suceso en un sistema de recopilación de auditoría, no es necesario notificarlo a ninguna persona física, organización, dispositivo o aplicación que haya ocasionado el suceso.

### Evaluación de la vulnerabilidad

Se registran los sucesos del proceso de auditoría, en parte para controlar las vulnerabilidades del sistema.

Las evaluaciones de la vulnerabilidad de la seguridad (SVA, en sus siglas en inglés) se llevan a cabo y se revisan tras un examen de los sucesos controlados. Las SVA se basan en datos de registro automatizados y se llevan a cabo con regularidad. Una SVA anual se incluirá en una entrada de la auditoría de cumplimiento anual.

## Compromiso y recuperación ante desastres

### Procedimientos de gestión de incidentes y compromisos

Las copias de seguridad de los datos de auditoría y registros de la base de datos se conservan en un almacén ex situ y estarán disponibles en caso de un compromiso o desastre.

Las copias de seguridad de claves privadas se generarán y conservarán de acuerdo con el apartado 5.2.4 de la DPS.

### Recursos informáticos, software y datos dañados

En caso de que se dañen los recursos informáticos, software y datos se informará a VeriSign Information Security y se aplicarán procedimientos de gestión de incidentes de VeriSign. Tales procedimientos exigen una escalación, investigación de incidentes y respuesta a los mismos adecuada. De ser necesario, se aplicarán los procedimientos de compromiso de claves o de recuperación ante desastres de VeriSign.

### Procedimientos de compromiso de clave privada de entidad

* + - 1. **Compromiso de clave de firma de claves**

Con un compromiso posible o conocido de clave de firma de claves de TLD/GTLD, el equipo de respuesta a incidentes de seguridad de VeriSign (VSIRT, en sus siglas en inglés) pone en marcha los procedimientos de respuesta a compromisos de clave de VeriSign. Este equipo, que incluye a personal de los departamentos de Seguridad de la información, Operaciones comerciales criptográficas, Servicios de producción y otros representantes directivos de VeriSign evalúa la situación, desarrolla un plan de acción y lo pone en práctica con la aprobación del equipo directivo de VeriSign.

* + - 1. **Compromiso de clave de firma de la zona**

Con un compromiso posible o conocido de clave de firma de la zona de TLD/GTLD, el equipo de respuesta a incidentes de seguridad de VeriSign (VSIRT, en sus siglas en inglés) pone en marcha los procedimientos de respuesta a compromisos de clave de VeriSign. Este equipo que incluye a los departamentos de Seguridad de la Información, Operaciones de Negocio de Criptografía, Servicios de Producción y otros representantes de la dirección de VeriSign evalúa la situación, desarrollan un plan de acción y lo ponen en marcha con la aprobación de la dirección de VeriSign.

### Capacidad de recuperación ante desastres informáticos y continuidad de la actividad

VeriSign ha puesto en marcha un emplazamiento de recuperación ante desastres que está física y geográficamente separado de sus instalaciones de seguridad principales. VeriSign ha desarrollado, puesto en marcha y probado planes de continuidad de la actividad y recuperación ante desastres de TI para disminuir los efectos de desastres naturales, ocasionados por el hombre y tecnológicos. Estos planes se prueban, validan y actualizan con regularidad para que sean operativos en caso de cualquier incidente o desastre.

Existen planes de recuperación ante desastres de TI y de continuidad de la actividad pormenorizados para abordar la restauración de los servicios de sistemas de información y funciones de negocio clave.

VeriSign cuenta con un equipo de respuesta a incidentes formal que está respaldado por un equipo de gestión de incidentes corporativo formal (CIMT, en sus siglas en inglés) y equipos de continuidad de las actividades en las unidades de negocio para responder y gestionar cualquier incidente o desastre que afecte a los empleados, operaciones, entornos e instalaciones de VeriSign. El emplazamiento de recuperación ante desastres de TI ha puesto en marcha las protecciones de seguridad física y controles operativos exigidos por las Políticas de seguridad física de VeriSign a fin de garantizar un entorno operativo de copia de seguridad sólido. En caso de producirse un incidente o desastre natural, ocasionado por el hombre o tecnológico que exija el cese temporal o permanente de las operaciones de las instalaciones principales de VeriSign, el equipo de respuesta a incidentes (IRT) y el equipo de gestión de incidentes corporativo (CIMT) de VeriSign inician el proceso de recuperación ante desastres de TI y continuidad de las actividades de VeriSign. VeriSign tiene capacidad para restaurar o recuperar operaciones esenciales tras un desastre con, al menos, apoyo para las funciones siguientes:

* Comunicación con el público
* Capacidad para importar y exportar KSR
* Generación de claves de firma clave
* Tratamiento y firma de contenidos de KSR
* Firma de un archivo de la zona
* Distribución del archivo de la zona firmado
* Generación de claves de firma de la zona

El entorno de recuperación ante desastres de VeriSign se sincroniza con regularidad con el sistema de producción dentro de los límites de tiempo establecidos en las Políticas de seguridad de la información y física de VeriSign. El entorno de recuperación ante desastres de VeriSign está protegido con medidas de seguridad física comparables a los niveles de seguridad física especificados en el apartado 4.1.2 de la DPS. Los planes de recuperación ante desastres de TI y de continuidad de las actividades de VeriSign se han diseñado para proporcionar una recuperación total de las funcionalidades esenciales tras un incidente o desastre en el emplazamiento principal de VeriSign. VeriSign prueba su entorno en su emplazamiento principal para respaldar todas las funciones, incluidas las de DNSSEC, tras cualquier desastre, excepto uno de grandes dimensiones que pudiera dejar todas las instalaciones inoperativas. Los resultados de dichas pruebas se revisan y se conservan a efectos de auditoría y planificación. De ser posible, se restablecen las operaciones en el emplazamiento principal de VeriSign tan pronto como resulta posible tras cualquier incidente o desastre. VeriSign conserva hardware y copias de seguridad de sobra de su software de sistema de infraestructura en sus instalaciones de recuperación ante desastres de TI. Asimismo, se hacen copias de seguridad de las claves privadas y se conservan a efectos de recuperación ante desastres de conformidad con el apartado 5.2.4 de la DPS.

## Terminación de la entidad

VeriSign ha adoptado un plan de terminación de las DNSSEC en el supuesto de que las funciones y responsabilidades del operador de ZSK de la zona y el operador de KSK de la zona TLD/GTLD deban trasladarse a otras entidades. VeriSign coordinará a todas las partes necesarias a fin de llevar a cabo la transición de forma segura y transparente.

# CONTROLES DE SEGURIDAD TÉCNICA

## Generación e instalación de par de claves

### Generación de par de claves

La generación de la clave de firma de claves de la zona y la clave de firma de la zona TLD/GTLD la llevan a cabo múltiples personas preseleccionadas, formadas y de confianza mediante sistemas y procesos fiables que proporcionan la seguridad y fortaleza criptográfica necesaria para las claves generadas. Los módulos criptográficos utilizados para la generación de las claves KSK y ZSK de TLD/GTLD cumplen todos los requisitos de la FIPS 140-2 nivel 3.

Todos los pares de clave KSK y ZSK se generan en actos de generación de clave planificados previamente de conformidad con los requisitos de la Guía de referencia de actos de claves y las Políticas de seguridad física e información de VeriSign. Las actividades realizadas en cada acto de generación de claves se registran y las personas intervinientes fechan y firman los registros. Estos registros se conservan a efectos de auditoría y seguimiento durante el tiempo que la dirección de VeriSign considera oportuno.

### Entrega de clave pública

La información de clave pública sobre las KSK procede de la respuesta de clave firmada XML del CBO. La información de clave pública para las ZSK procede de los centros de datos cerrados con llave desde dentro de los HSM que entrega el personal del CBO.

### Generación y comprobación de la calidad de los parámetros de la clave pública

Para el tamaño actual de la ZSK, se realizan pruebas de primalidad de los parámetros de RSA (p y q) para garantizar que la probabilidad de que los números no sean compuestos sea menor a 2^-100.

Las comprobaciones de calidad también incluyen la validación de que el tamaño del exponente público sea tanto eficiente respecto a los recursos y seguro.

* + 1. **Usos de la clave**

Cualquier clave privada KSK y ZSK de la zona TLD/GTLD se utilizará únicamente para firmar los conjuntos RR de la zona TLD/GTLD pertinente o firmar automáticamente sus propios conjuntos de RR DNSKEY para demostrar que se tiene la clave privada.

Cualquier registro de RRSIG derivado tendrá un período de validez máximo de 7 días. El RRSIG generado por la ZSK será válido durante siete días y el RRSIG generado por la KSK será válido durante 15 días

## Protección de la clave privada y controles de la ingeniería de los módulos criptográficos

Todas las funciones criptográficas relativas al componente privado de las KSK y ZSK debe realizarlas el HSM, esto es, el componente privado no será exportado del HSM, salvo si está en forma cifrada para una copia de respaldo de la clave.

### Normas y controles de los módulos criptográficos

Para la generación del par de claves KSK y ZSK de TLD/GTLD y el almacenamiento de la clave privada, VeriSign utiliza módulos de seguridad de hardware que están certificados por la FIPS 140-2 nivel 3.

### Control multipersonal de la clave privada (m-de-n)

VeriSign ha puesto en marcha mecanismos procedimentales y técnicos que exigen la participación de múltiples personas de confianza para realizar operaciones criptográficas sensibles. VeriSign utiliza el sistema de uso compartido de secretos para dividir los datos de activación necesarios para hacer uso de una clave privada KSK y ZSK de TLD/GTLD en distintas partes denominadas partes del secreto que están en poder de personas formadas y de confianza denominadas titulares de las partes. Es necesario un mínimo número de partes del secreto (m) del número total (n) de las partes del secreto creadas y distribuidas para un módulo de seguridad de hardware concreto con el fin de activar una clave privada ZSK de TLD/GTLD almacenada en el módulo. El número mínimo de partes necesarias para firmar un archivo de la zona TLD/GTLD es 3.

Se ha de tener en cuenta que el número de partes distribuidas para identificadores de recuperación ante desastres puede ser inferior al número distribuido para HSM operativos, aunque el número mínimo de partes necesarias (m) sigue siendo el mismo. Las partes del secreto se protegen de conformidad con la presente DPS.

### Depósito de la clave privada

Los componentes privados de las KSK y ZSK de TLD/GTLD no se depositan.

### Copia de seguridad de la clave privada

VeriSign crea copias de seguridad de las claves privadas KSK y ZSK de TLD/GTLD para la recuperación rutinaria y a efectos de recuperación ante desastres. Dichas claves se almacenan cifradas dentro de módulos criptográficos de hardware y dispositivos de almacenamiento de claves asociados. Los módulos criptográficos utilizados para el almacenamiento de la clave privada cumplen los requisitos de la presente DPS. Las claves privadas se copian para contar con copias de respaldo en los módulos criptográficos de hardware de conformidad con la presente DPS. Los módulos que contienen las copias de respaldo in situ de las claves privadas KSK y ZSK de TLD/GTLD cumplen los requisitos de la presente DPS. Los módulos que contienen las copias de recuperación ante desastres de las claves privadas KSK y ZSK de TLD/GTLD cumplen los requisitos de la presente DPS.

### Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas se almacenan cifradas dentro de módulos criptográficos de hardware.

### Trabajo de archivo de las claves privadas

Los pares de claves KSK y ZSK de TLD/GTLD no expiran, pero se retiran cuando se sustituyen. Los pares de claves sustituidos se conservan de forma segura en los HSM que cumplen los requisitos de la presente DPS. Estos pares de claves no se utilizarán para ningún acto de firma tras su sustitución y se pondrán a cero una vez retirados del servicio los HSM.

### Transmisión de la clave privada al o del módulo criptográfico

VeriSign genera pares de claves KSK y ZSK de TLD/GTLD en los HSM en los que se utilizarán las claves, con procedimientos de réplica para copiar las mismas claves en copias de seguridad (en el caso de KSK) y en copias utilizadas para firma activa (en el caso de ZSK). VeriSign hace copias asimismo de esos pares de claves a efectos de recuperación rutinaria y de recuperación ante desastres. Cuando los pares de claves se copian en otro HSM, esos pares de claves se transportan entre módulos de manera cifrada.

### Método de activación de la clave privada

Las claves privadas KSK y ZSK de TLD/GTLD se activarán median un mínimo de 3 m de n partes del secreto.

### Método de desactivación de la clave privada

Las claves privadas KSK y ZSK de TLD/GTLD se desactivan con el cierre del sistema.

### Método de destrucción de la clave privada

De ser necesario, VeriSign destruye las claves privadas KSK y ZSK de TLD/GTLD de una manera que garantice razonablemente que no quedan restos residuales de las claves que pudieran dar lugar a su reconstrucción.

VeriSign utiliza una función de puesta a cero de su HSM y otros medios oportunos para garantizar la completa destrucción de las claves privadas KSK y ZSK de TLD/GTLD. Al hacerlo, las actividades de destrucción de claves privadas se registran.

## Otros aspectos de la gestión del par de claves

### Trabajo de archivo de las claves públicas

Las claves públicas ZSK y KSK de TLD/GTLD se copian y archivan como parte de los procedimientos de copia de respaldo rutinarios de VeriSign.

### Períodos de uso de las claves

El período operativo de cada clave KSK y ZSK de TLD/GTLD acaba con su sustitución. Las claves KSK y ZSK de TLD/GTLD sustituidas nunca se volverán a utilizar para firmar un registro de recurso.

## Datos de activación

### Generación e instalación de los datos de activación

Los datos de activación (partes del secreto) utilizados para proteger los HSM que contienen las claves privadas de KSK y ZSK de TLD/GTLD de VeriSign se generan de acuerdo con los requisitos del apartado

5.2 de la DPS. La creación y distribución de las partes del secreto se registra.

De ser necesario, los datos de activación para las claves privadas KSK y ZSK de TLD/GTLD se transmiten directamente de la plataforma Host IS al HSM. Esta transmisión tiene lugar en la infraestructura segura de VeriSign.

### Activación de la protección de los datos

Los titulares de partes deben proteger sus partes del secreto y firmar un contrato en el que reconocen sus responsabilidades como tales.

Los datos de activación para las claves privadas KSK y ZSK de TLD/GTLD se retirarán del servicio con métodos de protección contra pérdidas, robo, modificación, divulgación y uso no autorizados de las claves privadas protegidas por los datos de activación. Tras el registro de los períodos de conservación del apartado 5.2.6, VeriSign retirará del servicio los datos de activación sobrescribiéndolos o destruyéndolos físicamente.

## Controles de seguridad informática

VeriSign se asegura de que los sistemas que contienen el software de clave y los archivos de datos son sistemas fiables seguros frente a accesos no autorizados. Asimismo, VeriSign limita el acceso a los servidores de producción a las personas que tienen una razón comercial válida para acceder a ellos. Los usuarios de aplicaciones generales no tienen cuentas en los servidores de producción.

VeriSign exige el uso de contraseñas que tengan una longitud de caracteres mínima y una combinación de caracteres alfanuméricos y especiales. VeriSign exige que las contraseñas se cambien periódicamente.

## Controles de seguridad de la red

VeriSign lleva a cabo todas las funciones de firmado en línea mediante redes protegidas conformes con sus Políticas de seguridad física e información para evitar el acceso no autorizado y otras actividades

malintencionadas. VeriSign protege sus comunicaciones de información sensible mediante firmas cifradas y digitales.

La red de producción de VeriSign está separada lógicamente de otros componentes. Esta separación evita el acceso a la red, salvo a través de procesos de aplicaciones definidos. VeriSign utiliza cortafuegos para

proteger la red de producción de intrusiones internas y externas y para limitar la naturaleza y alcance de las actividades en la red que puedan acceder a los sistemas de producción que están relacionados con las actividades de firma de las claves.

## Sello de tiempo

El tiempo derivado del procedimiento se utilizará para timbrar con sello de tiempo

* los registros de auditoría electrónicos y en papel
* Fechas de expiración y comienzo de las firmas DNSSEC Los tiempos deben ser razonablemente precisos.

## Controles técnicos del ciclo de vida

### Controles de desarrollo del sistema

VeriSign desarrolla y pone en marcha aplicaciones conforme a sus normas de desarrollo de sistemas y gestión de cambios.

Todo el software de VeriSign utilizado en los sistemas de producción se puede rastrear en archivos de control de versión.

### Controles de gestión de la seguridad

VeriSign dispone de mecanismos y políticas para controlar y supervisar la configuración de sus sistemas. VeriSign crea una almohadilla de todos los paquetes de software instalados en los sistemas de producción. Esta almohadilla se puede utilizar para comprobar la integridad del software a efectos forenses, aunque en la práctica la detección de la intrusión basada en host se utiliza para alertar cuando se modifican paquetes de software esenciales.

### Controles de seguridad del ciclo de vida

El sistema del firmante se diseña para exigir un mínimo de mantenimiento. Las actualizaciones esenciales para la seguridad y operaciones del sistema del firmante se aplicarán tras una prueba formal y aprobación. El origen de todo el software y cortafuegos se autenticará de forma segura a través de los medios disponibles.

Los componentes de hardware esenciales del sistema del firmante (HSM) se obtendrán directamente del fabricante y se transportarán en bolsas con precinto a su destino en las instalaciones seguras. Cualquier hardware será retirado del servicio mucho antes del fin de su vida útil especificada.

# FIRMA DE LA ZONA

El jefe de la zona TLD/GTLD proporcionará al mantenedor de la zona TLD/GTLD un conjunto RR DNSKEY firmado y válido que contendrá las claves vigentes del operador de ZSK de la zona TLD/GTLD y las KSK.

En función de la TLD/GTLD que se aplique, se usará una de las dos opciones.

Opción 1: el mantenedor de la zona TLD/GTLD incluye su conjunto de claves en el archivo de la zona TLD/GTLD, añade los 3 registros seguros siguientes (NSEC3) y crea firmas para todos los registros pertinentes. La zona TLD/GTLD se distribuye a continuación a los operadores de servidores de TLD/GTLD.

Opción 2: el mantenedor de la zona TLD/GTLD incluye su conjunto de claves en el archivo de la zona TLD/GTLD, añade el siguiente registro seguro (NSEC) y crea firmas para todos los registros pertinentes. La zona TLD/GTLD se distribuye entonces a los Operadores de los Servidores de TLD/GTLD.

El mantenedor de la zona TLD/GTLD realizará automáticamente la firma de la zona TLD/GTLD continua.

## Longitud y algoritmos de las claves

Los pares de claves deben tener la longitud suficiente para evitar que otros decidan la clave privada de los pares de claves mediante análisis criptográfico durante el período de uso esperado de los mismos.

El (los) par(es) de claves KSK de TLD/GTLD vigentes es un par de clave RSA con un tamaño de módulo de 2048 bits. El (los) par(es) de claves ZSK de TLD/GTLD vigentes es un par de clave RSA con un tamaño de módulo de 1024 bits.

## Negación de existencia autenticada

En función de la TLD/GTLD que se aplique, se usará una de las dos opciones.

Opción 1: la negación de la existencia autenticada se proporcionará a través del uso de registros NSEC3, según se especifica en RFC 5155 [RFC5155].

Opción 2: la negación de la existencia autenticada se proporcionará a través del uso de registros NSEC, según se especifica en RFC 4034 [RFC4034].

## Formato de firma

La función de almohadilla criptográfica utilizada junto con el algoritmo de firma debe ser lo suficientemente resistente para prever ataques durante el tiempo en el que la firma es válida.

En función del TLD/GTLD aplicado, se seguirá de una de las dos opciones siguientes.

Opción 1: las firmas KSK y ZSK de TLD/GTLD se generarán mediante almohadillas de cifrado SHA-256. Opción 2: las firmas KSK y ZSK de TLD/GTLD se generarán mediante almohadillas de cifrado SHA-512.

## Transmisión de la clave de firma de la zona

El sistema realiza la transmisión de la ZSK de TLD/GTLD trimestralmente de forma automática. La firma de clave ZSK de TLD/GTLD se lleva a cabo por adelantado (para mantener la KSK de TLD/GTLD fuera de línea lo máximo posible). Las ZSK de TLD/GTLD que se utilizarán entre tanto se generan previamente y se firman al mismo tiempo que las fechas de comienzo y expiración prevista de la firma.

## Transmisión de la clave de firma

Actualmente no hay transmisiones de KSK de TLD/GTLD planificadas precisas, pero VeriSign evaluará la necesidad de las mismas una vez al año aproximadamente.

## Duración de la firma y periodicidad de la firma

La práctica de la firma de la zona TLD/GTLD se divide en ciclos de tiempo continuos trimestrales de aproximadamente 90 días. Los ciclos de tiempo comienzan en las fechas siguientes de cada año:

15 de enero,

15 de abril, 15 de julio y 15 de octubre

Todos los registros DNSKEY generados por los cambios enumerados anteriormente se (1) conocen por adelantado y (2) se firman por adelantado por la KSK de TLD/GTLD. La recopilación de los registros DNSKEY para los que VeriSign genera previamente firmas digitales consiste en un período de 1 año.

El ciclo de tiempo nunca será inferior a 90 días, salvo en situaciones de urgencia (en las que una clave se vea comprometida) o si VeriSign decide empezar a utilizar distintas longitudes de clave.

El mantenedor de la zona TLD/GTLD genera una nueva ZSK que se utilizará en cada nuevo ciclo de tiempo. Por tanto, se lleva a cabo una transmisión de ZSK de TLD/GTLD al final de cada ciclo de tiempo.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ZSK n-1 ===|-->|

ZSK n ---|===================================|---> ZSK n+1 |---|===>

KSK n ===========================|---|++>|

KSK n+1 | |===============>

90 días con transmisión de ZSK y KSK

(-) publicación posterior o previa (+) revoca conjunto de bits

(=) utilizados para firmar ciclo de

Figura 1

En el caso de una transmisión de ZSK, las franjas de tiempo se utilizan para publicar previamente o con posterioridad en el orden siguiente: Franja 1:

publicación ZSK (n) + ZSK (n-1) + KSK, zona de firma con ZSK (n) Franjas 2-8: publicación ZSK (n) + KSK, zona de firma con ZSK (n)

Franja 9:

publicación ZSK (n) + ZSK (n+1) + KSK, zona de firma con ZSK (n)

El mantenedor de la zona TLD/GTLD selecciona e incluye el conjunto RR DNSKEY vigente y firma(s) correspondiente(s) y a continuación firma todos los registros acreditados dentro de la zona TLD/GTLD mediante la ZSK de TLD/GTLD vigente con un período de validez de 7 días.

Para cada una de estas franjas existe un conjunto de claves DNSKEY generadas previamente que se firma en el acto de firma.

|  |  |  |
| --- | --- | --- |
| RRSIG | 1 | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 ||---->| |
| RRSIG | 2 | |---->| |
| RRSIG | 3 | |---->| |
| RRSIG | 4 | |---->| |
| RRSIG | 5 | |---->| |
| RRSIG | 6 | |---->| |
| RRSIG | 7 | |---->| |
| RRSIG | 8 | |---->| |
| RRSIG | 9 | |---->| |

Período de validez de RRSIG DNSKEY dentro del ciclo

Figura 2

## Comprobación del conjunto de la clave de firma de la zona

El sistema del operador de KSK comprobará que los datos de firma son auténticos validando los datos de clave públicos contenidos en KSR.

## Comprobación de los registros de recursos

El sistema extractor/validador comprueba todas las firmas de registros de recursos antes de la distribución. La integridad de los contenidos de la zona sin firmar también se valida antes de la distribución.

## Registros de duración de los recursos

#### Tipo RR TTL

DNSKey 24 horas

Firmante por delegación (DS) 24 horas

RRSIG igual a la RR cubierta (varía en un máximo de 48 horas)

# AUDITORÍA DE CUMPLIMIENTO

Se lleva a cabo una auditoría anual de cumplimiento para el examen de las operaciones de DNSSEC para las operaciones del centro de datos de VeriSign y operaciones de gestión que dan apoyo a los servicios de firma de la zona TLD/GTLD, incluida la gestión de KSK y ZSK de TLD/GTLD.

## Periodicidad de la auditoría de cumplimiento de entidad

Las auditorías de cumplimiento se realizan al menos una vez al año a cargo exclusivo de la entidad auditada.

## Identidad y titulación del auditor

Las auditorías de cumplimiento de VeriSign las lleva a cabo una empresa pública de auditoría que demuestre competencia en tecnología de infraestructuras de claves públicas DNSSEC, herramientas y técnicas de seguridad de la información, auditoría de seguridad y funciones de certificación de terceros y esté acreditada por el American Institute of Certified Public Accountants (Instituto Americano de auditoras públicas certificadas, AICPA, en sus siglas en inglés), que exige que se tengan ciertos conjuntos de habilidades, medidas de aseguramiento de la calidad, tales como revisión inter pares, pruebas de competencia, normas respecto a la correcta asignación de personas a los contratos y requisitos para continuar la formación profesional.

## Relación del auditor con el auditado

Las auditorías de cumplimiento de las operaciones de VeriSign las lleva a cabo una empresa de auditoría pública independiente de VeriSign. Los terceros auditores no participarán en el control multipersonal para las ZSK y KSK de TLD/GTLD.

## Cuestiones analizadas en la auditoría

El alcance de la auditoría de cumplimiento anual de VeriSign incluye todas las operaciones de DNSSEC, tales como controles medioambientales de claves, operaciones de gestión de claves, controles administrativas y de infraestructuras, KSK y ZSK de TLD/GTLD y divulgación de gestión y prácticas de ciclo de vida de la firma.

## Medidas adoptadas como consecuencia de deficiencias

Respecto a las auditorías de cumplimiento de las operaciones de VeriSign, las excepciones o deficiencias significativas detectadas durante la auditoría de cumplimiento darán lugar a la determinación de acciones a adoptar. Esta determinación la realizará la dirección de VeriSign atendiendo a lo indicado por el auditor. La directiva de VeriSign será responsable del desarrollo y aplicación de un plan de acción correctivo. Si VeriSign decide que tales excepciones o deficiencias suponen una amenaza inmediata para la seguridad o integridad de las KSK y ZSK de TLD/GTLD, se desarrollará un plan de acción correctivo en el plazo de 30 días y se aplicará en un período de tiempo comercialmente razonable. Respecto a excepciones o deficiencias menos graves, la directiva de VeriSign evaluará la importancia de los problemas y decidirá el plan de acción oportuno.

## Comunicación de los resultados

Se puede encontrar una copia de la certificación de la directiva de VeriSign en [http://www.VeriSigninc.com/en\_US/repository/index.xhtml.](http://www.verisigninc.com/en_US/repository/index.xhtml)

# TEMAS JURÍDICOS

## Honorarios

No aplicable.

## Responsabilidad económica

No aplicable.

## Confidencialidad de la información comercial

### Alcance de la información confidencial

Los siguientes registros se mantendrán con carácter confidencial y privado (Información confidencial y privada):

* Claves privadas e información necesaria para recuperar dichas claves privadas
* Registros de operaciones (tanto registros completos como el seguimiento de auditoría de las operaciones)
* Registros de seguimiento de auditoría creados o conservados por VeriSign
* Informes de auditoría creados por VeriSign (en la medida en que se conserven) y sus respectivos auditores (internos o públicos)
* Planificación de contingencia y planes de recuperación ante desastres
* Medidas de seguridad para controlar las operaciones del hardware y software de VeriSign y la administración de claves DNS.

### Tipos de información no considerada confidencial

Toda la información correspondiente a la base de datos de dominios de primer nivel es información pública. Las claves públicas, revocación de claves y otra información de estado, así como los archivos de VeriSign e información contenida en ellos que no sea considerada Información confidencial y privada.

### Responsabilidad de protección de la información confidencial

VeriSign protege la información confidencial frente a compromisos y divulgación a terceros.

## Protección de la información de carácter personal

### Información tratada como privada

En la medida en que VeriSign reciba o procese, en nombre de un cliente, información identificable personalmente al prestar servicios de TLD/GTLD, dicha información será tratada como privada de conformidad con la Política de protección de datos de VeriSign, según se establece en [http://www.VeriSigninc.com/en\_US/privacy/index.xhtml.](http://www.verisigninc.com/en_US/privacy/index.xhtml)

### Información no considerada privada

Con sujeción a la legislación aplicable, toda la información que deba publicarse como parte de una base de datos Whois no se considerará privada.

### Responsabilidad de protección de la información privada

Al prestar servicios de TLD/GTLD, VeriSign actúa como procesador de datos y no como controlador de los mismos, y cualesquiera obligaciones que VeriSign pueda tener respecto a cualquier información identificable personalmente se regirá, con sujeción a la legislación aplicable, por el contrato con el cliente aplicable y en la medida en que no exista tal contrato por la Política de protección de datos establecida en [http://www.VeriSigninc.com/en\_US/privacy/index.xhtml.](http://www.verisigninc.com/en_US/privacy/index.xhtml)

### Divulgación en virtud de un proceso judicial o administrativo

VeriSign podrá divulgar Información confidencial y privada si, de buena fe, considera que es necesario para dar respuesta a procesos judiciales, administrativos o jurídicos de otra índole durante el proceso de investigación en una acción civil o administrativa, tales como citaciones, interrogatorios, solicitudes de admisión y solicitudes de elaboración de documentos.

## Limitaciones de la responsabilidad

VeriSign no será responsable de ninguna pérdida económica o derivada de daños incidentales o perjuicios derivados del cumplimiento de sus obligaciones en virtud del presente documento o del cumplimiento de las obligaciones del jefe de la zona TLD/GTLD y operadores de KSK y ZSK de la zona TLD/GTLD a tenor de la Declaración de prácticas de DNSSEC para el operador de KSK y ZSK de la zona TLD/GTLD. No se aceptará ninguna otra responsabilidad implícita o explícita.

## Vigencia y terminación

* + 1. **Vigencia**

La DPS entrará en vigor con su publicación en el archivo de VeriSign. Posibles modificaciones a la misma entrarán en vigor con su publicación en el archivo de VeriSign.

* + 1. **Terminación**

La presente DPS y posteriores modificaciones permanecerán en vigor hasta que sea sustituida por una versión nueva.

* + 1. **Disposición sobre resolución de conflictos**

Los conflictos entre participantes de DNSSEC se resolverán de conformidad con las disposiciones de los contratos aplicables entre las partes. Los conflictos que afecten a VeriSign exigirán un período inicial de negociación de sesenta (60) días, transcurridos los cuales se procederá a su resolución ante el tribunal federal o estatal correspondiente del condado de Fairfax, Virginia.

* + 1. **Legislación aplicable**

La presente DPS se regirá por las leyes de la mancomunidad de Virginia.

**Anexo A. Tabla de acrónimos y definiciones**

* 1. **Acrónimos**

**Índice de acrónimos**

|  |  |
| --- | --- |
| **Vigencia** | **Definición** |
| AD | Indicador de datos autenticados |
| AICPA | American Institute of Certified Public Accountants |
| BIND | Berkley Internet Name Domain (Nombre de dominio de |
| CC | Criterios comunes |
| CD | Comprobación deshabilitada |
| DNS | Sistema de nombre de dominio |
| DNSKEY | Clave de sistema de nombre de dominio |
| DNSSEC | Extensiones de seguridad del sistema de nombre de |
| DO | Indicador OK DNSSEC |
| DPS | Declaración de prácticas de DNSSEC |
| DS | Firmante por delegación |
| EAL | Nivel de aseguramiento de la evaluación (en virtud de loscriterios comunes) |
| FIPS | Federal Information Processing Standards (Normas |
| FISMA | Federal Information Security Management Act (Ley |
| gTLD | Dominio genérico de primer nivel |
| HSM | Módulo de seguridad de hardware |
| ISO | Organización Internacional de Normalización |
| KSKO | Operador de claves de firma de claves |
| NIST | National Institute of Standardization of Technology |
| NS | Servidor de nombres |
| NSEC | NextSecure (siguiente seguro) |
| NSEC3 | NextSecure3 (3 siguientes seguros) |
| PKI | Infraestructura de claves públicas |
| PMA | Autoridad de gestión de políticas |
| RFC | Solicitud de comentarios |
| RRSIG | Firma de registros de recursos |
| SEP | Punto de entrada seguro |
| SHA | Algoritmo de almohadilla seguro |
| SOA | Autoridad de inicio |
| SP | Publicación especial NIST |
| TLD | Dominio de primer nivel |
| TSIG | Firma de operaciones |
| TTL | Vida útil |
| VERT | Equipo de respuesta a urgencias de VeriSign |
| VSIRT | Equipo de respuesta a incidentes de seguridad de VeriSign |
| ZSKO | Operador de claves de firma de la zona |

* 1. **Definiciones**

**Definiciones**

|  |  |
| --- | --- |
| **Vigencia** | **Definición** |
| Cadena de confianza | Los registros de las claves DNS, firmas y firmante pordelegación unidos forman una cadena de datos firmados. |
| Compromiso | La violación (o presunta violación) de una política de seguridad, en la que se produce una divulgación no autorizada o pérdida de control sobre información sensible. Respecto a las claves privadas, un Compromiso es una pérdida, robo, divulgación, modificación o uso no autorizados y otros compromisos de la seguridad de tales claves privadas. |
| Auditoría de Cumplimiento | Auditoría periódica a la que se someten el Centro de procesamiento, Centro de servicios, Cliente PKI gestionado oCliente de entrada para determinar su cumplimiento de las normas que le son aplicables. |
| Información confidencial y privada | Información que debe mantenerse confidencial y privada. |
| Delegation Signer (DS) | Firmante por delegación (DS) es uno de los registros de recursos del archivo de la zona que indica que la zona delegada se ha firmado digitalmente. También garantiza que la zona principal reconoce la clave indicada para la zona delegada. |
| Derechos de propiedad intelectual (IPR) | Derechos en virtud de cualquier derecho de autor, patente,secreto comercial, marca comercial y cualquier otro derecho de propiedad intelectual. |
| Isla de seguridad | Una zona firmada que no tiene una cadena de confianza de la zonaprincipal. |
| Acto de generación de claves | Procedimiento por el que se genera un par de claves, su clave privada se transfiere a un módulo criptográfico, se hace una copia de respaldo de la misma y/o sus conjuntos de claves se firman. |
| Clave de firma de claves (KSK) | Una clave que firma el conjunto de claves. |
| Revisión de gestión | Auditoría de cumplimiento de la entidad o como parte del proceso de gestión de riesgos general durante la actividad comercial normal. |
| HSM fuera de línea | HSM que se mantienen fuera de línea por razones de seguridad a fin de protegerlos de posibles ataques de intrusos a través de la red. Estos HSM no firman directamente el archivo de la zona |
| HSM en línea | Los HSM que firman el archivo de la zona en virtud de la clavede firma de la zona se mantienen en línea para ofrecer servicios de firma continuos. |
| Zona principal | Zona que está en un nivel superior. |
| Autoridad de gestión de políticas (PMA) | Organización dentro de VeriSign responsable depublicar esta política. |
| Public Key Infrastructure | La arquitectura, organización, técnicas, prácticas y procedimientos que apoyan colectivamente la aplicación y funcionamiento de un sistema criptográfico de claves público. |
| Institución financiera regulada | Institución financiera que es regulada, supervisada y examinada por autoridades del gobierno, nacionales, estatales, provinciales o locales, que tienen facultades regulatorias sobre la misma con base en leyes del gobierno, nacionales, estatales, provinciales o locales en virtud de las que la institución financiera se constituye y tiene permiso para actuar. |
| Firma de registros de recursos (RRSIG) | Datos de firma del archivo de la zona. |
| RSA | Sistema criptográfico de claves público inventado por Rivest, Shamir y Adelman. |
| Parte del secreto | Parte de una clave privada o de los datos de activación necesarios para activar una clave privada conforme a uncontrato de uso compartido de secretos. |
| Riesgo complementario | Revisión de una entidad por parte de VeriSign tras detectar excepciones o deficiencias en una auditoría de cumplimiento de la entidad como parte del proceso de gestión de riesgos generaldurante la actividad comercial normal. |
| Posición de confianza | Posiciones dentro de las operaciones de DNSSEC que deben ocupar personas de confianza. |

|  |  |
| --- | --- |
| VeriSign | Respecto a cada parte pertinente del presente documento hace referencia a VeriSign, Inc. y a cualquier filial de completa titularidad de VeriSign responsable de las operaciones específicas en cuestión. |
| Archivo | Información relativa a DNSSEC accesible en línea. |
| Zona | Límite de responsabilidad para cada dominio. |
| Clave de firma de la zona (ZSK) | Clave que firma la zona COM |

**Anexo B. Histórico de modificaciones**

#### Histórico de modificaciones: Versión 1.0

|  |  |
| --- | --- |
| **Sección** | **Descripción** |
| Creación de la primera edición | **N/D** |
|  |  |
|  |  |
|  |  |
|  |  |