D&L

DECLARACIÓN DE PRÁCTICAS

Servicio de Valor Añadido como
Autoridad de Sellado de Tiempo

Información del documento	
Nombre de documento: Declaración de Prácticas del Servicio de Valor Añadido como Autoridad de Sellado de Tiempo DIGILINK	
Nombre de documento: DL-DPSVA-01	
Versión: 2.1	Aprobado por: Responsable del Servicio de Valor Añadido
Año: 2024	Dirigido a: INDECOPI

Control de versiones		
Versión	Fecha	Descripción
1.0	03-01-2022	Elaboración de documento inicial.
1.1	22-03-2022	Se realizaron cambios en el formato.
1.2	04-09-2023	Se realizaron cambios en el formato. Se ha incluido el logo y el código en la cabecera del documento.
2.0	18-09-2023	Se realizaron cambios en el documento. Se ha incluido el ítem 22. Niveles de Servicio.
2.1	25-01-2024	Cambio de Representante Legal de la empresa.

ÍNDICE

1	INTRODUCCIÓN	6
2	OBJETIVO	6
3	OBJETO DE LA ACREDITACIÓN	6
4	RESPONSABILIDADES.....	6
5	DEFINICIONES Y ABREVIACIONES	7
	5.1 DEFINICIONES	7
	5.2 ABREVIACIONES	8
6	PARTICIPANTES.....	8
	6.1 AUTORIDAD DE SELLADO DE TIEMPO DIGILINK (TSA DIGILINK).....	8
	6.2 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL.....	8
7	POLÍTICA DE SELLADO DE TIEMPO.....	8
8	IDENTIFICACIÓN	9
9	COMUNIDAD DE USUARIOS Y APLICABILIDAD.....	9
10	OBLIGACIONES Y RESPONSABILIDAD.....	9
	10.1 OBLIGACIONES DE LA TSA EN RELACIÓN A LOS SUSCRIPTORES	9
	10.2 OBLIGACIONES DE LOS SUSCRIPTORES	9
	10.3 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN.....	9
11	REQUERIMIENTOS EN LAS PRÁCTICAS DE LA TSA.....	10
	11.1 DECLARACIÓN Y PUBLICACIÓN DE PRÁCTICAS.....	10
	11.2 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DEL SVA	10
	11.3 FRECUENCIA DE PUBLICACIÓN	10
12	CONDICIONES Y TÉRMINOS DE USO.....	10
13	APROBACIÓN DEL DOCUMENTO DE DECLARACIÓN DE PRÁCTICAS.....	11
14	EVALUACIÓN DE CUMPLIMIENTO	11
15	CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES	11
	15.1 CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA.....	11
	15.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN	11
	15.1.2 ACCESO FÍSICO.....	11
	15.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO	12
	15.1.4 EXPOSICIÓN AL AGUA.....	12
	15.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS	12
	15.1.6 SISTEMA DE ALMACENAMIENTO	12
	15.1.7 ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN.....	12
	15.2 CONTROLES DE PROCEDIMIENTO	12
	15.2.1 ROLES DE CONFIANZA.....	12
	15.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA.....	13
	15.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL	13
	15.2.4 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES.....	13
	15.3 CONTROLES DE PERSONAL.....	14
	15.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES	14
	15.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES	14
	15.3.3 REQUISITOS DE FORMACIÓN.....	14

15.3.4	REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN.....	15
15.3.5	FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS.....	15
15.3.6	SANCIONES POR ACTUACIONES NO AUTORIZADAS.....	15
15.3.7	REQUISITOS DE CONTRATACIÓN DE TERCEROS.....	15
15.3.8	DOCUMENTACIÓN PROPORCIONADA AL PERSONAL.....	15
15.4	PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD	16
15.4.1	TIPOS DE EVENTOS REGISTRADOS.....	16
15.4.2	FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)	17
15.4.3	PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA	17
15.4.4	PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA.....	17
15.4.5	PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA	18
15.4.6	SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA).....	18
15.4.7	NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO.....	18
15.4.8	ANÁLISIS DE VULNERABILIDADES	18
15.5	ARCHIVO DE REGISTROS	19
15.5.1	TIPOS DE EVENTOS ARCHIVADOS	19
15.5.2	PERIODO DE CONSERVACIÓN	19
15.5.3	PROTECCIÓN DE ARCHIVOS	19
15.5.4	PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS.....	19
15.5.5	REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS	20
15.5.6	SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)	20
15.5.7	PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA.....	20
15.6	CAMBIO DE CLAVES DE UNA EC.....	20
15.7	RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE	20
15.7.1	PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES	20
15.7.2	ALTERACIÓN DE LOS RECURSOS HARDWARE, SOFTWARE Y/O DATOS.....	21
15.7.3	PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA AUTORIDAD	22
15.7.4	CAPACIDAD DE RECUPERACIÓN DESPUÉS DE UN DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE.....	22
16	AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES	22
16.1	FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES.....	22
16.2	IDENTIDAD/CUALIFICACIÓN DEL AUDITOR.....	22
16.3	RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA	23
16.4	ASPECTOS CUBIERTOS POR LOS CONTROLES	23
16.5	ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS	24
16.6	COMUNICACIÓN DE RESULTADOS.....	24
17	NOTIFICACIÓN DE CAMBIOS.....	24
18	INFORMACIÓN DE CONTACTO	24
19	CICLO DE VIDA DE LA GESTIÓN DE CLAVE	25
19.1	GENERACIÓN DE LA CLAVE DE LA TSA.....	25
19.2	CARACTERÍSTICAS TÉCNICAS DEL CERTIFICADO DIGITAL Y DE LOS ALGORITMOS UTILIZADOS	25
19.3	PROTECCIÓN DE LA CLAVE PRIVADA DE LA TSA.....	25
19.4	DISTRIBUCIÓN DE LA CLAVE PÚBLICA TSU	26
19.5	RE-EMISIÓN DE LA CLAVE DE LA TSU.....	26
19.6	GESTIÓN DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRÁFICO DE FIRMA.....	26
19.7	TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA DEL TSU	27
20	SELLO DE TIEMPO	27
20.1	SINCRONIZACIÓN DEL RELOJ CON LA UTC	27
21	TÉRMINO DE LA TSA	27

22	NIVELES DE SERVICIO.....	28
23	CUMPLIMIENTO DE REQUERIMIENTOS LEGALES.....	28
24	CONFORMIDAD	28

1 INTRODUCCIÓN

DIGILINK S.AC., que en adelante llamaremos “DIGILINK”, es una empresa peruana especializada en brindar servicios digitales innovadores de confianza basados en la firma digital desde el año 2021.

Entre sus servicios se encuentran sus funciones como Entidad de Certificación, Entidad de Registro y Autoridad de Sellado de Tiempo, para lo cual DIGILINK se encuentra acreditada ante el INDECOPI para su debido ejercicio.

En calidad de Entidad de Certificación, por medio de su proveedor de servicios GLOBALSIGN, emite certificados digitales a personas naturales y jurídicas.

Como Entidad de Registro, brinda los servicios de verificación de sus clientes, tanto para representantes legales, empleados o agentes automatizados, para la emisión, re-emisión o revocación de certificados digitales; así como el registro de las evidencias generadas.

Como entidad de Sellado de Tiempo, DIGILINK asume las responsabilidades de representación de los servicios de sello de tiempo brindados mediante su proveedor GLOBALSIGN, la cual es una infraestructura tercerizada y certificada.

2 OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas que utiliza DIGILINK para la administración de sus servicios como SVA de Sellado de Tiempo, en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)” establecida por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de emisión de sellos de tiempo brindados por DIGILINK a través de GLOBALSIGN. Esta última cuenta con la certificación Webtrust Program for Certification Authorities emitida por AICPA/CICA y certificación eIDAS; para todos los procesos de gestión y operación de los servicios de emisión de sellos de tiempo y certificados digitales.

4 RESPONSABILIDADES

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por GLOBALSIGN de acuerdo a su documento Declaración de Prácticas de Certificación publicado en:

<https://www.globalsign.com/en/repository>

DIGILINK cuenta con GLOBALSIGN para todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación GLOBALSIGN.

Asimismo, DIGILINK brinda los servicios de registro o verificación conforme a las Guías de Acreditación del INDECOPI, para realizar la verificación de identidad de las personas jurídicas y naturales solicitantes de los certificados digitales.

Las peticiones, quejas o reclamos sobre los servicios prestados por GLOBALSIGN a través de la Entidad de Certificación DIGILINK son recibidas directamente por DIGILINK. La línea telefónica para la atención a titulares y terceros para consultas relacionadas con el servicio que dispone DIGILINK es permanente.

5 DEFINICIONES Y ABREVIACIONES

5.1 DEFINICIONES

Autoridad de Sellado de Tiempo (TSA)	Autoridad que emite los sellos de tiempo, en los cuales confían los suscriptores y terceros que confían.
Declaración de Prácticas de la TSA	Conjunto de declaraciones acerca de políticas y prácticas que dirigen las actividades y procesos de la TSA y que son publicadas para conocimiento de suscriptores y terceros que confían.
Política de Sellado de Tiempo	Conjunto de directivas que dirigen la aplicabilidad y requisitos en la administración de un servicio de sello de tiempo para una determinada comunidad de usuarios y un determinado alcance.
Sello de Tiempo	Conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez. El sello de tiempo incluye: - La firma digital de la entidad de sellado de tiempo - Identificador electrónico único del documento (HASH o resumen) - Fecha y hora recogida de una fuente fiable de tiempo
Unidad de Sellado de Tiempo	Componentes de hardware y software que son administrados como una unidad para proveer sellos de tiempo desde una fuente de tiempo. Todas las TSU mencionadas en el presente documento pertenecen a GLOBALSIGN.
Sistemas de la TSA	Sistemas de tecnologías de la información que soportan la provisión de servicios de sellado de tiempo.

Suscriptor	Persona natural o jurídica que requiere los servicios provistos por una Autoridad emisora de sellos de tiempo – TSA y que está conforme con los acuerdos y obligaciones descritos en la Declaración de Prácticas y la Política de Sellado de Tiempo.
Tercero que confía	Persona natural o jurídica que recibe un documento con un sello de tiempo y confía en la validez de dicho sello provisto por la TSA de DIGILINK y GLOBALSIGN.

5.2 ABREVIACIONES

BIPM International Bureau of Weights and Measures (Bureau International Des Poids et Mesures)

GMT Greenwich Mean Time

IERS International Earth Rotation Service

TAI International Atomic Time (Temps atomique international)

TSA Time-Stamping Authority

TSU Time-Stamping Unit

UTC Coordinated Universal Time

6 PARTICIPANTES

6.1 AUTORIDAD DE SELLADO DE TIEMPO DIGILINK (TSA DIGILINK)

DIGILINK, en su papel de Autoridad de Sellado de Tiempo, es la persona jurídica privada que presta indistintamente servicios de emisión de sellados de tiempo

6.2 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL

La operación de los servicios de sellado de tiempo que ofrece DIGILINK son provistos por la Entidad de Certificación DIGILINK y su proveedor de infraestructura GLOBALSIGN, la cual emite certificados de firma electrónica.

7 POLÍTICA DE SELLADO DE TIEMPO

DIGILINK reconoce la Declaración de Prácticas de Certificación (CPS) y Política de Sellado de Tiempo de GLOBALSIGN, exigiendo su conformidad con la RFC 3628.

8 IDENTIFICACIÓN

La Política de Sellado de Tiempo de GLOBALSIGN, reconocida por DIGILINK tiene un identificador único:

- 1.3.6.1.4.1.4146.1.30 Timestamping Certificates Policy

iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 4146 certificate-policies(1) time-stamping(30)

9 COMUNIDAD DE USUARIOS Y APLICABILIDAD

DIGILINK no limita la comunidad de usuarios de los servicios de sellado de tiempo, estos pueden ser personas jurídicas del sector privado o estatal que deseen utilizar los sellos de tiempo de GLOBALSIGN y que estén de acuerdo con su Declaración de Prácticas y su Política de Sellado de Tiempo.

10 OBLIGACIONES Y RESPONSABILIDAD

DIGILINK, por medio de su proveedor GLOBALSIGN, asegura que los sistemas, personas y procesos que conforman los servicios de sellado de tiempo, cumplan con los requerimientos definidos en el ETSI EN 319 401 [4], verificando su cumplimiento con periodicidad.

En este sentido, DIGILINK se hace responsable de cumplir con las obligaciones contractuales y niveles de servicio acordados con cada cliente.

10.1 OBLIGACIONES DE LA TSA EN RELACIÓN A LOS SUSCRITORES

DIGILINK entregará los servicios con la confiabilidad y exactitud establecida en los respectivos contratos, en las respectivas políticas de sellado de tiempo y en el presente documento.

10.2 OBLIGACIONES DE LOS SUSCRITORES

Es responsabilidad de los suscriptores utilizar una aplicación de software acreditada ante el INDECOPI que realice las peticiones e interprete las respuestas conforme al formato establecido en la RFC 3161, las verificaciones del estado del certificado, así como realizar la correcta configuración de la hora local en estas aplicaciones.

10.3 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Los terceros que confían son responsables de verificar que los documentos sean firmados con un sello de tiempo, con un certificado digital reconocido por DIGILINK y que estos sellos tengan como parte de su número de identificación el OID, la identificación de la respectiva política de sellado de tiempo de GLOBALSIGN.

Asimismo deben verificar que el certificado de sello de tiempo se encuentra firmado y que la clave privada no estuvo comprometida en el momento en el que se realizó el sellado de tiempo.

11 REQUERIMIENTOS EN LAS PRÁCTICAS DE LA TSA

DIGILINK, por medio de su proveedor GLOBALSIGN, cumple los requerimientos del ETSI EN 319 401 [4], en su calidad de Autoridad de Sellado de Tiempo.

DIGILINK demuestra que cuenta con la confiabilidad necesaria para proveer los servicios de sellado de tiempo a sus clientes, a través del sometimiento de sus servicios a la evaluación provista por el INDECOPI como Autoridad Administrativa Competente.

Los certificados e infraestructura de software y hardware utilizados en los servicios de emisión de sellos de tiempo son provistos por GLOBALSIGN, cuya infraestructura es administrada rigurosamente evaluada por las auditorías para el logro de las certificaciones eIDAS, WebTrust for CA e ISO 27001.

Las evidencias de estas auditorías serán presentadas al INDECOPI en cada sesión de auditoría periódica.

11.1 DECLARACIÓN Y PUBLICACIÓN DE PRÁCTICAS

DIGILINK cuenta con una Declaración de Prácticas de la TSA la cual es de acceso público mediante su página web: WEB

11.2 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DEL SVA

El Responsable de la TSA de DIGILINK se encarga de administrar la presente Declaración de Prácticas de la TSA y los demás documentos relativos a este servicio.

11.3 FRECUENCIA DE PUBLICACIÓN

La Declaración de Prácticas de la TSA debe ser reconocida y validada ante INDECOPI anualmente desde su acreditación.

En caso se realicen modificaciones en el presente documento, estos cambios serán notificados a INDECOPI y publicados luego de su aprobación.

12 CONDICIONES Y TÉRMINOS DE USO

Las condiciones y términos de uso de los servicios de sellado de tiempo para todos los suscriptores y terceros corresponden serán definidos con cada cliente en los contratos con los suscriptores.

Será responsabilidad del suscriptor difundir, conforme corresponda en términos de confidencialidad, las condiciones adicionales que sean establecidas en el contrato, a toda la comunidad de usuarios que defina para el uso de los servicios contratados.

13 APROBACIÓN DEL DOCUMENTO DE DECLARACIÓN DE PRÁCTICAS

La presente Declaración de Prácticas y las Políticas de Sellado de Tiempo, son aprobadas y reconocidas por DIGILINK y su cumplimiento es supervisado por la autoridad máxima dentro de la TSA.

14 EVALUACIÓN DE CUMPLIMIENTO

DIGILINK y a la vez su proveedor GLOBALSIGN, como Autoridad emisora de sellos de tiempo, se someten a auditorías periódicas por parte del INDECOPI, como Autoridad Administrativa Competente. Asimismo, DIGILINK requiere a GLOBALSIGN el cumplimiento del reglamento eIDAS, WebTrust, y del estándar ISO 27001 para su infraestructura de sellado de tiempo.

15 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

15.1 CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA

GLOBALSIGN como prestador de servicios de DIGILINK, mantiene políticas de seguridad física y ambiental para los sistemas utilizados para la emisión y gestión de certificados que abarcan el control de acceso físico, protección contra desastres naturales, factores de seguridad contra incendios, fallas en las utilidades de apoyo (por ejemplo, energía, telecomunicaciones), colapso de estructuras y la recuperación de desastres. Los controles son implementados para evitar la pérdida, daño o compromiso de los activos y la interrupción de las actividades empresariales y el robo de la información y las instalaciones de procesamiento de la información.

15.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

GLOBALSIGN se encuentra dentro de un centro de datos seguro. El centro de datos es una instalación construida específicamente de hormigón y construcción de acero.

15.1.2 ACCESO FÍSICO

GLOBALSIGN opera dentro de un centro de datos seguro que proporciona seguridad con escáneres biométricos y sistemas de acceso a tarjetas. Se proporciona un sistema de vigilancia 24x7, circuito cerrado de circuito (CCTV) así como una grabación digital. Los guardias de seguridad calificados aseguran las instalaciones físicas y sólo a personal autorizado y personal de seguridad se les permite entrar en las instalaciones.

15.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

GLOBALSIGN opera dentro de un centro de datos seguro que está equipado con redundancia de energía y sistema de refrigeración. El UPS y la conmutación por error al generador de energía están en su lugar en el caso improbable de corte de energía.

15.1.4 EXPOSICIÓN AL AGUA

GLOBALSIGN está protegida contra el agua. Se encuentra sobre rasante y en una planta superior con suelo técnico. Además, hay un sistema de alarma de detección de agua y el personal de operaciones del centro de datos en el sitio está listo para responder a cualquier exposición al agua poco probable.

15.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

GLOBALSIGN opera dentro de un centro de datos seguro que está equipado con un sistema de detección y supresión de incendios.

15.1.6 SISTEMA DE ALMACENAMIENTO

El almacenamiento de los medios de respaldo está fuera del sitio, físicamente asegurado y protegido contra incendios y daños por agua.

15.1.7 ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

GlobalSign asegura que todos los medios utilizados para el almacenamiento de información sean desclasificados o destruidos de una manera generalmente aceptada antes de ser liberados para su eliminación.

15.2 CONTROLES DE PROCEDIMIENTO

15.2.1 ROLES DE CONFIANZA

GLOBALSIGN, como proveedor de infraestructura de DIGILINK, garantiza que todos los operadores y administradores, incluidos los especialistas en validación, actúen en la capacidad de un rol de confianza. Los roles de confianza son tales que no es posible ningún conflicto de intereses y los roles se distribuyen de manera que ninguna persona pueda eludir la seguridad del sistema de la EC.

Los roles de confianza incluyen, entre otros, los siguientes:

- **Desarrollador:** Responsable del desarrollo de sistemas de la EC.
- **Oficial de Seguridad / Jefe de Seguridad de la Información:** Responsabilidad general de administrar la implementación de las prácticas de seguridad de la EC;
- **Ingeniero de sistemas de Infra:** Autorizado para instalar, configurar y mantener los sistemas de la EC utilizados para la Gestión del ciclo de vida del certificado;

- **Operador de Infra:** Responsable de operar los sistemas de la EC en el día a día. Autorizada para realizar la copia de seguridad / recuperación del sistema, ver / mantener los archivos del sistema de la EC y los registros de auditoría;
- **Auditor:** Autorizado para ver archivos y registros de auditoría de los Sistemas Confiables de la EC;
- **Titular de datos de activación de CA:** Persona autorizada que contiene los datos de activación de la EC necesarios para la operación de módulo de seguridad de hardware de la EC;
- **Operador de Registro:** Es el responsable de verificar que la información suministrada por los solicitantes de certificados digitales sea auténtica e íntegra. Es el responsable de solicitar en nombre de los titulares la emisión o revocación de certificados digitales.
- **Titular de los datos de activación de CA:** persona autorizada que posee los datos de activación de la EC, necesario para el funcionamiento del módulo de seguridad de hardware de la EC.

15.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

Las claves privadas de la EC son respaldadas, almacenadas y recuperadas solo por personal en roles confiables usando, al menos, control dual en un ambiente físicamente seguro.

15.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Antes de designar a una persona a un rol de confianza, GLOBALSIGN realiza una comprobación de antecedentes. Cada función descrita anteriormente está identificada y autenticada de manera que garantice que la persona adecuada desempeñe el papel adecuado para apoyar a la EC.

15.2.4 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

GLOBALSIGN impone la separación de funciones, ya sea por el equipo de EC o por procedimientos o por ambos medios.

El personal de la EC se asigna específicamente a las funciones definidas en la Sección 28.2.1 anterior.

Los roles que requieren una separación de funciones incluyen:

- Los que realizan la aprobación de la generación y revocación de certificados (Operadores de Registro)
- Quienes realizan la instalación, configuración y mantenimiento de los sistemas CA (Ingeniero de sistema de Infra)
- Aquellos con la responsabilidad general de administrar la implementación de las prácticas de seguridad de la EC (Oficial de Seguridad)
- Aquellos que realizan tareas relacionadas con la gestión del ciclo de vida de las claves criptográficas (por ejemplo, custodios de componentes de claves). (Titular de los datos de activación de CA)
- Aquellos que realizan el desarrollo de sistemas de la EC (Desarrolladores)
- Aquellos que realizan la auditoría de sistemas de la EC (Operador de Infra, Auditor)

15.3 CONTROLES DE PERSONAL

15.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

Antes de la participación de cualquier persona en el Proceso de gestión de certificados, ya sea como empleado, agente o contratista independiente, GlobalSign verifica la identidad y la confiabilidad de dicha persona

GLOBALSIGN, como proveedor de infraestructura y operaciones de DIGILINK, emplea una cantidad suficiente de personal que posee el conocimiento experto, la experiencia y las calificaciones necesarias para los servicios ofrecidos, según corresponda a la función laboral.

El personal de la EC de GlobalSign cumple con el requisito a través de conocimientos, experiencia y calificaciones profesionales con capacitación y educación formal, experiencia real o una combinación de ambos. Las funciones y responsabilidades confiables, como se especifica en la Sección 28.2.1, se documentan en las descripciones de trabajo. El personal de la EC de GlobalSign (tanto temporales como permanentes) tiene descripciones de tareas definidas desde el punto de vista de separación de deberes y menos privilegio, determinando la sensibilidad de posición en función de los derechos y niveles de acceso. El personal de la EC de GlobalSign es formalmente nombrado para funciones de confianza.

15.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

Todo el personal de la EC de GlobalSign en funciones de confianza está libre de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones de la EC. GlobalSign no designa a un rol de confianza a ninguna persona conocida por vincularse con un delito grave u otro delito si tal convicción afecta su idoneidad para el puesto. El personal no tiene acceso a las funciones de confianza hasta que se completen los controles necesarios y se analicen los resultados, siempre y cuando dichos controles sean permitidos por la jurisdicción en la que la persona será empleada. Todas las personas que ocupen roles de confianza serán seleccionadas sobre la base de lealtad, confiabilidad e integridad, y estarán sujetas a investigación de antecedentes donde lo permita la ley.

Cualquier uso de la información revelada por los archivos de antecedentes por GlobalSign debe estar en conformidad con las leyes aplicables de la jurisdicción donde la persona está empleada.

15.3.3 REQUISITOS DE FORMACIÓN

GLOBALSIGN, como proveedor de infraestructura y operaciones de DIGILINK, proporciona a todo el personal que realiza tareas de verificación de información capacitación en habilidades que cubren conocimientos básicos de Infraestructura de clave pública, políticas y procedimientos de autenticación y

verificación (incluida la Política de certificados y/o Declaración de prácticas de certificación), amenazas comunes al proceso de verificación de información (incluido el phishing). y otras tácticas de ingeniería social) y los requisitos básicos.

GlobalSign mantiene registros de dicha capacitación y garantiza que el personal encargado de las tareas como Operadores de Registro mantenga un nivel de habilidad que le permita realizar dichas tareas de manera satisfactoria.

GlobalSign documenta que cada Operador de Registro posee las habilidades requeridas por una tarea antes de permitir que el especialista en validación realice esa tarea.

GlobalSign requiere que todos los especialistas en validación aprueben un examen proporcionado por la EC sobre los requisitos de verificación de información descritos en los Requisitos básicos.

15.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

Todo el personal en roles de confianza mantiene niveles de habilidad consistentes con la capacitación anual de GlobalSign y programas de desempeño con relevancia para su rol de confianza.

Cualquier cambio significativo en las operaciones cuenta con un plan de capacitación (concientización), y la ejecución de tal el plan está documentado.

GlobalSign brinda capacitación en seguridad y privacidad de la información al menos una vez al año a todos los empleados.

15.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS

GlobalSign asegura que cualquier cambio en el personal no afectará la efectividad operativa del servicio o la seguridad del sistema.

15.3.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS

Se aplican sanciones disciplinarias apropiadas al personal que viola las disposiciones y políticas dentro de la PC, DPC y procedimientos operativos relacionados con la EC de GLOBALSIGN, como proveedor de servicios de DIGILINK.

15.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS

El personal contratado empleado para las operaciones de GlobalSign está sujeto al mismo proceso, procedimientos, evaluación, control de seguridad y capacitación como personal permanente de la EC.

15.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

GlobalSign pone a disposición de su personal su CPS, cualquier CP correspondiente y cualquier estatuto, política o contrato pertinente. Se proporcionan otros documentos técnicos, operativos y administrativos (por

ejemplo, manuales de administrador, manuales de usuario, etc.) para que el personal de confianza pueda desempeñar sus funciones.

Se mantiene la documentación que identifica a todo el personal que recibió la capacitación y el nivel de entrenamiento completado.

15.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

15.4.1 TIPOS DE EVENTOS REGISTRADOS

Se generarán archivos de registro de auditoría para todos los eventos relacionados con la seguridad y los servicios de la CA. Donde sea posible, los registros de auditoría de seguridad se generarán automáticamente. Cuando esto no sea posible, se utilizará un cuaderno de bitácora, un formulario en papel u otro mecanismo físico. Todos los registros de auditoría de seguridad, tanto electrónicos como no electrónicos, se conservarán y estarán disponibles durante las auditorías de cumplimiento.

GlobalSign garantiza que todos los eventos relacionados con el ciclo de vida de los Certificados se registren de manera que se garantice la trazabilidad a una persona en un rol de confianza para cualquier acción requerida para los servicios de CA. Como mínimo, cada registro de auditoría incluye los siguientes elementos (registrados de forma automática o manual):

- El tipo de evento;
- La fecha y hora en que ocurrió el evento;
- Éxito o fracaso cuando corresponda;
- La identidad de la entidad y / u operador que causó el evento;
- La identidad a la que se dirigió el evento; y
- La causa del evento.

GlobalSign registra los detalles de las acciones tomadas para procesar una solicitud de certificado y emitir un Certificado, incluida toda la información generada y la documentación recibida en relación con la solicitud de certificado; la hora y la fecha; y el personal involucrado. GlobalSign pone estos registros a disposición de su auditor calificado como prueba del cumplimiento de la EC con el esquema de auditoría de la EC asociado estipulado en la introducción.

GlobalSign registra al menos los siguientes eventos:

Certificado de CA y eventos de ciclo de vida de claves, que incluyen:

- Generación, respaldo, almacenamiento, recuperación, archivo y destrucción de claves;
- Solicitudes de certificados, solicitudes de renovación y renovación de claves y revocación;
- Aprobación y rechazo de solicitudes de Certificados;

- Eventos de gestión del ciclo de vida del dispositivo criptográfico; y
- Generación de listas de revocación de certificados y entradas OCSP;
- Introducción de nuevos perfiles de certificado y retiro de perfiles de certificado existentes.

Eventos de gestión del ciclo de vida del certificado de suscriptor, que incluyen:

- Solicitudes de certificados, solicitudes de renovación y renovación de claves y revocación;
- Todas las actividades de verificación estipuladas en esta CPS;
- Aprobación y rechazo de solicitudes de certificados;
- Emisión de Certificados; y
- Generación de listas de revocación de certificados y entradas OCSP.

Eventos de seguridad, que incluyen:

- Intentos de acceso al sistema PKI exitosos y fallidos;
- Acciones de PKI y del sistema de seguridad realizadas;
- Cambios de perfil de seguridad.
- Instalación, actualización y eliminación de software en un sistema de certificados;
- Fallos del sistema, fallas de hardware y otras anomalías;
- Actividades de cortafuegos y enrutadores; y
- Entradas y salidas de la instalación de CA

15.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG)

Los registros de auditoría se revisan periódicamente para detectar cualquier evidencia de actividad maliciosa y después de cada operación importante.

15.4.3 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

GlobalSign conserva todos los registros de auditoría generados durante al menos diez años. GlobalSign pone estos registros de auditoría a disposición del auditor calificado cuando lo solicite.

15.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

Los eventos se registran de tal manera que no se pueden eliminar ni destruir (excepto para transferirlos a medios a largo plazo) durante el período de tiempo que se conservan.

Los registros de eventos están protegidos para evitar alteraciones y detectar manipulaciones y para garantizar que solo las personas con acceso confiable

autorizado puedan realizar cualquier operación sin modificar la integridad, autenticidad y confidencialidad de los datos.

Los registros de eventos están sellados con fecha de manera segura que garantiza, desde la fecha de creación del registro hasta el final del período de archivo, que existe un vínculo confiable entre el evento y el momento de su realización.

15.4.5 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA

Los registros de auditoría y los resúmenes de auditoría se respaldan en una ubicación segura (por ejemplo, una caja fuerte a prueba de fuego), bajo el control de un rol de confianza autorizado y separados de la generación de su fuente de componentes. La copia de seguridad del registro de auditoría está protegida al mismo grado que los originales.

15.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

Los procesos de auditoría se inician al inicio del sistema y finalizan solo cuando se apaga. El sistema de recopilación de auditorías garantiza la integridad y disponibilidad de los datos recopilados. Si es necesario, el sistema de recopilación de auditorías protege la confidencialidad de los datos. En el caso de que ocurra un problema durante el proceso de cobro de la auditoría, GlobalSign determina si suspender las operaciones de GlobalSign hasta que se resuelva el problema, informando debidamente a los propietarios de activos afectados por GlobalSign.

15.4.7 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

No se estipula.

15.4.8 ANÁLISIS DE VULNERABILIDADES

GLOBALSIGN, en calidad de proveedor de DIGILINK, mantiene un programa de seguridad que incluye una evaluación anual de riesgos que:

- Identifica amenazas internas y externas previsibles que podrían resultar en acceso no autorizado, divulgación, uso indebido, alteración o destrucción de cualquier certificado de datos o procesos de gestión de certificados;
- Evalúa la probabilidad y el daño potencial de estas amenazas, teniendo en cuenta la sensibilidad de los datos del certificado y los procesos de gestión del certificado; y
- Evalúa la suficiencia de las políticas, procedimientos, sistemas de información, tecnología y otros arreglos que GlobalSign tiene implementados para contrarrestar tales amenazas. Con base en la evaluación de riesgos, GlobalSign desarrolla, implementa y mantiene un plan de seguridad que consta de procedimientos, medidas y productos de seguridad diseñados para lograr los objetivos establecidos anteriormente y para gestionar y controlar los riesgos identificados

durante la evaluación de riesgos, acorde con la sensibilidad de los datos del certificado y los procesos de gestión del certificado.

- El plan de seguridad incluye salvaguardas administrativas, organizativas, técnicas y físicas adecuadas a la sensibilidad de los datos del certificado y los procesos de gestión del certificado. El plan de seguridad también toma en cuenta la tecnología disponible y el costo de implementar las medidas específicas e implementa un nivel razonable de seguridad apropiado al daño que podría resultar de una violación de la seguridad y la naturaleza de los datos a proteger.

15.5 ARCHIVO DE REGISTROS

15.5.1 TIPOS DE EVENTOS ARCHIVADOS

GLOBALSIGN y la ER de DIGILINK archivan registros con suficiente detalle para establecer la validez de una firma y del funcionamiento adecuado del sistema de la EC.

15.5.2 PERIODO DE CONSERVACIÓN

GlobalSign conserva toda la documentación relacionada con las solicitudes de certificado y su verificación, y todos los Certificados y su revocación, por al menos el período de retención definido por los requisitos de WebTrust y / o eIDAS para el tipo de Certificado.

El período de retención es de 10 años después de que cualquier Certificado basado en esa documentación deje de ser válido, a menos que se especifique lo contrario en un acuerdo con GlobalSign.

15.5.3 PROTECCIÓN DE ARCHIVOS

Los archivos se crean de tal manera que no se pueden eliminar ni destruir (excepto para la transferencia a los medios de comunicación a largo plazo) dentro del período de tiempo para el que se requiere que se mantengan. Las protecciones de archivo garantizan que solo el acceso confiable autorizado pueda realizar operaciones sin modificar la integridad, autenticidad y confidencialidad de los datos. Si los medios originales no pueden retener los datos durante el período requerido, el sitio de archivo definirá un mecanismo para transferir periódicamente los datos archivados a nuevos medios.

15.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS

Se realizan copias de seguridad de archivos que son del sistema de la EC de GlobalSign en línea o del sistema sin conexión. Las copias de seguridad en línea se duplican semanalmente y cada copia de seguridad se almacena en una ubicación que es diferente del sistema en línea original. Una copia de seguridad se almacena en un medio de seguridad de seguridad contra incendios. Una copia de seguridad fuera de línea se toma al final de cualquier ceremonia clave (con la excepción de cualquier material encriptado que se almacena por

separado de acuerdo con los procedimientos de ceremonia clave) y se almacena en un lugar fuera de sitio dentro de los 30 días de la ceremonia.

15.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Si se utiliza un servicio de registro de fecha y hora para fechar los registros, debe cumplir con los requisitos definidos en la Sección 29.8. Sellado de tiempo, todos los registros deben tener datos que indiquen el momento en que ocurrió el evento.

15.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

El sistema de colección de archivos cumple con los requisitos de seguridad de la Sección 28.

15.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA.

El almacenamiento de medios de la información de archivo de la EC de GlobalSign se comprueba en el momento de su creación. Periódicamente, las muestras estadísticas de la información archivada se prueban para comprobar la integridad continuada y la legibilidad de la información.

Sólo los equipos autorizados de GlobalSign, la función de confianza y otras personas autorizadas pueden acceder al archivo. Las solicitudes para obtener y verificar la información del archivo son coordinadas por los operadores en funciones de confianza (auditor interno, el gerente encargado del proceso y el oficial de seguridad).

15.6 CAMBIO DE CLAVES DE UNA EC

GlobalSign puede cambiar periódicamente el material clave para las ECs Emisoras de acuerdo a la sección 29.3.2. También se puede modificar la información del Sujeto del certificado y modificar los perfiles de Certificado para que se adhieran a las mejores prácticas. Las claves privadas utilizadas para firmar certificados de suscriptor anteriores se mantienen hasta que expiren todos los certificados de suscriptor.

15.7 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

15.7.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

GlobalSign tiene un plan de respuesta a incidentes y un plan de recuperación ante desastres. GlobalSign documenta los procedimientos de recuperación de desastres y continuidad del negocio diseñados para notificar y proteger razonablemente a los proveedores de software de aplicación, suscriptores y partes de confianza en caso de un desastre, compromiso de seguridad o falla comercial.

GlobalSign no divulga planes de continuidad comercial a suscriptores, partes que confían ni proveedores de software de aplicación, pero proporcionará planes de continuidad comercial y planes de seguridad a los auditores de CA de GlobalSign a pedido.

GlobalSign prueba, revisa y actualiza anualmente estos procedimientos. El plan de continuidad comercial incluye:

1. Las condiciones para activar el plan;
2. Procedimientos de emergencia;
3. Procedimientos alternativos;
4. Procedimientos de reanudación;
5. Un programa de mantenimiento para el plan;
6. Requisitos de concienciación y educación;
7. Las responsabilidades de los individuos;
8. Objetivo de tiempo de recuperación (RTO);
9. Prueba periódica de planes de contingencia;
10. El plan de GlobalSign para mantener o restaurar las operaciones comerciales de la CA de manera oportuna luego de la interrupción o falla de los procesos comerciales críticos;
11. Un requisito para almacenar materiales criptográficos críticos (es decir, dispositivos criptográficos seguros y materiales de activación) en una ubicación alternativa;
12. Qué constituye una interrupción aceptable del sistema y un tiempo de recuperación;
13. Con qué frecuencia se realizan copias de seguridad de la información y el software comerciales esenciales;
14. La distancia de las instalaciones de recuperación al sitio principal de la CA; y
15. Procedimientos para asegurar sus instalaciones en la medida de lo posible durante el período posterior a un desastre y antes de restaurar un entorno seguro, ya sea en el sitio original o en un sitio remoto.

15.7.2 ALTERACIÓN DE LOS RECURSOS HARDWARE, SOFTWARE Y/O DATOS

Si algún equipo se daña o deja de funcionar, pero las claves privadas no se destruyen, la operación debe restablecerse lo más rápido posible, dando prioridad a la capacidad de generar información sobre el estado del certificado de acuerdo con el plan de recuperación de desastres de GlobalSign.

15.7.3 PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA AUTORIDAD

En caso de que una clave privada de la EC de GlobalSign sea comprometida, perdida, destruida o se sospecha que es comprometida:

GlobalSign CA, después de investigar el problema, decidirá si el Certificado de la EC de GlobalSign debe ser revocado. Si es así, entonces:

- Todos los Suscriptores a los que se haya expedido un Certificado serán notificados en la primera oportunidad factible; y
- Se generará un nuevo par de claves de la EC de GlobalSign o se utilizará una jerarquía alternativa de EC existente para crear nuevos certificados de suscriptor.

15.7.4 CAPACIDAD DE RECUPERACIÓN DESPUÉS DE UN DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE

El plan de recuperación ante desastres se ocupa de la continuidad del negocio, tal como se describe en la Sección 28.7.1. Los sistemas de información del estado del certificado deben ser desplegados para proporcionar disponibilidad las 24 horas del día, 365 días al año.

16 AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

Los procedimientos dentro de este documento y la DPC de GLOBALSIGN abarcan todas las partes relevantes de los estándares PKI actualmente aplicables para las diversas industrias PKI verticales en las que la EC debe operar. En caso la EC que no se encuentre limitada por `dNSNameConstraints`, se auditan para verificar el cumplimiento de los Principios y criterios del servicio fiduciario AICPA / CICA para las autoridades de certificación.

16.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

GlobalSign mantiene su cumplimiento con las normas AICPA identificadas anteriormente a través de un Auditor Calificado anualmente. La auditoría cubre todas las actividades de GlobalSign CA.

GlobalSign mantiene su cumplimiento con los estándares AICPA / eIDAS identificados anteriormente a través de un auditor calificado de forma anual (AICPA), bianual (eIDAS) y contigua. La auditoría cubre todas las actividades de GlobalSign.

16.2 IDENTIDAD/CUALIFICACIÓN DEL AUDITOR

Con respecto a las auditorías de GlobalSign, son realizadas por Ernst & Young como un "auditor calificado" que posee la siguientes calificaciones y habilidades:

- Independencia del sujeto de la auditoría.
- La capacidad de realizar una auditoría que aborde los criterios especificados en una auditoría elegible como estipulado en el apartado 31 de este documento.
- Emplea a personas que tienen competencia en el examen de tecnología PKI, herramientas y técnicas de seguridad de la información, auditoría de tecnología de la información y seguridad, y la función de atestación de terceros.
- Certificado, acreditado, autorizado o evaluado de otra manera que cumple con la calificación requisitos de los auditores bajo el esquema de auditoría.
- De conformidad con la ley, la regulación gubernamental o el código de ética profesional; y
- Excepto en el caso de una agencia de auditoría interna del gobierno, mantiene Seguro de responsabilidad / errores y omisiones con límites de póliza de al menos un millón (\$ 1,000,000) dólares estadounidenses en cobertura.

Para eIDAS, la auditoría la realiza un organismo de evaluación de la conformidad acreditado por un Organismo de acreditación nacional de un estado miembro de la Unión sobre la base de EN ISO / IEC 17065 según lo perfilado por ETSI EN 319403 y en particular contra los requisitos definidos en el Reglamento eIDAS (UE) No 910/2014.

Para eIDAS del Reino Unido, la auditoría la realiza un organismo de evaluación de la conformidad acreditado sobre la base de EN ISO / IEC 17065 según lo perfilado por ETSI EN 319403 y en particular contra los requisitos definido en el Reglamento eIDAS del Reino Unido (eIDAS (Legislación del Reino Unido) y la Identificación Electrónica y Reglamento de 2016 sobre servicios fiduciarios para transacciones electrónicas)

En relación a las auditorías a las que se somete la EC de DIGILINK, el evaluador debe cumplir con los siguientes requerimientos:

- Ser autorizado por el INDECOPI.
- Ser independiente de la EC, y no haber realizado trabajos para ella dentro de los 2 años anteriores a la ejecución de la auditoría.
- Contar con experiencia significativa en tecnologías de la información, seguridad y tecnologías de PKI y criptográficas

16.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

GlobalSign y DIGILINK seleccionan un auditor que es completamente independiente de GlobalSign y DIGILINK.

16.4 ASPECTOS CUBIERTOS POR LOS CONTROLES

La auditoría debe cumplir con los requisitos del esquema de auditoría bajo el cual se realiza la evaluación. Estos requisitos pueden variar a medida que se actualizan los esquemas de auditoría. Un esquema de auditoría será aplicable a la EC en el año siguiente a la adopción del esquema actualizado.

16.5 ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

La EC debe seguir el mismo proceso si los auditores externos presentan un incumplimiento sustancial y deben crear un plan de acción correctiva adecuado para eliminar la deficiencia.

16.6 COMUNICACIÓN DE RESULTADOS

Los resultados de las auditorías de GLOBALSIGN, deben informarse a la Autoridad de Políticas de GlobalSign para su análisis y resolución de cualquier deficiencia a través de un plan de acción correctiva posterior. Los resultados también podrían estar disponibles para cualquier otra entidad apropiada que pueda tener derecho a una copia de los resultados por ley, reglamento o acuerdo. Se pueden encontrar copias de los informes de auditoría de WebTrust para CA de GlobalSign en: <https://www.globalsign.com/en/repository/>

17 NOTIFICACIÓN DE CAMBIOS

DIGILINK notificará los cambios realizados a este documento a los suscriptores, terceros que confían y demás interesados en sus servicios de sellado de tiempo, y publicará las nuevas versiones en su sitio web.

Asimismo, se notificarán los cambios en las políticas de GLOBALSIGN, los cuales serán publicados en la siguiente dirección:

<https://www.globalsign.com/en/repository/>

18 INFORMACIÓN DE CONTACTO

Datos de la Entidad de Certificación:

Nombre: DIGILINK S.A.C.

Dirección: Calle Mayorazgo 149, Urb. Chacarilla Del Estanque, San Borja

Domicilio: Lima

Teléfono: 933333583 - 998732355

Correo electrónico: informes@digilink.pe

Página Web: <https://digilink.pe>

Datos de la Entidad Prestadora de Servicios:

Nombre: GMO GLOBALSIGN

Dirección: Two International Drive, Suite 150, Portsmouth

Domicilio: New Hampshire 03801

Teléfono: 603-570-7060

Línea Gratuita: 1-877-775-4562

Fax: 603-570-7059

Correo electrónico: contacto@globalsign.com

Página Web: www.globalsign.com/en

19 CICLO DE VIDA DE LA GESTIÓN DE CLAVE

GlobalSign, como proveedor de servicios de Digilink, utiliza varias claves privadas para cumplir con su servicio. Utiliza un par de claves privadas para emitir los certificados de marca de tiempo de clave pública que se utilizan dentro de las TSU. Uno o más pares de claves privadas se utilizan dentro de la TSU para emitir la marca de tiempo.

Todas las claves privadas se almacenan en un módulo de seguridad de hardware (HSM) FIPS 140-2 Nivel 3.

19.1 GENERACIÓN DE LA CLAVE DE LA TSA

La generación de la(s) clave(s) de firma de la TSU se llevan a cabo en un entorno físicamente seguro (según la sección 15.1) por personal en funciones de confianza (según la sección 15.3) bajo al menos un control dual. El personal autorizado para llevar a cabo esta función se limita a aquellos requeridos para hacerlo según las prácticas de GlobalSign.

19.2 CARACTERÍSTICAS TÉCNICAS DEL CERTIFICADO DIGITAL Y DE LOS ALGORITMOS UTILIZADOS

Las características del certificado digital son señaladas en la Política de Sellado de Tiempo de GLOBALSIGN y de los algoritmos utilizados en los servicios de sellado de tiempo, en la Declaración de Prácticas de Certificación de GLOBALSIGN.

19.3 PROTECCIÓN DE LA CLAVE PRIVADA DE LA TSA

La clave de firma privada de TSU se mantiene y se usa dentro de un módulo criptográfico que cumple con FIPS PUB 140-2 [i.9], nivel 3.

Cada clave de firma privada de TSU siempre está asociada con un solo certificado de TSU. Una TSU está conectada exactamente a un módulo de seguridad de hardware, lo que garantiza que solo se utilice una clave privada por TSU.

Las claves privadas de TSU no están respaldadas.

19.4 DISTRIBUCIÓN DE LA CLAVE PÚBLICA TSU

GlobalSign garantiza la integridad y autenticidad de las claves (públicas) de verificación de firmas de TSU de la siguiente manera:

- Las claves (públicas) de verificación de firma de TSU están disponibles para las partes que confían en certificados disponibles públicamente. Los certificados se pueden encontrar en el sitio de soporte de GlobalSign: <https://support.globalsign.com>
- La TSU no emite una marca de tiempo antes de que su certificado de verificación de firma (clave pública) se cargue en la TSU o su dispositivo criptográfico. Al obtener un certificado de verificación de firma (clave pública), GlobalSign verifica que este certificado se haya firmado correctamente (incluida la verificación de la cadena de certificados ante su autoridad de certificación de confianza).

19.5 RE-EMISIÓN DE LA CLAVE DE LA TSU

La vida útil del certificado de la TSU no debe ser mayor que el período de tiempo durante el cual el algoritmo elegido y la longitud de la clave se reconocen como adecuados para su propósito.

Una vez al año o cuando ocurren cambios significativos, la Autoridad de Políticas de GlobalSign verifica cualquier algoritmo criptográfico utilizado dentro de la TSU con los algoritmos reconocidos como adecuados.

Si un algoritmo se ve comprometido o ya no es adecuado, GlobalSign volverá a generar las claves privadas afectadas.

19.6 GESTIÓN DEL CICLO DE VIDA DEL HARDWARE CRIPTOGRÁFICO DE FIRMA

Todo el hardware será inspeccionado durante el proceso de puesta en servicio para garantizar la conformidad con el suministro y que no se encuentre evidencia de manipulación.

El hardware y el software adquiridos se compran de una manera que reduce la probabilidad de que se manipule algún componente en particular (por ejemplo, asegurándose de que el equipo se seleccionó al azar en el momento de la compra).

La instalación, activación y duplicación de las claves de firma de TSU en hardware criptográfico debe ser realizada solo por personal en roles confiables usando al menos control dual en un ambiente físicamente seguro.

Las claves de firma privadas de TSU almacenadas en el módulo criptográfico de TSU se borrarán al retirar el dispositivo de una manera que sea prácticamente imposible recuperarlas.

19.7 TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA DEL TSU

La validez de todas las claves privadas utilizadas nunca excede la validez de los certificados emitidos con esas claves privadas.

Después de la expiración de las claves privadas, las claves privadas dentro del hardware criptográfico se destruyen de tal manera que las claves privadas no se pueden recuperar ni utilizar más. El Administrador de claves de GlobalSign define los períodos de validez de las claves.

20 SELLO DE TIEMPO

El Servicio de sello de tiempo calificado de GlobalSign emite sellos de tiempo calificados que se ajustan al perfil de sello de tiempo definido en el ETSI EN 319 422 [5] y se encuentran conformes a la RFC 3161. Dichos sellos se encuentran sincronizados a la fuente de tiempo del Laboratorio Nacional de Metrología de Francia, la cual es reconocida por el BIPM.

La provisión de un token de marca de tiempo en respuesta a una solicitud queda a discreción de GlobalSign.

20.1 SINCRONIZACIÓN DEL RELOJ CON LA UTC

El reloj de la TSA está sincronizado con la UTC con una precisión de +/- 1 segundo o mejor. En cualquier caso en el que el reloj de la TSA se desvíe aún más de la precisión, no se emitirá ninguna marca de tiempo hasta que se vuelva a sincronizar el reloj.

Específicamente, se tratan los siguientes temas:

- Calibración continua del reloj TSU
- Supervisión de la precisión del reloj TSU
- Análisis de amenazas contra ataques a señales horarias.
- Comportamiento al saltar / agregar segundos intercalares

GlobalSign registra todos los registros relacionados con los siguientes eventos relacionados con la sincronización del reloj:

- Se registrarán todos los eventos relacionados con la sincronización del reloj de una TSU con UTC (incluida la recalibración o sincronización de los relojes utilizados en la marca de tiempo).
- Se registrarán todos los eventos relacionados con la detección de pérdida de sincronización.

21 TÉRMINO DE LA TSA

Antes de su finalización, la TSA de DIGILINK informará a los clientes y terceros que confían sobre el cese de sus operaciones con al menos treinta (30) días calendario de anticipación. Mientras que, al INDECOPI, se le informará con al menos sesenta (60) días calendario de anticipación.

Todas las solicitudes y contratos con los clientes serán transferidos al INDECOPI o a otro Prestador de Servicios de Certificación designado por éste.

En caso de una operación de transferencia de titularidad, los nuevos dueños u operadores solicitarán la evaluación de cumplimiento al INDECOPI para garantizar que se mantienen los requisitos de acreditación.

Se advertirá a todos los clientes y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de sellos de tiempo por una TSA que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección:

www.digilink.pe

22 NIVELES DE SERVICIO

Se describen los niveles de servicio del Data Center donde se encuentra implementada la infraestructura que da soporte a la Entidad de Certificación:

SLA	Criterio	Nivel de Servicio
Disponibilidad del Sistema / Servicio	Disponible	96.50% (*)
Disponibilidad de la plataforma Cloud del Sistema	Disponible	99.95% (**)

(*) Disponibilidad medida mensualmente

(**) Disponibilidad medida mensualmente

23 CUMPLIMIENTO DE REQUERIMIENTOS LEGALES

DIGILINK, como Autoridad emisora de sellos de tiempo, cumple los requerimientos legales establecidos en la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, el Reglamento y la Ley de Firmas y Certificados Digitales – Ley 27269.

24 CONFORMIDAD

Este documento ha sido aprobado por el Responsable de EC, ER y TSA de DIGILINK, y tiene carácter normativo sobre todos los servicios de sellado de tiempo, por lo que cualquier incumplimiento por parte de las personas mencionadas en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.