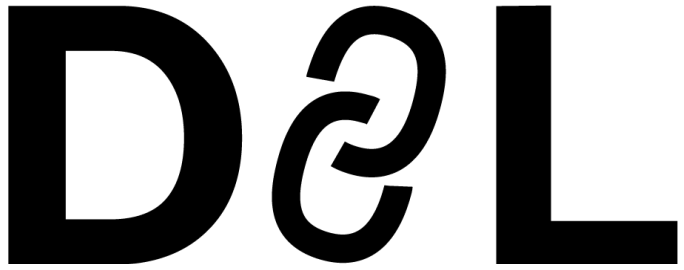

DECLARACIÓN DE PRÁCTICAS Y POLÍTICA DE CERTIFICACIÓN

Entidad de Certificación

Información del documento	
Nombre de documento: **Declaración de Prácticas y Política de Certificación de DIGILINK**	
Código de documento: **DL-DPPCER-01**	
Versión: **2.1**	Aprobado por: **Responsable de la Entidad de Certificación**
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. Se especificaron secciones dentro del documento.
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 33. Niveles de Servicio.
2.1	25-01-2024	Cambio de Representante Legal de la empresa.

ÍNDICE

1 INTRODUCCIÓN 8
2 OBJETIVO 8
3 OBJETO DE LA ACREDITACIÓN 8
4 DEFINICIONES Y ABREVIACIONES 8
4.1 PKI PARTICIPANTES 9
4.1.1 ENTIDAD DE CERTIFICACIÓN DIGILINK (EC DIGILINK) 9
4.1.2 ENTIDAD DE REGISTRO DIGILINK (ER DIGILINK) 9
4.1.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL (GLOBALSIGN) 10
4.1.4 TITULAR 10
4.1.5 SUSCRIPTOR 10
4.1.6 SOLICITANTE 10
4.1.7 TERCERO QUE CONFÍA 11
4.1.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR 11
5 SERVICIOS DE CERTIFICACIÓN DIGITAL 11
6 RESPONSABILIDADES DE DIGILINK 11
7 USO DEL CERTIFICADO 12
7.1 TIPOS DE CERTIFICADO 12
7.2 USOS ADECUADOS DEL CERTIFICADO 13
7.3 USOS PROHIBIDOS DEL CERTIFICADO Y EXCLUSIÓN DE RESPONSABILIDAD 14
8 PERSONA DE CONTACTO 14
9 RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES 15
10 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE CP Y DPC 15
11 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS 15
12 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN 16
12.1 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN 17
12.2 PLAZO O FRECUENCIA DE LA PUBLICACIÓN 17
12.3 CONTROLES DE ACCESO A LOS REPOSITORIOS 18
13 IDENTIFICACIÓN Y AUTENTICACIÓN 18
13.1 NOMBRES 18
13.1.1 TIPOS DE NOMBRES 18
13.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO 18
13.1.3 ANONIMATO Y SEUDOANONIMATO DE LOS TITULARES 18
13.1.4 REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE 19
13.1.5 SINGULARIDAD DE LOS NOMBRES 19
13.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS RECONOCIDAS. 19
14 VALIDACIÓN INICIAL DE LA IDENTIDAD 19
15 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES 19

16 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN ... 19

17 REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS ... 20

17.1 SOLICITUD DEL CERTIFICADO ... 20
17.2 QUIÉN PUEDE SOLICITAR UN CERTIFICADO ... 20
17.3 PROCESO DE REGISTRO Y RESPONSABILIDADES ... 20

18 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS ... 20

18.1 REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN ... 20
18.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO ... 20
18.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO ... 20

19 EMISIÓN DE CERTIFICADOS ... 20

19.1 ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS ... 20
19.2 NOTIFICACIÓN AL SOLICITANTE POR LA EC DE LA EMISIÓN DEL CERTIFICADO ... 20

20 ACEPTACIÓN DEL CERTIFICADO ... 21

20.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO ... 21
20.2 PUBLICACIÓN DEL CERTIFICADO POR LA EC ... 21
20.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES ... 21

21 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO ... 21

21.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR ... 21
21.2 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN ... 22

22 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES ... 22

23 RE-EMISIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES ... 22

24 MODIFICACIÓN DE CERTIFICADOS ... 22

25 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS ... 23

25.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO ... 23
25.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN ... 26
25.3 PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN ... 26
25.4 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN ... 26
25.5 FRECUENCIA DE EMISIÓN DE LAS CRLS ... 26
25.6 TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS ... 26
25.7 REVOCACIÓN ON-LINE/DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO ... 27
25.8 REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ON-LINE ... 27
25.9 OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN ... 27
25.10 REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS ... 28
25.11 CIRCUNSTANCIAS PARA LA SUSPENSIÓN ... 28
25.12 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN ... 28
25.13 PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN ... 28
25.14 LÍMITES DEL PERIODO DE SUSPENSIÓN ... 28
25.15 NOTIFICACIÓN DE LA REVOCACIÓN DE UN CERTIFICADO ... 28

26 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS ... 28

26.1 CARACTERÍSTICAS OPERACIONALES ... 28
26.2 DISPONIBILIDAD DEL SERVICIO ... 29
26.3 CARACTERÍSTICAS OPCIONALES ... 29
26.4 FINALIZACIÓN DE LA VIGENCIA DE UN CERTIFICADO ... 29

27 CUSTODIA Y RECUPERACIÓN DE CLAVES ... 29

27.1 PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES ... 29
27.2 PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE LA CLAVE DE SESIÓN ... 29

28 CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OPERACIONALES ... 30

28.1 CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA 30
28.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN 30
28.1.2 ACCESO FÍSICO 30
28.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO 30
28.1.4 EXPOSICIÓN AL AGUA 30
28.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS 30
28.1.6 SISTEMA DE ALMACENAMIENTO 30
28.1.7 ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN 31
28.2 CONTROLES DE PROCEDIMIENTO 31
28.2.1 ROLES DE CONFIANZA 31
28.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA 31
28.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL 32
28.2.4 ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES 32
28.3 CONTROLES DE PERSONAL 32
28.3.1 REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES 32
28.3.2 PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES 33
28.3.3 REQUISITOS DE FORMACIÓN 33
28.3.4 REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN 33
28.3.5 FRECUENCIA Y SECUENCIA DE ROTACIÓN DE TAREAS 34
28.3.6 SANCIONES POR ACTUACIONES NO AUTORIZADAS 34
28.3.7 REQUISITOS DE CONTRATACIÓN DE TERCEROS 34
28.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL 34
28.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD 34
28.4.1.1 TIPOS DE EVENTOS REGISTRADOS 34
28.4.2 FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA (LOG) 36
28.4.3 PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA 36
28.4.4 PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA 36
28.4.5 PROCEDIMIENTOS DE BACKUP DE LOS REGISTROS DE AUDITORÍA 36
28.4.6 SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA) 36
28.4.7 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO 37
28.4.8 ANÁLISIS DE VULNERABILIDADES 37
28.5 ARCHIVO DE REGISTROS 37
28.5.1 TIPOS DE EVENTOS ARCHIVADOS 37
28.5.2 PERIODO DE CONSERVACIÓN 37
28.5.3 PROTECCIÓN DE ARCHIVOS 38
28.5.4 PROCEDIMIENTOS DE BACKUP DEL ARCHIVO DE REGISTROS 38
28.5.5 REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS 38
28.5.6 SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA) 38
28.5.7 PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA. 38
28.6 CAMBIO DE CLAVES DE UNA EC 39
28.7 RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE Y DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE 39
28.7.1 PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES 39
28.7.2 ALTERACIÓN DE LOS RECURSOS HARDWARE, SOFTWARE Y/O DATOS 40
28.7.3 PROCEDIMIENTO DE ACTUACIÓN ANTE LA VULNERABILIDAD DE LA CLAVE PRIVADA DE UNA AUTORIDAD 40
28.7.4 CAPACIDAD DE RECUPERACIÓN DESPUÉS DE UN DESASTRE NATURAL U OTRO TIPO DE CATÁSTROFE 40
28.8 CESE DE UNA EC O ER 40

29 CONTROLES TÉCNICOS DE SEGURIDAD 41

29.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES 41
29.1.1 GENERACIÓN DEL PAR DE CLAVES 41
29.1.2 ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES 42
29.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO 42
29.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA EC A TERCEROS ACEPTANTES 42
29.1.5 TAMAÑO DE LAS CLAVES 42
29.1.6 PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD 44

29.1.7 USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509) 44
29.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS 44
29.2.1 CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS 44
29.2.2 CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA 44
29.2.3 CUSTODIA DE LA CLAVE PRIVADA 45
29.2.4 BACKUP DE LA CLAVE PRIVADA 45
29.2.5 ARCHIVO DE LA CLAVE PRIVADA 45
29.2.6 TRANSFERENCIA DE LA CLAVE PRIVADA A/DESDE EL MÓDULO CRIPTOGRÁFICO 45
29.2.7 ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO 45
29.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA 45
29.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA 45
29.2.10 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA 46
29.2.11 EVALUACIÓN DEL MÓDULO CRIPTOGRÁFICO 46
29.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES 46
29.3.1 ARCHIVO DE LA CLAVE PÚBLICA 46
29.3.2 PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES 46
29.4 DATOS DE ACTIVACIÓN 47
29.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN 47
29.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN 47
29.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN 47
29.5 CONTROLES DE SEGURIDAD INFORMÁTICA 47
29.5.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS 47
29.5.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA 48
29.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA 48
29.6.1 CONTROLES DE DESARROLLO DE SISTEMAS 48
29.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD 48
29.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA 49
29.7 CONTROLES DE SEGURIDAD DE LA RED 49
29.8 SELLADO DE TIEMPO 49
29.8.1 SERVICIOS DE FIRMA DE SELLADO DE TIEMPO PDF 49
30 PERFILES DE CERTIFICADOS, CRL Y OCSP 50
30.1 PERFIL DE CERTIFICADO 50
30.1.1 NÚMERO DE VERSIÓN 50
30.1.2 EXTENSIONES DEL CERTIFICADO 50
30.1.3 IDENTIFICADORES DE OBJETOS DE ALGORITMO 50
30.1.4 FORMULARIOS DE NOMBRES 50
30.1.5 LIMITACIONES DE LOS NOMBRES 51
30.1.6 IDENTIFICADOR DE OBJETO DE LA POLÍTICA DE CERTIFICACIÓN 51
30.1.7 USO DE LA EXTENSIÓN POLICY CONSTRAINS 51
30.1.8 SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS 51
30.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICIES 51
30.1.10 NÚMEROS SERIALES 51
30.2 PERFIL DE CRL 52
30.2.1 NÚMERO DE VERSIÓN 52
30.2.2 CRL Y EXTENSIONES CRL 52
30.3 PERFIL OCSP 52
30.3.1 NÚMERO DE VERSIÓN 52
30.3.2 EXTENSIONES OCSP 53
31 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES 53
31.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES 53
31.2 IDENTIDAD/CUALIFICACIÓN DEL AUDITOR 54
31.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA 54
31.4 ASPECTOS CUBIERTOS POR LOS CONTROLES 55
31.5 ACCIONES A TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS 55
31.6 COMUNICACIÓN DE RESULTADOS 55

32 OTROS ASUNTOS LEGALES Y COMERCIALES 55
32.1 TARIFAS 55

32.1.1 TARIFAS DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS 55
32.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS 55
32.1.3 TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO 55
32.1.4 TARIFAS DE OTROS SERVICIOS 55
32.1.5 POLÍTICA DE REEMBOLSO 56
32.2 RESPONSABILIDADES FINANCIERAS 56
32.2.1 COBERTURA DEL SEGURO 56
32.2.2 OTROS BIENES 56
32.2.3 SEGURO O GARANTÍA DE COBERTURA PARA LAS ENTIDADES FINALES 56
32.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL 56
32.3.1 ÁMBITO DE LA INFORMACIÓN CONFIDENCIAL 56
32.3.2 INFORMACIÓN NO CONFIDENCIAL 57
32.3.3 DEBER DE PROTEGER LA INFORMACIÓN CONFIDENCIAL 57
32.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL 57
32.4.1 PLAN DE PRIVACIDAD 57
32.4.2 INFORMACIÓN TRATADA COMO PRIVADA 57
32.4.3 INFORMACIÓN NO CALIFICADA COMO PRIVADA 57
32.4.4 RESPONSABILIDAD DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL 57
32.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR DATOS DE CARÁCTER PERSONAL 57
32.4.6 REVELACIÓN EN EL MARCO DE UN PROCESO ADMINISTRATIVO O JUDICIAL 58
32.4.7 OTRAS CIRCUNSTANCIAS DE REVELACIÓN DE INFORMACIÓN 58
32.5 DERECHOS DE PROPIEDAD INTELECTUAL 58
32.6 OBLIGACIONES 58
32.6.1 OBLIGACIONES DE LA EC 58
32.6.2 OBLIGACIONES DE LA ER 59
32.6.3 OBLIGACIONES DEL TITULAR 59
32.6.4 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN 60
32.6.5 OBLIGACIONES DE LA ENTIDAD 60
32.6.6 OBLIGACIONES DE OTROS PARTICIPANTES 60
32.7 RENUNCIAS DE GARANTÍAS 60
32.8 LIMITACIONES DE RESPONSABILIDAD 60
32.9 INDEMNIZACIONES 61
32.9.1 INDEMNIZACIÓN POR GLOBALSIGN 61
32.9.2 INDEMNIZACIÓN POR SUSCRIPTORES 61
32.9.3 INDEMNIZACIÓN POR LAS PARTES QUE CONFÍAN 61
33 NIVELES DE SERVICIO 61
34 CONFORMIDAD CON LA LEY APLICABLE 61
35 CONFORMIDAD 61
36 BIBLIOGRAFÍA 62

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 objeto la descripción de las operaciones y prácticas que utiliza DIGILINK para la administración de sus servicios como Entidad de Certificación Digital – EC, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital brindados por DIGILINK a través de la Entidad de Certificación GLOBALSIGN, la cual cuenta con la certificación Webtrust Program for Certification Authorities emitida por AICPA/CICA.

DIGILINK representa a GLOBALSIGN para todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y la Entidad de Certificación GLOBALSIGN.

4 DEFINICIONES Y ABREVIACIONES

Entidad de Certificación – EC	Entidad que presta servicios de emisión, revocación, re-emisión, modificación, suspensión de certificados digitales en el

	marco de la regulación establecida por la IOFE.
Entidad de Registro – ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital y que custodia de forma segura las evidencias de dichos procesos.
Declaración de Prácticas de Certificación – DPC o DPC	Documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus prácticas de certificación.
Política de Certificación – PC o CP	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida y/o clase de aplicación con requisitos de seguridad comunes.
Titular	Entidad que requiere los servicios provistos por la EC de GLOBALSIGN, y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

4.1 PKI PARTICIPANTES

4.1.1 ENTIDAD DE CERTIFICACIÓN DIGILINK (EC DIGILINK)

DIGILINK, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios relacionados con las funciones de infraestructura de clave pública (PKI) como el registro de suscriptores, emisión, re-emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

4.1.2 ENTIDAD DE REGISTRO DIGILINK (ER DIGILINK)

DIGILINK, brinda los servicios de Entidad de Registro, la cual se encarga de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante

la verificación de su identidad y su registro. Asimismo, la ER puede iniciar o transmitir solicitudes de revocación de certificados y solicitudes de reemisión de certificados.

4.1.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL (GLOBALSIGN)

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Certificación y Registro de DIGILINK, la cual emite certificados digitales de GLOBALSIGN cuando esta entidad así lo requiere y garantizan la continuidad del servicio a los suscriptores y titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que ofrece DIGILINK son provistos en un acuerdo con la Entidad de Certificación de GLOBALSIGN.

4.1.4 TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la DPC de DIGILINK.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por GLOBALSIGN como prestador de servicios de DIGILINK, conforme a lo establecido en el presente documento.

4.1.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

4.1.6 SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo la DPC de DIGILINK.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

4.1.7 TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación de GLOBALSIGN a un titular. El Tercero que confía, a su vez puede ser o no titular.

4.1.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el certificado.

5 SERVICIOS DE CERTIFICACIÓN DIGITAL

DIGILINK brinda los servicios de emisión, re-emisión y revocación de los certificados de la Entidad de Certificación GLOBALSIGN.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritas en la Declaración de Prácticas y la Política de Certificación de GLOBALSIGN:

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

6 RESPONSABILIDADES DE DIGILINK

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.

7 USO DEL CERTIFICADO

7.1 TIPOS DE CERTIFICADO

CATEGORÍA	TIPO DE CERTIFICADO	DESCRIPCIÓN	REQUISITOS
PERSONA NATURAL	PERSONA NATURAL	Aquellas que tienen la plena capacidad de ejercicio de sus derechos civiles. Las personas naturales asumirán la responsabilidad de titulares y suscriptores de los certificados digitales que adquieren.	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del solicitante - Contrato firmado
PERSONA JURÍDICA	PERSONA JURÍDICA CERTIFICADO DE REPRESENTANTE LEGAL	En el certificado digital del representante legal quedarán registrados todos sus atributos o facultades, los cuales le permitirán utilizar el certificado digital en nombre y representación de la persona jurídica.	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del solicitante - Vigencia de poder del Representante legal - Ficha RUC - Contrato firmado
	PERSONA JURÍDICA CERTIFICADO DE ATRIBUTOS / EMPLEADO / PERTENENCIA A EMPRESA	Los certificados digitales de los funcionarios o empleados tienen atributos limitados al desenvolvimiento de sus funciones dentro de la persona jurídica.	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del solicitante - Vigencia de poder del Representante legal - Ficha RUC - Contrato firmado (firma del

			Representante y empleado)
	PERSONA JURÍDICA FIRMA DE AGENTES AUTOMATIZADOS	Los certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados. La titularidad de certificados y firmas digitales generadas a partir de dicho certificado digital corresponderá a la persona jurídica.	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del solicitante - Vigencia de poder del Representante legal - Ficha RUC - Contrato firmado
	PROFESIONALES COMO PERSONA JURÍDICA	Aquellas personas que se encuentran colegiadas y habilitadas profesionalmente y desean firmar como profesionales asociados a empresa.	- Documento nacional de identidad o Cédula de extranjería - Formulario con datos del solicitante - Vigencia de poder del Representante legal - Ficha RUC - Constancia de Habilidad - Contrato firmado

7.2 USOS ADECUADOS DEL CERTIFICADO

Los usos adecuados de los Certificados emitidos son especificados en la Política de Certificación de GLOBALSIGN.

Los Certificados emitidos bajo esta DPC pueden ser utilizados con los siguientes propósitos:

Identificación del Titular: El Titular del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.

Integridad del documento firmado: La utilización del Certificado garantiza que el documento firmado es integro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.

No repudio de origen: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

7.3 USOS PROHIBIDOS DEL CERTIFICADO Y EXCLUSIÓN DE RESPONSABILIDAD

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta DPC.

Los certificados no garantizan que el sujeto sea digno de confianza, que opere una empresa de renombre o que el equipo en el que se haya instalado el certificado esté libre de defectos, malware o virus.

Los certificados emitidos bajo este DPC no se pueden utilizar:

- Para cualquier aplicación o mecanismo donde los problemas con el certificado podrían causar un riesgo de seguridad (por ejemplo, riesgo humano o ambiental)
- Donde esté prohibido por la ley

Se consideran indebidos aquellos usos que no están definidos en esta DPC y en la DPC de GLOBALSIGN y en consecuencia para efectos legales, DIGILINK y GLOBALSIGN quedan eximidas de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de certificados digitales según esta DPC y la DPC de GLOBALSIGN.

8 PERSONA 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 de Registro o Verificación:

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: https://www.globalsign.com/en

9 RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por DIGILINK son responsables de revisar la presente DPC y las Políticas DIGILINK, a fin de ser enterados de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

10 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE CP Y DPC

DIGILINK administra los documentos de Declaración de Prácticas, y todos los documentos normativos de la EC de DIGILINK.

Para cualquier consulta contactar:

- Nombre: PEDRO SEGUNDO CASTAÑEDA VARGAS
- Cargo: Responsable de la Entidad de Certificación de DIGILINK
- Dirección de correo electrónico: pedro.castaneda@digilink.pe

11 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Certificación – DPC y de Registro – RPS de DIGILINK, así como la Política de Seguridad, Política y Plan de Privacidad de la Entidad de Certificación y de Registro, y otra documentación relevante son publicadas en la siguiente dirección:

https://digilink.pe

Asimismo, la Declaración de Prácticas y Política de Certificación de GLOBALSIGN y otra documentación relevante son publicadas en la siguiente dirección:

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

Todas las modificaciones relevantes en la documentación de DIGILINK, serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por el Responsable de la EC de DIGILINK antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Las modificaciones relativas a la DPC u otra documentación relativa, serán publicadas luego de ser aprobadas por el INDECOPI.

12 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

Certificado Raíz GLOBALSIGN como prestador de servicios de DIGILINK

https://secure.globalsign.net/cacert/root-r6.crt

Certificados Subordinadas GLOBALSIGN como prestador de servicios de DIGILINK

http://secure.globalsign.com/cacert/gsaatlsha2g4.crt

http://secure.globalsign.com/cacert/gsgccr6aatlca2020.crt

Lista de Certificados Revocados (CRL)

http://crl.globalsign.com/root-r6.crl

http://crl.globalsign.com/ca/gsaatlsha2g4.crl

http://crl.globalsign.com/gsgccr6aatlca2020.crl

Declaración de Prácticas de Certificación (DPC)

https://digilink.pe

Validación de Certificados

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

12.1 PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Responsable de la EC de DIGILINK es el encargado de la autorización de la publicación de la DPC y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página https://digilink.pe/

La Lista de Certificados Revocados es publicada en la página web de GLOBALSIGN y está firmada digitalmente por la Entidad de Certificación GLOBALSIGN. Asimismo, se encuentran la CP y DPC que incluyen todo el material requerido por el RFC 3647 y están estructurados de acuerdo con dicho estándar.

La información del estado de los certificados digitales vigentes está disponible para consulta mediante protocolo OCSP.

12.2 PLAZO O FRECUENCIA DE LA PUBLICACIÓN

Certificado Raíz

El certificado raíz se publicará y permanecerá en la página Web de la Entidad de Certificación GLOBALSIGN durante todo el tiempo en que se estén prestando servicios de certificación digital.

Certificado Subordinada

El certificado de la EC Subordinada se publicará y permanecerá en la página Web de la Entidad de Certificación GLOBALSIGN durante todo el tiempo en que se estén prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

La Entidad de Certificación GLOBALSIGN publicará en la página Web, la lista de certificados revocados en los eventos y con la periodicidad definidas en el numeral.

Declaración de Prácticas de Certificación (DPC)

Con autorización del Responsable de la Entidad de Certificación de DIGILINK y el INDECOPI, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados al INDECOPI y publicados en la página Web de La Entidad de Certificación DIGILINK junto con la nueva versión. La Auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

Validación de Certificados

La Entidad de Certificación GLOBALSIGN publicará los certificados emitidos en un repositorio en formato X.509 V3 los cuales podrán ser consultados en la dirección www.globalsign.com/en

12.3 CONTROLES DE ACCESO A LOS REPOSITORIOS

La consulta a los repositorios disponibles en la página web de la Entidad de Certificación GLOBALSIGN, antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de La Entidad de Certificación GLOBALSIGN, que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta y a la página Web por parte de personas ajenas a GLOBALSIGN.

13 IDENTIFICACIÓN Y AUTENTICACIÓN

DIGILINK mantiene prácticas y procedimientos documentados para autenticar la identidad y/u otros atributos del Solicitante detallados en la Declaración de Prácticas de Registro.

13.1 NOMBRES

13.1.1 TIPOS DE NOMBRES

El documento guía que GLOBALSIGN, como prestador de servicios de DIGILINK, utiliza para la identificación única de los titulares de certificados emitidos está definido en la estructura del Nombre Distintivo (DNs: Distinguished Names) y cumple los requerimientos X.500, RFC-822 y X.400. Los Nombres comunes (CNs: Common Names) respetan la singularidad del espacio de nombres y no son engañosos.

13.1.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

En los casos en que un producto de GLOBALSIGN permite el uso de un rol o nombre de departamento y donde se incluye el campo de OU en el DN, se pueden agregar elementos únicos adicionales al DN dentro del campo de OU para permitir que las Partes de Confianza diferencien entre los certificados con los Elementos comunes DN.

13.1.3 ANONIMATO Y SEUDOANONIMATO DE LOS TITULARES

GLOBALSIGN, como prestador de servicios de DIGILINK, pueden emitir Certificados anónimos o seudónimos de entidad final, siempre que dichos códigos no estén prohibidos por la política aplicable y, si es posible, se conserva la singularidad del espacio de nombres. GLOBALSIGN CA se reserva el derecho de revelar la identidad del Suscriptor si así lo requiere la ley. Las solicitudes de nombres de dominio internacionalizados (IDN) en Certificados se marcarán para una revisión manual adicional. El nombre de host descodificado se someterá a una revisión adicional para intentar mitigar el riesgo de phishing y otros usos fraudulentos y el nombre de host descodificado puede compararse con solicitudes de certificado previamente rechazadas o certificados revocados. GLOBALSIGN puede rechazar solicitudes basadas en criterios de mitigación de riesgos, incluidos nombres con riesgo de phishing u otros usos fraudulentos, nombres que aparecen en las listas de navegación segura de

Google y nombres que figuran en la base de datos mantenida por el Grupo de trabajo Anti-Phishing.

13.1.4 REGLAS PARA LA INTERPRETACIÓN DE VARIAS FORMAS DE NOMBRE

Los Nombres Distintivos en los certificados se interpretan usando el estándar X.500 y la sintaxis ASN.1.

13.1.5 SINGULARIDAD DE LOS NOMBRES

GLOBALSIGN refuerza la singularidad de cada nombre de sujeto en un certificado. Un nombre de organización y estado y/o localidad únicos o un nombre de individuo único y estado y/o localidad con una dirección de correo electrónico opcional de un individuo afiliado a la Organización como empleado, agente, contratista, socio comercial o cliente. Para mayor información, consultar la DPC de GLOBALSIGN.

13.1.6 RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS RECONOCIDAS.

Los suscriptores no pueden solicitar certificados con ningún contenido que infrinja los derechos de propiedad intelectual de un tercero. GLOBALSIGN no requiere que se verifique el derecho de un Solicitante a usar una marca registrada. GLOBALSIGN se reserva el derecho de revocar cualquier certificado que esté involucrado en una disputa.

14 VALIDACIÓN INICIAL DE LA IDENTIDAD

DIGILINK, a través de su Entidad de Registro, realiza la validación de identidad de los solicitantes de certificados digitales. Sus prácticas se encuentran detalladas en la Declaración de Prácticas de Registro de DIGILINK.

15 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RE-EMISIÓN DE CLAVES

DIGILINK admite solicitudes de re-emisión de claves de los Suscriptores antes de la expiración del Certificado existente del Suscriptor. Dichas solicitudes son atendidas por la Entidad de Registro de DIGILINK y se encuentran detalladas en la Declaración de Prácticas de Registro de DIGILINK.

16 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

DIGILINK, a través de su Entidad de Registro, atiende las peticiones de revocación de conformidad con las causales de revocación especificadas en el documento de Declaración de Prácticas de Registro de DIGILINK y autentica la identidad de quien solicita la revocación de certificado.

17 REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS

17.1 SOLICITUD DEL CERTIFICADO

Dicho procedimiento le corresponde a la Entidad de Registro de DIGILINK y el mismo se describe en el documento Declaración de Prácticas de Registro de DIGILINK.

17.2 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Dicho procedimiento le corresponde a la Entidad de Registro de DIGILINK y el mismo se describe en el documento Declaración de Prácticas de Registro de DIGILINK.

17.3 PROCESO DE REGISTRO Y RESPONSABILIDADES

Dicho procedimiento le corresponde a la Entidad de Registro de DIGILINK y el mismo se describe en el documento Declaración de Prácticas de Registro de DIGILINK.

18 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

18.1 REALIZACIÓN DE LAS FUNCIONES DE IDENTIFICACIÓN Y AUTENTICACIÓN

Dicho procedimiento le corresponde a la Entidad de Registro de DIGILINK y el mismo se describe en el documento Declaración de Prácticas de Registro de DIGILINK.

18.2 APROBACIÓN O RECHAZO DE LAS SOLICITUDES DE CERTIFICADO

Dicho procedimiento le corresponde a la Entidad de Registro de DIGILINK y el mismo se describe en el documento Declaración de Prácticas de Registro de DIGILINK.

18.3 PLAZO PARA PROCESAR LAS SOLICITUDES DE CERTIFICADO

Dicho procedimiento le corresponde a la Entidad de Registro de DIGILINK y el mismo se describe en el documento Declaración de Prácticas de Registro de DIGILINK.

19 EMISIÓN DE CERTIFICADOS

19.1 ACTUACIONES DE LA EC DURANTE LA EMISIÓN DE CERTIFICADOS

GLOBALSIGN, a través de la Entidad de Registro de DIGILINK, procederá a la emisión de certificados digitales mediante la autenticación de múltiples factores de sus operadores. Los operadores de la Entidad de Registro de DIGILINK realizarán la validación de toda la información enviada por el Suscriptor y garantizarán que cualquier base de datos utilizada para almacenar datos del Suscriptor, se encuentre adecuadamente protegida contra modificaciones o manipulaciones no autorizadas.

19.2 NOTIFICACIÓN AL SOLICITANTE POR LA EC DE LA EMISIÓN DEL CERTIFICADO

GLOBALSIGN, en calidad de proveedor de servicios de DIGILINK, notificará al Suscriptor de la emisión de su certificado a la dirección de correo electrónico que fue proporcionada por el Suscriptor durante el proceso de validación o por cualquier otro método equivalente. El correo electrónico puede contener el certificado en sí o un enlace para descargar, según el tipo de Certificado solicitado.

20 ACEPTACIÓN DEL CERTIFICADO

20.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

Digilink informará al Suscriptor que no puede usar el Certificado hasta que haya revisado y verificado la exactitud de los datos incorporados en el Certificado. A menos que el Suscriptor notifique a la EC o ER dentro de los siete (7) días posteriores a la recepción, el Certificado se considerará aceptado.

Dicho procedimiento le corresponde a la Entidad de Registro de DIGILINK y el mismo se describe en el documento Declaración de Prácticas de Registro de DIGILINK.

20.2 PUBLICACIÓN DEL CERTIFICADO POR LA EC

GLOBALSIGN, como prestador de servicios de DIGILINK, publica el certificado al entregárselo al Suscriptor y puede publicarlo en uno o más Registros de transparencia de certificados. Además, para los clientes de Enterprise PKI, GLOBALSIGN puede publicar el Certificado en un directorio como LDAP.

20.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA EC A OTRAS ENTIDADES

Dicho procedimiento le corresponde a la Entidad de Registro de DIGILINK y el mismo se describe en el documento Declaración de Prácticas de Registro de DIGILINK.

21 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO

21.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL TITULAR

Los suscriptores deben proteger su clave privada teniendo cuidado de evitar la divulgación a terceros. El contrato de Suscriptor identifica las obligaciones del Suscriptor con respecto a la protección de Clave Privada. Las claves privadas sólo se deben utilizar como se especifica en los campos de uso de clave y de uso extendido de clave como se indica en el Certificado correspondiente. Donde es posible hacer una copia de seguridad de una clave privada, los suscriptores deben utilizar el mismo nivel de cuidado y protección atribuido a la clave privada en vivo. Al final de la vida útil de una clave privada, los suscriptores deben eliminar de forma segura la clave privada y los fragmentos que se han dividido para fines de copia de seguridad.

En el caso del Servicio de firma digital de GLOBALSIGN, y con el consentimiento del Suscriptor, GLOBALSIGN alojará, protegerá y administrará los Certificados de corta duración y sus correspondientes Claves privadas.

Para los Certificados calificados donde la clave privada relacionada con la clave pública certificada reside en un QSCD, las claves de suscriptor deben generarse y almacenarse dentro de un Dispositivo de creación de firma calificado (QSCD) reconocido. Se debe monitorear el estado de la certificación QSCD y se deben tomar las medidas adecuadas si cambia el estado de la certificación de un QSCD.

21.2 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

De acuerdo con la DPC de GLOBALSIGN, se describen las condiciones bajo las cuales los terceros que confían pueden confiar en los certificados incluyendo los servicios de certificado apropiados disponibles para verificar la validez del certificado como CRL y/u OCSP.

GLOBALSIGN también ofrece un acuerdo de terceros que confían a los Suscriptores, cuyo contenido debe presentarse al tercero que confía antes de confiar en un Certificado de la CA emisora. Los terceros que confían deben utilizar la información para realizar una evaluación del riesgo y, como tales, son las únicas responsables de realizar la evaluación del riesgo antes de confiar en el Certificado o de cualquier garantía realizada.

El software utilizado por los terceros que confían debe ser totalmente compatible con las normas X.509, incluyendo las mejores prácticas para encadenar decisiones en torno a políticas y uso de claves.

22 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

La Entidad de Certificación GLOBALSIGN, no atiende requerimientos de renovación de un certificado sin cambio de claves.

23 RE-EMISIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Para la Entidad de Certificación GLOBALSIGN, un requerimiento de re-emisión de un certificado con cambio de claves es un requerimiento normal de solicitud de un certificado digital como si fuera uno nuevo y por consiguiente implica el cambio de claves y así lo reconoce y acepta el solicitante.

La EC de DIGILINK comunicará al suscriptor, con una anticipación de al menos 30 días antes de la expiración del certificado, para que pueda renovar a tiempo dicho certificado. Si el suscriptor no solicita la re-emisión de certificado, el certificado expirará. Luego de ello, el suscriptor deberá realizar el proceso de validación de identidad desde la etapa inicial.

Las precisiones sobre el proceso de re-emisión son definidas en la Declaración de Prácticas de Registro de DIGILINK como Entidad de Registro.

24 MODIFICACIÓN DE CERTIFICADOS

GLOBALSIGN, como proveedor de servicios de DIGILINK trata la modificación de la misma manera que la emisión 'Nueva'.

GLOBALSIGN modifica los Certificados que hayan sido renovados previamente o con una nueva clave. El Certificado original es revocado una vez completada la modificación, sin embargo, el Certificado original no se renueva, vuelve a introducirse ni modificarse.

25 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

La revocación de certificados es un proceso mediante el cual el número de serie de un certificado se incluye efectivamente en la lista negra al agregar el número de serie y la fecha de la revocación a una CRL. La CRL en sí se firmará digitalmente con la misma clave privada que originalmente firmó el certificado que se revocará. Agregar un número de serie a la CRL permite a las Partes que Confían establecer que el ciclo de vida de un Certificado ha terminado. GLOBALSIGN puede eliminar los números de serie cuando los Certificados revocados pasan su fecha de vencimiento para promover una administración más eficiente del tamaño de los archivos de CRL.

25.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

GLOBALSIGN puede revocar cualquier Certificado a su entera discreción.

La revocación de un Certificado de Suscriptor se realiza dentro de las veinticuatro (24) horas bajo las siguientes circunstancias:

- El Suscriptor solicita por escrito a DIGILINK que desea revocar el Certificado;

- El Suscriptor notifica a DIGILINK que la Solicitud de Certificado original no fue autorizada y no otorga autorización retroactiva;

- DIGILINK o GLOBALSIGN obtienen pruebas razonables de que la clave privada del suscriptor correspondiente a la clave pública en el certificado sufrió un compromiso de clave;

- DIGILINK o GLOBALSIGN conocen un método demostrado o comprobado que puede calcular fácilmente la clave privada del suscriptor basándose en la clave pública del certificado (como una clave débil de Debian, consulte https://wiki.debian.org/SSLkeys);

- DIGILINK o GLOBALSIGN reciben una notificación o se da cuenta de la terminación inesperada del contrato o las funciones comerciales de un Suscriptor o Sujeto.

La revocación de un Certificado de Suscriptor debe realizarse dentro de las veinticuatro (24) horas y se realiza dentro de los 5 días si ocurre una o más de las siguientes situaciones:

- El Certificado ya no cumple con los requisitos de tipo de algoritmo y tamaño de clave de los Requisitos básicos, indicados en la DPC de GLOBALSIGN;

- DIGILINK o GLOBALSIGN obtienen evidencia de que el Certificado fue mal utilizado;

- DIGILINK o GLOBALSIGN reciben un aviso o se da cuenta de que el Suscriptor violó cualquiera de sus obligaciones materiales bajo el Acuerdo de Suscriptor o los Términos de Uso;

- DIGILINK o GLOBALSIGN tienen conocimiento de que se ha utilizado un certificado comodín para autenticar un nombre de dominio totalmente calificado subordinado engañoso y fraudulento;

- DIGILINK o GLOBALSIGN recibe un aviso o se da cuenta de un cambio sustancial en la información contenida en el Certificado;

- DIGILINK o GLOBALSIGN tiene conocimiento de que el Certificado no se emitió de acuerdo con los Requisitos básicos o el CP o DPC de GLOBALSIGN;

- DIGILINK o GLOBALSIGN determina que la información que aparece en el Certificado no es precisa o es engañosa;

- El derecho de GLOBALSIGN a emitir Certificados conforme a los Requisitos básicos vence o se revoca o cancela, a menos que GLOBALSIGN haya hecho arreglos para continuar manteniendo el Repositorio de CRL / OCSP;

- DIGILINK o GLOBALSIGN tiene conocimiento de un método demostrado o comprobado que expone la clave privada del suscriptor a un compromiso o si hay evidencia clara de que el método específico utilizado para generar la clave privada fue defectuoso;

- La revocación es requerida por el presente documento o la DPD de GLOBALSIGN;

- El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para los Proveedores de Software de Aplicación o las Partes que Confían (por ejemplo, el CA/B Forum podría determinar que un algoritmo criptográfico/firmaobsoleto o un tamaño de clave presenta un riesgo inaceptable y que dichos Certificados deben ser revocados y reemplazado por otras ECs dentro de un período de tiempo determinado);

- DIGILINK o GLOBALSIGN recibe una notificación o se da cuenta de cualquier circunstancia que indique que el uso de la dirección de correo electrónico en el Certificado ya no está permitido legalmente;

- Se sospecha que la clave privada de la EC utilizada para emitir el certificado ha sido comprometida;

- DIGILINK o GLOBALSIGN deja de operar por cualquier motivo y no ha acordado que otra EC brinde soporte de revocación para el Certificado;

La revocación de un Certificado de Suscriptor también puede realizarse dentro de un período de tiempo comercialmente razonable en las siguientes circunstancias:

- El Suscriptor o el administrador de la organización solicita la revocación del Certificado a través de la cuenta de correo electrónica registrada que controla el ciclo de vida del Certificado;

- El Suscriptor solicita la revocación a través de ER de DIGILINK;

- DIGILINK o GLOBALSIGN recibe una notificación o se da cuenta de que el Suscriptor ha sido agregado como parte denegada o a una lista negra de personas prohibidas, o está operando desde un destino prohibido según las leyes de la jurisdicción de operación de GLOBALSIGN;

- Pago vencido de las tarifas aplicables por parte del Suscriptor;

- Tras la solicitud de revocación de un Certificado;

- Si se ha vuelto a emitir un Certificado, DIGILINK o GLOBALSIGN puede revocar el Certificado emitido anteriormente;

- Bajo ciertos acuerdos de licencia, DIGILINK o GLOBALSIGN puede revocar Certificados luego de la expiración o terminación del acuerdo de licencia;

- DIGILINK o GLOBALSIGN determina que el uso continuo del Certificado es perjudicial para el negocio de DIGILINK, GLOBALSIGN o de terceros. Al considerar si el uso del Certificado es perjudicial para el negocio o la reputación de DIGILINK, GLOBALSIGN o de un tercero, se considerará, entre otras cosas, la naturaleza y el número de quejas recibidas, la identidad de los denunciantes, la legislación pertinente en vigor y las respuestas al supuesto uso perjudicial por parte del Suscriptor;

- Muerte de un suscriptor.

La revocación de un Certificado de EC subordinada se realiza dentro de los siete (7) días en las siguientes circunstancias:

- La EC subordinada solicita por escrito a GLOBALSIGN que proporcionó el Certificado de EC subordinada, que GLOBALSIGN revoque el Certificado;

- El Suscriptor notifica a DIGILINK o GLOBALSIGN que la Solicitud de Certificado original no fue autorizada y no otorga autorización retroactiva;

- GLOBALSIGN obtiene evidencia razonable de que la clave privada de la CA subordinada correspondiente a la clave pública en el certificado sufrió un compromiso de clave o ya no cumple con los requisitos para el tipo de algoritmo y el tamaño de clave de los requisitos básicos;

- GLOBALSIGN obtiene evidencia de que el Certificado fue mal utilizado;

- GLOBALSIGN tiene conocimiento de que el Certificado no se emitió de acuerdo con o que la EC subordinada no ha cumplido con los Requisitos básicos o DPCs aplicables;

- GLOBALSIGN determina que la información que aparece en el Certificado es inexacta o engañosa;

- La EC emisora o la EC subordinada cesa sus operaciones por cualquier motivo y no ha acordado que otra CA proporcione soporte para la revocación del Certificado;

- El derecho de la EC emisora o la EC subordinada de emitir Certificados bajo los Requisitos básicos expira o se revoca o termina, a menos que la EC emisora haya hecho arreglos para continuar manteniendo el Repositorio CRL/OCSP;

- La DPC de GLOBALSIGN requiere la revocación;

- El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para los proveedores de software de aplicación o las partes que confían (por ejemplo, el CA/B Forum podría determinar que un algoritmo criptográfico/firma obsoleto o un tamaño de clave presenta un riesgo inaceptable y que dichos Certificados deben ser revocados y reemplazados por la EC dentro de un período de tiempo determinado).

Para cualquier EC raíz de confianza, GLOBALSIGN puede revocar la EC emisora si la EC raíz de confianza ya no cumple con los términos y condiciones contractuales del acuerdo entre las dos partes.

25.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de DIGILINK – RPS.

25.3 PLAZO EN EL QUE LA EC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de DIGILINK – RPS.

25.4 REQUISITOS DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

Los procedimientos relativos a la Entidad de Registro son descritos en el documento de Declaración de Prácticas de Registro o Verificación de DIGILINK – RPS.

25.5 FRECUENCIA DE EMISIÓN DE LAS CRLS

Si un certificado de Entidad Final contiene un CDP (CRL Distribution Point), entonces esa CRL se actualiza al menos cada 7 días (cada 24 horas para las CRL de certificados calificados) y el valor del campo nextUpdate no supera los 10 días del valor del thisUpdate campo.

Si un certificado de CA contiene un CDP, esa CRL se actualiza al menos una vez cada 12 meses y dentro de las 24 horas posteriores a la revocación de un certificado de CA subordinado, y el valor del campo nextUpdate no supera los 12 meses del valor del campo thisUpdate .

Para los Certificados Calificados, el estado de revocación real se publicará / estará disponible a través de todos los mecanismos de revocación dentro de los 60 minutos posteriores a la decisión de revocación y nunca se revertirá.

25.6 TIEMPO MÁXIMO DE LATENCIA DE LAS CRLS

El tiempo entre la generación y publicación de la CRL es menor a una (1) hora, tal como lo establece el INDECOPI.

25.7 REVOCACIÓN ON-LINE/DISPONIBILIDAD DE VERIFICACIÓN DEL ESTADO

GLOBALSIGN admite respuestas OCSP además de CRL. Los tiempos de respuesta generalmente no superan los diez (10) segundos en condiciones normales de funcionamiento de la red.

Las respuestas OCSP operan de acuerdo con RFC6960 y RFC5019. Las respuestas OCSP estarán firmadas por un Respondedor OCSP cuyo Certificado está firmado por GLOBALSIGN que emitió el Certificado cuyo estado de revocación se verifica. El certificado de firma OCSP contiene una extensión de tipo id-pkix-ocsp-nocheck, según lo define RFC6960.

25.8 REQUISITOS DE COMPROBACIÓN DE LA REVOCACIÓN ON-LINE

Los terceros que confían deben confirmar la información de revocación, de lo contrario todas las garantías quedarán anuladas.

Para conocer el estado de los certificados de suscriptor:

- GLOBALSIGN actualizará la información proporcionada a través de un OCSP Respondedor al menos cada cuatro días. Las respuestas de OCSP de este servicio no excederá un tiempo de vencimiento de siete días.

Para conocer el estado de los certificados de CA subordinada:

- GLOBALSIGN actualizará la información proporcionada a través de un respondedor OCSP al menos (i) cada doce meses y (ii) dentro de las 24 horas posteriores a la revocación de un Certificado de CA subordinada.

Los Respondedores de OCSP que reciban una solicitud de estado de un Certificado que no ha sido emitido, no responderán con un estado "bueno" para dichos Certificados.

Los respondedores OCSP para las CA que no están técnicamente restringidas no responderán con un estado "bueno" para dichos Certificados.

La Entidad de Certificación GLOBALSIGN requerirá que las solicitudes de OCSP contengan los siguientes datos:

- Versión del protocolo
- Solicitud de servicio
- Identificador de certificado de destino

25.9 OTRAS FORMAS DISPONIBLES DE DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN

No se estipula.

25.10 REQUISITOS ESPECIALES DE RENOVACIÓN DE CLAVES COMPROMETIDAS

GLOBALSIGN, a través de la EC y ER de DIGILINK, utilizará métodos comercialmente razonables para informar a los Suscriptores de que su Clave Privada puede haber sido comprometida. Esto incluye los casos en los que se han descubierto nuevas vulnerabilidades o cuando GLOBALSIGN, a su propia discreción, decide que la evidencia sugiere que se ha producido un posible Compromiso de claves. Cuando el Compromiso de claves no sea disputado, GLOBALSIGN revocará Certificados de las ECs emisoras o Certificados de entidades finales de suscriptores dentro de las 24 horas y publicará CRL en línea dentro de los treinta (30) minutos de creación y ARL dentro de las doce (12) horas.

25.11 CIRCUNSTANCIAS PARA LA SUSPENSIÓN

GLOBALSIGN como prestador de servicios de DIGILINK no realiza el servicio de suspensión de certificados digitales.

25.12 QUIÉN PUEDE SOLICITAR LA SUSPENSIÓN

GLOBALSIGN como prestador de servicios de DIGILINK no realiza el servicio de suspensión de certificados digitales.

25.13 PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN

GLOBALSIGN como prestador de servicios de DIGILINK no realiza el servicio de suspensión de certificados digitales.

25.14 LÍMITES DEL PERIODO DE SUSPENSIÓN

GLOBALSIGN como prestador de servicios de DIGILINK no realiza el servicio de suspensión de certificados digitales.

25.15 NOTIFICACIÓN DE LA REVOCACIÓN DE UN CERTIFICADO

La publicación de un certificado revocado en la CRL constituye la prueba y una notificación pública de su revocación.

26 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

26.1 CARACTERÍSTICAS OPERACIONALES

GLOBALSIGN, como prestador de servicios de DIGILINK, proporciona un servicio de estado de certificado ya sea en forma de un punto de distribución de CRL o un respondedor OCSP o ambos en los certificados. GLOBALSIGN no elimina las entradas de revocación en CRL u OCSP hasta 10 años después de la Fecha de vencimiento del Certificado revocado. Para

otros tipos de certificados, no elimina las entradas de revocación en CRL u OCSP hasta después de la fecha de vencimiento del certificado revocado.

GLOBALSIGN envía una notificación por correo electrónico a los suscriptores en el mes (generalmente 30 días y 7 días) antes del vencimiento, informando a los suscriptores sobre el próximo vencimiento de sus certificados.

26.2 DISPONIBILIDAD DEL SERVICIO

GLOBALSIGN opera y mantiene su capacidad CRL y OCSP con recursos suficientes para proporcionar un tiempo de respuesta de diez segundos o menos en condiciones normales de operación. GLOBALSIGN mantiene un repositorio en línea 24x7 que el software de la aplicación puede usar para verificar automáticamente el estado actual de todos los certificados vigentes emitidos por GLOBALSIGN.

GLOBALSIGN mantiene una capacidad continua 24x7 para responder internamente a un Informe de problema de certificado de alta prioridad y, cuando corresponda, reenviar dicha queja a las autoridades policiales y/o revocar un Certificado que sea objeto de dicha queja.

26.3 CARACTERÍSTICAS OPCIONALES

No se estipula.

26.4 FINALIZACIÓN DE LA VIGENCIA DE UN CERTIFICADO

Los suscriptores pueden terminar su suscripción a los servicios de Certificado al tener su Certificado revocado o naturalmente dejarlo caducar. Para la raíz de confianza, los contratos entre GLOBALSIGN y el suscriptor raíz de confianza deben mantenerse durante toda la vida del certificado, a menos que GLOBALSIGN utilice la revocación del certificado como método para terminar el contrato.

27 CUSTODIA Y RECUPERACIÓN DE CLAVES

27.1 PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE CLAVES

Las claves privadas de la EC nunca se custodian. GLOBALSIGN no ofrece servicios de custodia de claves a los suscriptores.

27.2 PRÁCTICAS Y POLÍTICAS DE CUSTODIA Y RECUPERACIÓN DE LA CLAVE DE SESIÓN

No se estipula.

28 CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OPERACIONALES

28.1 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.

28.1.1 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.

28.1.2 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.

28.1.3 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.

28.1.4 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.

28.1.5 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.

28.1.6 SISTEMA DE ALMACENAMIENTO

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

28.1.7 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.

28.2 CONTROLES DE PROCEDIMIENTO

28.2.1 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 integra. 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.

28.2.2 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.

28.2.3 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.

28.2.4 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)

28.3 CONTROLES DE PERSONAL

28.3.1 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.

28.3.2 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.

28.3.3 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.

28.3.4 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.

28.3.5 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.

28.3.6 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.

28.3.7 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.

28.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

GLOBALSIGN pone a disposición de su personal su DPC, 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.

28.4 PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

28.4.1.1 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 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 (tales como, instalación, activación, desinstalación, retiro del dispositivo, entre otros);
- Generación de listas de revocación de certificados y entradas OCSP; e
- 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 DPC;
- 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

28.4.2 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.

28.4.3 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.

28.4.4 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.

28.4.5 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.

28.4.6 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.

28.4.7 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

No se estipula.

28.4.8 ANÁLISIS DE VULNERABILIDADES

GLOBALSIGN, en calidad de proveedor de DIGILINK, realiza evaluaciones de riesgo anuales que:

- Identifican amenazas internas y externas previsibles que podrían resultar en acceso no autorizado, divulgación, mal uso, alteración o destrucción de cualquier Certificado de Datos o Proceso de Gestión de Certificado;
- Evalúan 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
- Evalúan la suficiencia de las políticas, procedimientos, sistemas de información, tecnología y otros arreglos que la EC tiene implementados para contrarrestar tales amenazas.

GLOBALSIGN, como proveedor de infraestructura y operaciones de DIGILINK, realiza evaluaciones de vulnerabilidad periódicas que cubren todos los activos de EC de GLOBALSIGN relacionados con la emisión de certificados, productos y servicios. Las evaluaciones se enfocan en amenazas internas y externas que podrían resultar en acceso no autorizado, manipulación, modificación, alteración o destrucción del proceso de emisión del Certificado.

28.5 ARCHIVO DE REGISTROS

28.5.1 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.

28.5.2 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 periodo 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.

Con respecto a los archivos generados por la ER de Digilink, la destrucción de dichos archivos de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI.

28.5.3 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.

28.5.4 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.

28.5.5 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.

28.5.6 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.

28.5.7 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).

Cabe señalar que los archivos generados por los servicios de certificación de Digilink se encontrarán disponibles si son requeridos para propósitos legales, a fin de evidenciar su correcta operación.

28.6 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.

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

28.7.1 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.

28.7.2 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.

28.7.3 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;

- Digilink no emitirá nuevos certificados hasta que se supere el incidente;

- 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;

- Digilink le comunicará al INDECOPI el motivo del compromiso, así como las acciones realizadas; y

- Digilink brindará información a los Suscriptores y Terceros que confían, sobre mecanismos para identificar documentos comprometidos, como facilitar un listado de números de serie de los certificados afectados.

28.7.4 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.

28.8 CESE DE UNA EC O ER

Antes de su finalización, la EC de DIGILINK informará a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario

de anticipación. Mientras que, al INDECOPI, se le informará con por lo menos sesenta (60) días calendario de anticipación.

Todas las solicitudes y contratos de suscriptores y titulares 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 suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por una EC o ER que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección:

https://digilink.pe/

Por otro lado, GLOBALSIGN mantiene sus propios procedimientos en caso de cese de servicios, lo cuales se encuentran detallados en su DPC.

29 CONTROLES TÉCNICOS DE SEGURIDAD

29.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

29.1.1 GENERACIÓN DEL PAR DE CLAVES

Generación del par de claves de la EC

Para los pares de claves de CA raíz, GLOBALSIGN realiza los siguientes controles;

1. prepara y sigue un guión de generación clave,
2. hace que un auditor calificado sea testigo del proceso de generación del par de claves de la CA raíz o grabe un video de todo el proceso de generación del par de claves de la CA raíz, y
3. hace que un auditor calificado emita un informe en el que opina que GLOBALSIGN siguió el guión de la ceremonia de claves durante su proceso de generación de claves y certificados y los controles utilizados para garantizar la integridad y confidencialidad del par de claves.

En otros pares de claves de CA, GLOBALSIGN realiza los siguientes controles:

4. Genera las claves en un entorno físicamente seguro como se describe en este documento;
5. Genera las claves de la CA utilizando personal en roles confiables bajo los principios de control de múltiples personas y conocimiento dividido;
6. Genera las claves de la CA dentro de los módulos criptográficos que cumplan con los requisitos técnicos y comerciales aplicables, tal como se describe en la Política de certificados y / o la Declaración de prácticas de certificación de la CA;
7. Registra sus actividades de generación de claves de CA; y

8. Mantiene controles efectivos para proporcionar una seguridad razonable de que la clave privada se generó y protegió de conformidad con los procedimientos descritos en su Política de certificados y / o Declaración de prácticas de certificación y (si corresponde) en su Script de generación de claves.

Generación del par de claves del suscriptor

Para las claves de suscriptor generadas por GLOBALSIGN, la generación de claves se realiza en un dispositivo criptográfico seguro que cumple con FIPS 140-2 utilizando el algoritmo de generación de claves y el tamaño de clave especificado en el presente documento.

GLOBALSIGN también rechaza una solicitud de certificado si tiene una clave privada débil conocida

29.1.2 ENTREGA DE LA CLAVE PRIVADA A LOS TITULARES

GLOBALSIGN garantiza la integridad de cualquier clave pública / privada y la aleatoriedad del material de la clave a través de un RNG o PRNG adecuado. Si GLOBALSIGN detecta o sospecha que la Clave Privada se ha comunicado a una persona no autorizada o una organización no afiliada al Suscriptor, GLOBALSIGN revoca todos los Certificados que incluyen la Clave Pública correspondiente a la Clave Privada comunicada.

29.1.3 ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

GLOBALSIGN solo acepta claves públicas de ERs que hayan sido protegidas durante el tránsito y cuya autenticidad e integridad de su origen se haya verificado adecuadamente mediante la ER, tal como se describe en la Declaración de Prácticas de Registro de DIGILINK.

29.1.4 ENTREGA DE LA CLAVE PÚBLICA DE LA EC A TERCEROS ACEPTANTES

GLOBALSIGN garantiza que sus claves públicas se entreguen a las partes que confían de tal manera que se eviten los ataques de sustitución. Se anima a los navegadores web comerciales y a los operadores de plataformas a incorporar claves públicas de certificados raíz en sus almacenes raíz y sistemas operativos. La clave pública de la EC es entregada por el suscriptor en forma de una cadena de certificados o mediante un repositorio operado por GLOBALSIGN y referenciado dentro del perfil del certificado emitido a través de AIA (acceso a la información de la autoridad).

29.1.5 TAMAÑO DE LAS CLAVES

GLOBALSIGN sigue la publicación especial NIST 800-133 Revision 2 (2020) - Recomendación para la generación de claves criptográficas - para los plazos recomendados y las mejores prácticas en la elección de pares clave para las ECs de raíz, las entidades emisoras y los certificados de entidad final entregados a los suscriptores. Cualquier EC subordinada del programa raíz de confianza, fuera del control directo de GLOBALSIGN, está obligada contractualmente a utilizar las mismas prácticas recomendadas.

GLOBALSIGN selecciona de los siguientes Tamaños de Clave / Hashes para Certificados Raíces, Certificados de EC emisoras y Certificados de entidad final así como Responders de estado de certificados de CRL / OCSP.

Los certificados deben cumplir los siguientes requisitos para el tipo de algoritmo y el tamaño de la clave.

Certificados de CA raíz

	Período de validez que comienza el 31 de diciembre de 2010 o antes	Período de validez que comienza después del 31 de diciembre de 2010
Algoritmo de resumen	SHA-1, SHA-256, SHA-384 o SHA-512	SHA-256, SHA-384 o SHA-512
Tamaño mínimo del módulo RSA (bits)	2048	2048
Curva ECC	NIST P-256, P-384 o P-521	NIST P-256, P-384 o P-521

Certificados subordinados

	Período de validez que comienza el 31 de diciembre de 2010 o antes y finaliza el 31 de diciembre de 2013 o antes	Período de validez que comienza después del 31 de diciembre de 2010 o finaliza después del 31 de diciembre de 2013
Algoritmo de resumen	SHA-1, SHA-256, SHA-384 o SHA-512	SHA-1[6], SHA-256, SHA-384 o SHA-512
Mínimo RSA A tamaño del módulo (bits)	1024	2048
Curva ECC	NIST P-256, P-384 o P-521	NIST P-256, P-384 o P-521

Certificados de suscriptor

Algoritmo de resumen	SHA-1[7], SHA-256, SHA-384 o SHA-512
Tamaño mínimo del módulo RSA (bits)	2048
Curva ECC	NIST P-256, P-384 o P-521
RSASSA-PSS[8]	

Para mayor detalle, revisar la DPC de GLOBALSIGN.

29.1.6 PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

GLOBALSIGN genera pares clave de acuerdo con FIPS 186 y utiliza técnicas razonables para validar la idoneidad de las claves públicas presentadas por los suscriptores. Las llaves débiles conocidas serán probadas y rechazadas en el punto de presentación.

29.1.7 USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509)

GLOBALSIGN establece el uso clave de los Certificados en función del campo de aplicación propuesto a través del campo de uso de claves v3 para X.509 v3.

Las Claves Privadas correspondientes a Certificados Raíz no se utilizarán para firmar Certificados excepto en los siguientes casos:

1. Certificados autofirmados para representar a la propia CA raíz;
2. Certificados para CA subordinadas y certificados cruzados;
3. Certificados para verificación de respuesta OCSP.

29.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

GLOBALSIGN implementa protecciones físicas y lógicas para evitar la emisión de certificados no autorizados. La protección de la clave privada de la EC fuera del sistema o dispositivo validado especificado anteriormente debe consistir en seguridad física, cifrado o una combinación de ambos, implementados de manera que se evite la divulgación de la clave privada de la EC. GLOBALSIGN cifra su clave privada con un algoritmo y una longitud de clave que, según el estado del arte, es capaz de resistir ataques criptoanalíticos durante la vida residual de la clave cifrada o parte de la clave.

29.2.1 CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

GLOBALSIGN garantiza que todos los sistemas que firman Certificados y CRL o generan respuestas OCSP utilizan FIPS 140-2 nivel 3 como el nivel mínimo de protección criptográfica. Las ECs que exigen que los suscriptores utilicen sistemas FIPS 140-2 de nivel 2 o superior para la protección de clave privada deben obligar contractualmente al suscriptor a utilizar dicho sistema o proporcionar un mecanismo adecuado para garantizar la protección. Un mecanismo adecuado utilizado por GLOBALSIGN es la limitación de un CSP (Proveedor de servicios criptográficos) adecuado vinculado a una plataforma de hardware compatible con FIPS conocida como parte del proceso de inscripción.

29.2.2 CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

GLOBALSIGN activa claves privadas para operaciones criptográficas con control de varias personas (utilizando datos de activación de la EC) que realizan tareas asociadas con sus roles de confianza. Los roles de confianza permitidos para participar en los controles de esta clave

privada para varias personas están fuertemente autenticados (es decir, token con código PIN).

29.2.3 CUSTODIA DE LA CLAVE PRIVADA

GLOBALSIGN no custodia las claves privadas por ningún motivo.

29.2.4 BACKUP DE LA CLAVE PRIVADA

Si es necesario para la continuidad del negocio, GLOBALSIGN realiza una copia de seguridad de las claves privadas raíz y subordinadas bajo el mismo control de varias personas que la clave privada original. GLOBALSIGN no respalda las claves privadas del suscriptor.

29.2.5 ARCHIVO DE LA CLAVE PRIVADA

GLOBALSIGN no archiva las claves privadas del suscriptor y garantiza que se purgue cualquier ubicación temporal donde pueda haber existido una clave privada en cualquier ubicación de la memoria durante el proceso de generación.

29.2.6 TRANSFERENCIA DE LA CLAVE PRIVADA A/DESDE EL MÓDULO CRIPTOGRÁFICO

Las claves privadas de la EC de GLOBALSIGN se generan, activan y almacenan en los módulos de seguridad del hardware. Cuando las claves privadas están fuera de un módulo de seguridad de hardware (para almacenamiento o transferencia), se cifran. Las claves privadas nunca existen en texto sin formato fuera de un módulo criptográfico.

Si GLOBALSIGN se da cuenta de que la clave privada de una EC subordinada se ha comunicado a una persona no autorizada o una organización no afiliada a la EC subordinada, GLOBALSIGN revocará todos los certificados que incluyan la clave pública correspondiente a la clave privada comunicada.

29.2.7 ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO

GLOBALSIGN almacena las claves privadas en al menos un dispositivo FIPS 140-2 nivel 3.

29.2.8 MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

GLOBALSIGN es responsable de activar la clave privada de acuerdo con las instrucciones y la documentación proporcionada por el fabricante del módulo de seguridad del hardware. Los suscriptores son responsables de proteger las Claves Privadas de acuerdo con las obligaciones que se presentan en el Contrato de Suscriptor o Términos de uso.

29.2.9 MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

GLOBALSIGN garantiza que los módulos de seguridad de hardware que se han activado no se dejan sin supervisión o de otro modo están disponibles para acceso no autorizado. Durante el tiempo en que el Módulo de Seguridad del Hardware de la EC de GLOBALSIGN está en línea y en funcionamiento, sólo se utiliza para firmar Certificados y CRL / OCSP de

una ER autenticada. Cuando una EC ya no está operativa, las claves privadas se quitan del módulo de seguridad del hardware.

29.2.10 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

Las claves privadas de la EC de GLOBALSIGN se destruyen cuando ya no son necesarias o cuando los Certificados a los que corresponden han caducado o han sido revocados. Destruir claves privadas significa que GLOBALSIGN destruye todos los datos de activación secreta de EC asociadas en el mundo de la seguridad de tal manera que ninguna información se puede utilizar para deducir cualquier parte de la clave privada.

Las claves privadas generadas por GLOBALSIGN se almacenan en GCC en formato PKCS 12 hasta que el suscriptor capte el par de claves. Cuando el suscriptor reconoce la recepción del par de claves o cuando transcurren 30 días después de la generación de claves, el par de claves del suscriptor se elimina automáticamente de GCC.

29.2.11 EVALUACIÓN DEL MÓDULO CRIPTOGRÁFICO

Ver Sección 29.2.1.

29.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

29.3.1 ARCHIVO DE LA CLAVE PÚBLICA

GLOBALSIGN archiva las claves públicas de los certificados.

29.3.2 PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES

Los Certificados GLOBALSIGN y los Certificados renovados tienen un período de validez máximo de:

Tipo	Uso de clave privada	Período de validez máximo
Certificados raíz[9]	27 años	40 años
Sub-CA / CA emisoras de confianza pública	Sin estipulación	17 años
Raíz de confianza	Sin estipulación	10 años
Certificados PersonalSign	Sin estipulación	39 meses
Certificados de entidad final AATL	Sin estipulación	39 meses
Certificado calificado para firmas y sellos electrónicos	Sin estipulación	39 meses
Certificados de sellado de tiempo	15 meses	11 años
Firma de PDF para certificados de Adobe CDS	Sin estipulación	39 meses

El período de uso del par de claves puede tener hasta el mismo período de validez que el período de validez del certificado.

Los certificados firmados por una CA específica deben caducar antes del final del período operativo de ese par de claves.

GLOBALSIGN cumple con los requisitos básicos con respecto al período de validez máximo. En el caso de que un Certificado de Suscriptor tenga un período de validez reducido, se pueden utilizar reemisiones posteriores para recuperar ese período de validez perdido.

29.4 DATOS DE ACTIVACIÓN

29.4.1 GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

La generación y el uso de los datos de activación de GLOBALSIGN utilizados para activar las claves privadas de GLOBALSIGN se realizan durante una ceremonia clave (consulte la Sección 29.1.1). Los datos de activación son generados automáticamente por el HSM apropiado o de tal manera que satisfaga las mismas necesidades. Luego se entrega a un titular de una parte de la clave que es una persona en un papel de confianza. El método de entrega mantiene la confidencialidad e integridad de los datos de activación.

29.4.2 PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de la EC están protegidos contra la divulgación a través de una combinación de mecanismos de control de acceso criptográfico y físico. Los datos de activación de GLOBALSIGN se almacenan en tarjetas inteligentes.

29.4.3 OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de la EC de GLOBALSIGN sólo pueden ser mantenidos por el personal de EC de GLOBALSIGN en funciones de confianza.

29.5 CONTROLES DE SEGURIDAD INFORMÁTICA

29.5.1 REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

Las siguientes funciones de seguridad informática son proporcionadas por el sistema operativo, o mediante una combinación de sistema operativo, software y protecciones físicas. Los componentes de la PKI de la CA emisora incluyen las siguientes funciones:

- Requerir inicios de sesión autenticados para un rol de confianza;
- Proporcionar control de acceso discrecional con privilegios mínimos;
- Proporcionar capacidad de auditoría de seguridad (protegida en integridad);
- Prohibir la reutilización de objetos;
- Requerir el uso de una política de contraseña segura;
- Requerir el uso de criptografía para la comunicación de la sesión;
- Requerir ruta confiable para identificación y autenticación;
- Proporcionar medios para la protección de códigos maliciosos;
- Proporcionar medios para mantener la integridad del software y el firmware;
- Proporcionar aislamiento de dominio y particionamiento de diferentes sistemas y procesos; y

- Proporcionar autoprotección para el sistema operativo.

Para las cuentas capaces de causar directamente la emisión de certificados, la CA emisora cumple la autenticación multifactor.

29.5.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

No se estipula.

29.6 CONTROLES TÉCNICOS DEL CICLO DE VIDA

29.6.1 CONTROLES DE DESARROLLO DE SISTEMAS

Los controles de desarrollo del sistema para la EC de GLOBALSIGN son los siguientes:

- Usar software que ha sido diseñado y desarrollado bajo una metodología de desarrollo documentada y formal;

- Todo el hardware será inspeccionado durante el proceso de puesta en marcha para asegurar la conformidad con el suministro y no hay evidencia de manipulación encontrada. El hardware y el software adquiridos se compran de una manera para reducir la probabilidad de que cualquier componente particular fue manipulado (por ejemplo, asegurando que el equipo fue seleccionado al azar en el momento de la compra);

- El hardware y el software se desarrollan en un entorno controlado, y los procesos de desarrollo se definen y documentan. Este requisito no se aplica a los equipos comerciales de venta directa o software;

- El hardware y el software están dedicados a realizar actividades de EC. No hay otras aplicaciones, dispositivos de hardware, conexiones de red o software de componentes instalados que no formen parte de la operación de EC;

- Se toma el cuidado adecuado para evitar que el software malicioso se cargue en el equipo. Solamente las aplicaciones necesarias para realizar las operaciones de la EC se instalan en el equipo y se obtienen de fuentes autorizadas por la política local. El hardware y el software de GLOBALSIGN se analizan en busca de código malicioso en el primer uso y periódicamente después; y

- Las actualizaciones de hardware y software se compran o desarrollan de la misma manera que el equipo original y son instaladas por personal de confianza y aprobado de una manera definida.

29.6.2 CONTROLES DE GESTIÓN DE SEGURIDAD

La configuración del sistema de GLOBALSIGN, así como las modificaciones y actualizaciones, están documentadas y controladas por la administración de GLOBALSIGN. Existe un mecanismo para detectar modificaciones no autorizadas en el software o la configuración de EC de GLOBALSIGN. Se utiliza una metodología de gestión de configuración formal para la instalación y el mantenimiento continuo del sistema de la EC de GLOBALSIGN. El software

de GLOBALSIGN, cuando se carga por primera vez, se comprueba como suministrado por el proveedor, sin modificaciones, y es la versión destinada al uso.

29.6.3 CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

GLOBALSIGN, como prestador de servicios de DIGILINK, mantiene un plan de mantenimiento para asegurar el nivel de confianza de software y hardware que son evaluados y certificados.

29.7 CONTROLES DE SEGURIDAD DE LA RED

Los componentes de PKI de GLOBALSIGN implementan medidas de seguridad apropiadas para asegurar que estén protegidos contra la denegación de servicio y los ataques de intrusión. Tales medidas incluyen el uso de guardias de seguridad, firewalls y routers de filtrado. Los puertos y servicios de red no utilizados están desactivados. Todos los dispositivos de control de límites utilizados para proteger la red en la que se alojan equipos PKI niegan todos los servicios necesarios, a excepción de los necesarios, al equipo PKI incluso si dichos servicios están habilitados para otros dispositivos en la red.

29.8 SELLADO DE TIEMPO

Todos los componentes de GLOBALSIGN se sincronizan regularmente con un servicio de tiempo confiable. GLOBALSIGN utiliza una fuente GPS y una fuente DCF77 y tres relojes de fuente NTP no autenticados para establecer la hora correcta para:

- Tiempo de validez inicial de un certificado de CA;

- Revocación de un Certificado CA;

- Publicación de actualizaciones de CRL; y

- Emisión de Certificados de Entidad Final del Suscriptor.

Se pueden usar procedimientos electrónicos o manuales para mantener el tiempo del sistema. Los ajustes del reloj son eventos auditables.

29.8.1 SERVICIOS DE FIRMA DE SELLADO DE TIEMPO PDF

Todas las firmas digitales creadas por los certificados de firma PDF tienen la capacidad de incluir un sello de tiempo de confianza emitida desde un servidor de la Autoridad de sello de tiempo (TSA) compatible con RFC 3161 encadenado a un certificado raíz de Adobe. El Certificado TSA deberá estar ubicado en un nivel 2 de FIPS 140-2 o superior. Los servicios de Timestamping pueden ser proporcionados por GLOBALSIGN o por un agente de outsourcing de la EC de GLOBALSIGN. En el caso de que un servicio de sellado de tiempo sea administrado por un agente externo, GLOBALSIGN emitirá un Certificado de registro de fecha y hora de conformidad con su DPC. Los sellos provistos se encuentran sincronizados a la fuente de tiempo del Laboratorio Nacional de Metrología de Francia, la cual es reconocida por el BIPM.

30 PERFILES DE CERTIFICADOS, CRL Y OCSP

30.1 PERFIL DE CERTIFICADO

30.1.1 NÚMERO DE VERSIÓN

GLOBALSIGN emite Certificados de conformidad con X.509 Versión 3.

30.1.2 EXTENSIONES DEL CERTIFICADO

GLOBALSIGN emite Certificados de conformidad con RFC 5280 y las mejores prácticas aplicables, incluido el cumplimiento de los Requisitos de línea base del Foro CA / B actuales. La criticidad también sigue las mejores prácticas para prevenir riesgos innecesarios para las Partes que Confían cuando se aplica a restricciones de nombre.

Los certificados de entidad final y CA subordinada incluyen una extensión de uso de clave extendido que contiene KeyPurposeId (s) que describen los usos previstos del certificado. KeyPurposeId anyExtendedKeyUsage no se incluye en los certificados de confianza pública

30.1.3 IDENTIFICADORES DE OBJETOS DE ALGORITMO

GLOBALSIGN emite Certificados con algoritmos indicados por los siguientes OID:

SHA1WithRSAEncryption {iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 5}
SHA256WithRSAEncryption {iso (1) member-body (2) us (840) rsadsi (113549)) pkcs (1) pkcs-1 (1) 11}
SHA384WithRSAEncryption {iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 12}
SHA512WithRSAEncryption {iso (1) miembro-cuerpo (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 13}

ECDSAWithSHA256 {iso (1) member - body (2) us (840) ansi - X9-62 (10045) firmas (4) ecdsa - with - SHA2 (3) 2} ECDSAWithSHA384 {iso (1) member - body (2) us (840) ansi - X9-62 (10045) firmas (4) ecdsa - with - SHA2 (3) 3} ECDSAWithSHA512 {iso (1) member - body (2) us (840) ansi - X9-62 (10045) firmas (4) ecdsa - with - SHA2 (3) 4} RSASSA-PSS {iso (1) miembro-cuerpo (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) rsassa-pss (10)}

30.1.4 FORMULARIOS DE NOMBRES

GLOBALSIGN emite Certificados con formularios de nombres que cumplen con RFC 5280.

30.1.5 LIMITACIONES DE LOS NOMBRES

GLOBALSIGN puede emitir Certificados con restricciones de nombre cuando sea necesario y marcar como críticos cuando sea necesario como parte del programa Trusted Root.

El nombre de GLOBALSIGN restringe el uso de los siguientes métodos:

- Si el certificado incluye el uso de la clave extendida id-kp-serverAuth, entonces el certificado DEBE tener restricciones de nombre con restricciones en dNSName, iPAddress y DirectoryName.
- Si el certificado incluye el uso de la clave extendida id-kp-emailProtection, DEBE incluir la extensión X.509v3 de restricciones de nombre con restricciones en rfc822Name, con al menos un nombre en allowedSubtrees, cada uno de los cuales tiene su propiedad validada.
- GLOBALSIGN PUEDE también incluir restricciones de nombre en certificados con el uso de clave extendido id-kp- emailProtection con restricciones en dNSName, iPAddress y DirectoryName como se describe en la sección 7.1.5 de los Requisitos básicos del CA/B Forum

30.1.6 IDENTIFICADOR DE OBJETO DE LA POLÍTICA DE CERTIFICACIÓN

GLOBALSIGN sigue la Sección 7.1.6 de los Requisitos básicos del CA/B Forum.

30.1.7 USO DE LA EXTENSIÓN POLICY CONSTRAINS

No se estipula.

30.1.8 SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

La EC de GLOBALSIGN emite Certificados con un calificador de política y un texto adecuado para ayudar a los terceros que confían a determinar la aplicabilidad.

30.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICIES

No se estipula.

30.1.10 NÚMEROS SERIALES

La EC debe emitir certificados que incluyan un número de serie de certificado no secuencial único (dentro del contexto del DN del sujeto del emisor y el número de serie del certificado de CA) mayor que cero (0) que contenga al menos 64 bits de salida de un CSPRNG.

Los certificados están configurados para cumplir con los requisitos de perfil aplicables de ETSI EN 319 412 y ETSI TS 119 495.

30.2 PERFIL DE CRL

30.2.1 NÚMERO DE VERSIÓN

Las CRL´s emitidas por GLOBALSIGN, como prestador de servicios de DIGILINK, cumplen con la RFC 5280.

Las CRL tienen los siguientes campos:

- **Editor** El DN del sujeto de la CA emisora
- **Fecha efectiva** Fecha y hora
- **Próxima actualización** Fecha y hora
- **Algoritmo de firma** sha256RSA etc. (según el producto)
- **Algoritmo hash exclusivo** sha256 etc. (según el producto)
- **Números seriales)** Lista de números de serie revocados
- **Fecha de revocación** Fecha de revocación

30.2.2 CRL Y EXTENSIONES CRL

Las CRL tienen las siguientes extensiones:

- **Número de CRL** Número de serie que aumenta monótonamente para cada CRL
- **Identificador de clave de autoridad** AKI de la CA emisora para los requisitos de encadenamiento / validación

Se admiten las siguientes extensiones:

- **Código de razón** Identifica el motivo de la revocación del certificado.

La extensión está presente para una entrada de CRL para un certificado de CA raíz o CA subordinada, incluidos los certificados cruzados. Los valores admitidos son keyCompromise (1), affiliationChanged (3), superseded (4), cessationOfOperation (5).

La extensión puede estar presente para una entrada de CRL para un certificado de entidad final de abonado. Los valores admitidos son keyCompromise (1), affiliationChanged (3), reemplazado (4), certificateHold (6). El valor certificateHold.

30.3 PERFIL OCSP

GLOBALSIGN opera un respondedor de perfil de estado de certificado en línea (OCSP) de acuerdo con RFC 6960 y RFC 5019 y destaca esto dentro de la extensión AIA a través de una URL de respuesta OCSP.

30.3.1 NÚMERO DE VERSIÓN

GLOBALSIGN emite respuestas OCSP Versión 1 con los siguientes campos:

- Respondedor IDSHA-1 Hash de la clave pública del respondedor
- Tiempo producido hora en que se firmó esta respuesta
- Estado del certificado estado referenciado (bueno / revocado / desconocido)
- ThisUpdate / NextUpdateRecommended intervalo de validez de la respuesta
- Algoritmo de firmaSHA256 RSA, etc. (según el producto)
- Firma Firma valor generado por el respondedor
- Certificados Certificado OCSP Respondedor

Una solicitud OCSP debe contener los siguientes datos:

- Versión del protocolo
- Solicitud de servicio
- Identificador de certificado de destino

Se admiten los siguientes campos:

- revocationReasonIdentifies el motivo de la revocación del Certificado.

Este campo está presente para las respuestas OCSP para un Certificado de CA raíz o CA subordinada, incluidos los Certificados cruzados, y puede estar presente para un Certificado de entidad final de suscriptor, si se revoca el Certificado. El CRLReason indicado contiene un valor permitido para CRL, como se especifica en el presente documento.

30.3.2 EXTENSIONES OCSP

No se estipula.

31 AUDITORÍA DE CONFORMIDAD 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.

31.1 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.

31.2 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

31.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

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

31.4 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.

31.5 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.

31.6 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/

32 OTROS ASUNTOS LEGALES Y COMERCIALES

32.1 TARIFAS

32.1.1 TARIFAS DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

Las tarifas serán definidas por DIGILINK de acuerdo a los acuerdos celebrados con sus clientes. Dichas tarifas serán señaladas en las respectivas propuestas comerciales.

32.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

DIGILINK puede cobrar por el acceso a cualquier base de datos que almacene Certificados emitidos.

32.1.3 TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO

GLOBALSIGN, a través de DIGILINK, puede cobrar tarifas adicionales a los Suscriptores que tienen una gran comunidad de Partes que Confían y optan por no utilizar el servicio OCSP u otras técnicas similares para reducir la carga en la infraestructura de estado del Certificado de GLOBALSIGN.

32.1.4 TARIFAS DE OTROS SERVICIOS

GLOBALSIGN, a través de DIGILINK, puede cobrar por otros servicios adicionales como el sello de tiempo.

32.1.5 POLÍTICA DE REEMBOLSO

Una vez solicitado un certificado, esta solicitud se convierte en un contrato de prestación de servicios y no está sujeto a reembolso alguno.

32.2 RESPONSABILIDADES FINANCIERAS

32.2.1 COBERTURA DEL SEGURO

GLOBALSIGN, como proveedor de servicios de DIGILINK, mantiene un seguro comercial de responsabilidad civil general con límites de póliza de al menos dos millones de dólares estadounidenses ($ 2,000,000) en cobertura y un seguro de errores y omisiones/responsabilidad profesional con un límite de póliza de al menos cinco millones de dólares estadounidenses ($ 5,000,000) en cobertura. Las pólizas de seguro de GLOBALSIGN incluyen cobertura para (1) reclamos por daños que surjan de un acto, error u omisión, incumplimiento involuntario de contrato, y (2) reclamaciones por daños que surjan de la infracción de los derechos de propiedad de cualquier tercero (excluyendo la infracción de derechos de autor, patente y marca registrada), invasión de la privacidad y daños publicitarios. El seguro se lleva a cabo a través de compañías calificadas como mínimo A- en cuanto a la Calificación del titular de la póliza en la edición actual de Best's Insurance Guide (o con una asociación de compañías, cada uno de los miembros de las cuales está calificado de esta manera).

32.2.2 OTROS BIENES

No se estipula.

32.2.3 SEGURO O GARANTÍA DE COBERTURA PARA LAS ENTIDADES FINALES

GLOBALSIGN ofrece una Política de garantía a los suscriptores publicada en el sitio web de GLOBALSIGN en https://www.globalsign.com/en/company/corporate-policies

32.3 CONFIDENCIALIDAD DE LA INFORMACIÓN COMERCIAL

32.3.1 ÁMBITO DE LA INFORMACIÓN CONFIDENCIAL

Los siguientes elementos se clasifican como información confidencial y, por lo tanto, están sujetos a un cuidado y atención razonables por parte de GLOBALSIGN, incluidos los Operadores de Registro y los administradores:

- Información personal como se detalla en la Sección 32.4;

- registros de auditoría de los sistemas de la EC y ER;

- Datos de activación utilizados para activar las Claves privadas de la EC;

- Documentación interna de procesos empresariales de GLOBALSIGN CA, incluidos los planes de recuperación de desastres (DRP) y Planes de Continuidad de Negocios (BCP); e

- Informes de auditoría de un auditor independiente como se detalla en la Sección 31.

32.3.2 INFORMACIÓN NO CONFIDENCIAL

Cualquier información no definida como confidencial dentro de esta DPC se considerará pública. La información sobre el estado del certificado y los propios certificados, se consideran públicos.

32.3.3 DEBER DE PROTEGER LA INFORMACIÓN CONFIDENCIAL

GLOBALSIGN, como prestador de servicios de DIGILINK, protege la información confidencial a través del entrenamiento y cumplimiento con empleados, agentes y contratistas.

32.4 PROTECCIÓN DE LA INFORMACIÓN PERSONAL

32.4.1 PLAN DE PRIVACIDAD

GLOBALSIGN protege la información personal de acuerdo con una Política de Privacidad publicada en el sitio web de GLOBALSIGN en https://www.globalsign.com/repository

32.4.2 INFORMACIÓN TRATADA COMO PRIVADA

GLOBALSIGN y DIGILINK tratan toda la información recibida de los Solicitantes que normalmente no se colocará en un Certificado como privado. Esto se aplica tanto a los Solicitantes que tienen éxito en la expedición de un Certificado y los que son infructuosos y rechazados. GLOBALSIGN y DIGILINK capacitan periódicamente al personal de la ER y el staff de verificadores, así como a cualquier persona que tenga acceso a la información sobre la debida cuidado y atención que debe aplicarse.

32.4.3 INFORMACIÓN NO CALIFICADA COMO PRIVADA

La información del estado del certificado y cualquier contenido del certificado se consideran no privados.

32.4.4 RESPONSABILIDAD DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

GLOBALSIGN, como proveedor de servicios de DIGILINK, es responsable de almacenar de forma segura información privada de acuerdo con su Política de Privacidad publicada y puede almacenar información recibida en papel o en formato digital. Cualquier copia de seguridad de información privada debe ser cifrada cuando se transfiere a medios de copia de seguridad adecuados. La Política de privacidad se publica en el sitio web de GLOBALSIGN en https://www.globalsign.com/repository

32.4.5 NOTIFICACIÓN Y CONSENTIMIENTO PARA USAR DATOS DE CARÁCTER PERSONAL

La información personal obtenida de los Solicitantes durante el proceso de inscripción y solicitud se considera privada y se requiere permiso del Solicitante para permitir el uso de

dicha información. DIGILINK o DIGILINK incluyen cualquier consentimiento requerido en el Acuerdo de Suscriptor, incluyendo cualquier permiso requerido para obtener información adicional de terceros que pueda ser aplicable al proceso de validación del producto o servicio ofrecido por GLOBALSIGN o DIGILINK.

32.4.6 REVELACIÓN EN EL MARCO DE UN PROCESO ADMINISTRATIVO O JUDICIAL

GLOBALSIGN puede divulgar información privada sin previo aviso a los Solicitantes o Suscriptores cuando así lo requiera la ley o la regulación.

32.4.7 OTRAS CIRCUNSTANCIAS DE REVELACIÓN DE INFORMACIÓN

No se estipula.

32.5 DERECHOS DE PROPIEDAD INTELECTUAL

GLOBALSIGN, como proveedor de servicios de DIGILINK, no viola a sabiendas los derechos de propiedad intelectual de terceros. Las Claves Públicas y Privadas siguen siendo propiedad de los Suscriptores que las tienen legítimamente. GLOBALSIGN mantiene la propiedad de los Certificados; sin embargo, otorga permiso para reproducir y distribuir los Certificados sobre una base no exclusiva, libre de regalías, siempre que se reproduzcan y distribuyan en su totalidad.

32.6 OBLIGACIONES

32.6.1 OBLIGACIONES DE LA EC

DIGILINK está obligada según normativa vigente a lo siguiente:

- Respetar lo dispuesto en la normatividad vigente y en esta DPC.
- Publicar esta DPC en la página Web de DIGILINK.
- Informar al INDECOPI sobre las modificaciones de esta DPC.
- Mantener publicada en la página Web de DIGILINK la última versión de la DPC.
- Mantener publicada en la página Web de GLOBALSIGN la última versión de su DPC.
- Proteger y custodiar de manera segura y responsable la clave privada de la EC.
- Emitir certificados conforme a los estándares definidos en la presente DPC.
- Generar certificados consistentes con la información suministrada por el solicitante o titular.
- Conservar la información sobre los certificados emitidos de conformidad con la normatividad vigente.

- Emitir certificados cuyo contenido mínimo se encuentre en conformidad con la normativa vigente para los diferentes tipos de certificados.
- Publicar el estado de los certificados emitidos en un repositorio de acceso libre.
- No mantener copia de la clave privada del solicitante o titular.
- Revocar los certificados según lo dispuesto en esta DPC.
- Actualizar y publicar la lista de certificados revocados CRL con los últimos certificados revocados.
- Notificar al Solicitante o Titular la revocación del certificado digital dentro de las 24 horas siguientes a la revocación del certificado de conformidad con esta DPC.

32.6.2 OBLIGACIONES DE LA ER

La ER se encuentra obligada a a:

1. Conocer y dar cumplimiento a lo dispuesto en la presente DPC.
2. Comprobar la identidad de los Solicitantes y Titulares de certificados digitales.
3. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
4. Archivar y custodiar la documentación suministrada por el solicitante o titular, durante el tiempo establecido por la legislación vigente.
5. Respetar lo dispuesto en los contratos firmados entre DIGILINK y el titular
6. Identificar e informar a la EC las causas de revocación suministradas por los solicitantes sobre los certificados digitales vigentes.

32.6.3 OBLIGACIONES DEL TITULAR

El Titular como titular de un certificado digital está obligado a cumplir con lo dispuesto por la normativa vigente y lo dispuesto en la presente DPC, como es:

1. Suministrar toda la información requerida en el Formulario de Solicitud de Certificados Digitales para facilitar su oportuna y plena identificación.
2. Cumplir con lo aceptado y firmado en el Formulario de Solicitud de certificado digital.
3. Proporcionar con exactitud y veracidad la información requerida.
4. Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del certificado.
5. Custodiar y proteger de manera responsable su clave privada.
6. Dar uso al certificado de conformidad con la presente DPC para cada uno de los tipos de certificado.
7. Solicitar como titular de manera inmediata la revocación de su certificado digital cuando tenga conocimiento que existe una causal definida en la presente DPC.
8. No hacer uso de la clave privada ni del certificado digital una vez cumplida su vigencia o se encuentre revocado.

9. Informar a los terceros de confianza de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado.
10. Informar al Tercero que confía para verificar el estado de un certificado dispone de la lista de certificados revocados CRL, publicada de manera periódica por GLOBALSIGN, como prestador de servicios de DIGILINK.

32.6.4 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Los Terceros que confían en su calidad de parte que confía en los certificados digitales emitidos por GLOBALSIGN, está en la obligación de:

1. Conocer lo dispuesto sobre Certificación Digital en la Normatividad vigente.
2. Conocer lo dispuesto en la presente DPC.
3. Verificar el estado de los certificados antes de realizar operaciones con certificados digitales.
4. Verificar la Lista de certificados Revocados CRL antes de realizar operaciones con certificados digitales.
5. Conocer y aceptar las condiciones sobre garantías, usos y responsabilidades al realizar operaciones con certificados digitales.

32.6.5 OBLIGACIONES DE LA ENTIDAD

Conforme lo establecido en las Políticas de Certificación anexadas a este documento, en el caso de los certificados donde se acredite la vinculación del Titular con la misma será obligación de la Entidad solicitar a la ER la suspensión/revocación del certificado cuando cese o se modifique dicha vinculación.

32.6.6 OBLIGACIONES DE OTROS PARTICIPANTES

No se estipula.

32.7 RENUNCIAS DE GARANTÍAS

Excepto en la medida en que lo prohíbe la ley o se dispone de otro modo aquí, GLOBALSIGN renuncia a todas las garantías, incluyendo cualquier garantía de comerciabilidad y / o aptitud para un propósito en particular.

32.8 LIMITACIONES DE RESPONSABILIDAD

GLOBALSIGN, como proveedor de servicios de DIGILINK, establece los límites de responsabilidad en su DPC.

32.9 INDEMNIZACIONES

32.9.1 INDEMNIZACIÓN POR GLOBALSIGN

GLOBALSIGN, como proveedor de servicios de DIGILINK, establece los términos de su indemnización en su DPC.

32.9.2 INDEMNIZACIÓN POR SUSCRIPTORES

En la medida en que lo permita la ley, cada Suscriptor indemnizará a GLOBALSIGN, sus socios y cualquier entidad raíz de confianza, y sus respectivos directores, funcionarios, empleados, agentes y contratistas por cualquier pérdida, daño o gasto, incluidos los honorarios razonables de abogados, relacionados a (i) cualquier tergiversación u omisión de un hecho material por parte del Suscriptor, independientemente de si la tergiversación u omisión fue intencional o no intencional; (ii) El incumplimiento del suscriptor del Acuerdo de suscripción, esta DPC o la ley aplicable; (iii) el Compromiso o uso no autorizado de un Certificado o Clave Privada causado por la negligencia del Suscriptor; o (iv) el uso indebido del Certificado o la Clave Privada por parte del Suscriptor.

32.9.3 INDEMNIZACIÓN POR LAS PARTES QUE CONFÍAN

En la medida en que lo permita la ley, cada Parte que Confía indemnizará a GLOBALSIGN, sus socios y cualquier entidad con firma cruzada, y sus respectivos directores, funcionarios, empleados, agentes y contratistas por cualquier pérdida, daño o gasto, incluidos los honorarios razonables de abogados. , relacionado con el (i) incumplimiento por parte de la Parte que Confía del Acuerdo de la Parte que Confía, esta DPC o la ley aplicable; (ii) dependencia irrazonable de un Certificado; o (iii) no verificar el estado del Certificado antes de su uso.

33 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

34 CONFORMIDAD CON LA LEY APLICABLE

DIGILINK es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación para Entidades de Certificación Digital EC, Ley N° 27269, Ley de Firmas y Certificados Digitales, su reglamento aprobado por el D.S. 052-2008-PCM y sus modificatorias, para el reconocimiento legal de los servicios de valor añadido emitidos bajo las directrices definidas en el presente documento.

35 CONFORMIDAD

Este documento ha sido aprobado y su cumplimiento es supervisado anualmente por el Responsable de la Entidad de Certificación de DIGILINK, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

36 BIBLIOGRAFÍA

a) Guía de Acreditación para Entidades de Certificación Digital EC, INDECOPI
b) Ley de Firmas y Certificados Digitales – Ley 27269
c) Decreto Supremo 052-2008
d) Decreto Supremo 070-2011
e) Decreto Supremo 105-2012