POLÍTICA Y PLAN DE SEGURIDAD

Entidad de Certificación y Autoridad de Sellado de Tiempo

Información del documento	
Nombre de documento: **Política y Plan de Seguridad de EC y TSA de DIGILINK**	
Código de documento: **DL-POL-02**	
Versión: **1.1**	Aprobado por: **Responsable de la EC y TSA**
Año: **2021**	Dirigido a: **INDECOPI**

Control de versiones		
Versión	**Fecha**	**Descripción**
1.0	27-11-2021	Elaboración de documento inicial.
1.1	22-03-2022	Se realizaron cambios en el formato.

ÍNDICE

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, reemisión 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 OBJETO

En principio, este documento tiene como objetivo la declaración de cumplimiento de las medidas de seguridad. Asimismo, se realiza una descripción de las operaciones y prácticas que lleva a cabo DIGILINK para garantizar la seguridad de la información que es tratada durante todo el proceso de certificación digital.

Todas las prácticas se realizan conforme al marco del cumplimiento de los requerimientos de la Guía de Acreditación de Entidades de Certificación Digital (EC) y para Prestadores de Servicios de Valor Añadido (SVA) tipo Autoridad de Sellado de Tiempo, establecidas por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital y de sellado de tiempo de DIGILINK, por medio de su proveedor de servicios GLOBALSIGN.

4 DEFINICIONES Y ABREVIACIONES

4.1 ABREVIACIONES

AAC: Autoridad Administrativa Competente

DN: (Distingued Name) Nombre Distintivo

EC: Entidad de Certificación

ER: Entidad de Registro

CPS: (Certification Practice Statement) Declaración de Prácticas de Certificación

CRL: Lista de Certificados Revocados

IOFE: Infraestructura Oficial de Firma Electrónica

PC: Política de Certificación

4.2 DEFINICIONES

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.
Autoridad de Sellado de Tiempo - TSA	Autoridad que emite los sellos de tiempo, en los cuales confían los suscriptores y terceros que confían.
Declaración de Prácticas de Certificación – DPC o CPS	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.

5 ALCANCE

El presente documento es aplicable a las operaciones de la EC y la TSA brindado por Digilink.

6 RESPONSABILIDADES

Las responsabilidades contractuales, garantías financieras y coberturas de seguros de los servicios de certificación digital y de sellado de tiempo son brindadas por GLOBALSIGN, en calidad de proveedor de servicios de DIGILINK.

No obstante, DIGILINK representa todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano con la EC y TSA.

Las peticiones, quejas o reclamos para la atención de suscriptores y terceros debido a consultas relacionadas con el servicio que dispone la EC y TSA, son recibidas directamente por DIGILINK mediante la línea telefónica o correo electrónico. Asimismo, pueden acercarse hacia la oficina de DIGILINK, indicando que presenta una queja, reclamo o petición. Los datos de Contacto se encuentran en la sección 8 de la CPS.

7 CONTROLES FÍSICOS DE LA INSTALACIÓN, GESTIÓN Y OPERACIONALES

GLOBALSIGN, como proveedor de servicios de DIGILINK mantiene políticas de seguridad física y ambiental para los sistemas utilizados para la emisión y gestión de certificados. Dicho proceso de gestión de certificados de GlobalSign DEBE incluir:

- Seguridad física y controles ambientales;
- Controles de integridad del sistema, incluida la gestión de la configuración, el mantenimiento de la integridad del código de confianza y la detección/prevención de malware;

- Gestión de seguridad de red y firewall, incluidas restricciones de puerto y filtrado de direcciones IP;
- Gestión de usuarios, asignaciones independientes de roles de confianza, educación, concienciación y formación; y
- controles de acceso lógico, registro de actividad y tiempos de espera de inactividad para proporcionar responsabilidad individual.

El programa de seguridad de GLOBALSIGN incluye una evaluación de riesgos anual que:

1. Identifica amenazas internas y externas previsibles que podrían resultar en un acceso no autorizado, divulgación, uso indebido, alteración o destrucción de cualquier Datos de certificado o Procesos de gestión de certificados;
2. Evalúa la probabilidad y el daño potencial de estas amenazas, teniendo en cuenta la sensibilidad de los Datos del certificado y los Procesos de gestión del certificado; y
3. Evalúa la suficiencia de las políticas, procedimientos, sistemas de información, tecnología y otros arreglos que GlobalSign tiene para contrarrestar tales amenazas.

Con base en la Evaluación de Riesgos, GlobalSign desarrolla, implementa y mantiene un plan de seguridad que consta de procedimientos, medidas y productos de seguridad diseñados para lograr los objetivos establecidos anteriormente y para administrar y controlar los riesgos identificados durante la Evaluación de Riesgos, acorde con la sensibilidad. de los Procesos de Gestión de Certificados y Datos de Certificados.

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

7.1 CONTROLES FÍSICOS DE LA INFRAESTRUCTURA TECNOLÓGICA

GlobalSign, como proveedor de DIGILINK, mantiene políticas de seguridad física y ambiental para los sistemas utilizados para la emisión y administración de Certificados que cubren el control de acceso físico, la protección contra desastres naturales, los factores de seguridad contra incendios, fallas de los servicios públicos de apoyo (por ejemplo, energía, telecomunicaciones), colapso de estructuras, fugas de plomería, protección contra robo, allanamiento de morada y recuperación de desastres. Los controles se implementan para evitar la pérdida, daño o compromiso de los activos y la interrupción de las actividades

comerciales y el robo de la información y las instalaciones de procesamiento de la información.

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.1.4 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.

7.1.5 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.

7.1.6 SISTEMA DE ALMACENAMIENTO

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

7.1.7 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.

7.1.8 BACKUP FUERA DE LA INSTALACIÓN

GlobalSign realiza copias de seguridad periódicas fuera del sitio de datos críticos. Los datos respaldados se almacenan en una ubicación externa protegida físicamente.

7.2 CONTROLES DE PROCEDIMIENTO

7.2.1 ROLES DE CONFIANZA

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

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

• **Desarrollador**: Responsable del desarrollo de sistemas de la EC.

• **Oficial de Seguridad / Jefe de Seguridad de la Información**: Responsabilidad general de administrar la implementación de las prácticas de seguridad de la EC;

• **Ingeniero de sistemas de Infra**: Autorizado para instalar, configurar y mantener los sistemas de la EC utilizados para la Gestión del ciclo de vida del certificado;

• **Operador de Infra**: Responsable de operar los sistemas de la EC en el día a día. Autorizada para realizar la copia de seguridad / recuperación del sistema, ver / mantener los archivos del sistema de la EC y los registros de auditoría;

• **Auditor**: Autorizado para ver archivos y registros de auditoría de los Sistemas Confiables de la EC;

• **Titular de datos de activación de CA**: Persona autorizada que contiene los datos de activación de la EC necesarios para la operación de módulo de seguridad de hardware de la EC;

• **Operador de Registro**: Es el responsable de verificar que la información suministrada por los solicitantes de certificados digitales sea auténtica e íntegra. Es el responsable de solicitar en nombre de los titulares la emisión o revocación de certificados digitales.

• **Titular de los datos de activación de CA**: persona autorizada que posee los datos de activación de la EC,necesario para el funcionamiento del módulo de seguridad de hardware de la EC..

7.2.2 NÚMERO DE PERSONAS REQUERIDAS POR TAREA

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

7.2.3 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.

7.2.4 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 6.2.1 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)

7.3 CONTROLES DE PERSONAL

7.3.1 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 privilegios, 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.

7.3.2 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.

7.3.3 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

7.3.4 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.

7.3.5 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.

7.3.6 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.

7.3.7 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.

7.3.8 DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

GlobalSign pone a disposición de su personal su CPS, cualquier CP correspondiente y cualquier estatuto, política o contrato pertinente. Se proporcionan otros documentos técnicos, operativos y administrativos (por ejemplo, manuales de administrador, manuales de usuario, etc.) para que el personal de confianza pueda desempeñar sus funciones.

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

7.4 PROCEDIMIENTOS DE CONTROL DE SEGURIDAD

A fin de garantizar una correcta gestión de la seguridad en los sistemas de información, GLOBALSIGN lleva a cabo los controles descritos a continuación.

7.4.1 TIPOS DE EVENTOS REGISTRADOS

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

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

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

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

GlobalSign registra al menos los siguientes eventos:

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

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

- Aprobación y rechazo de solicitudes de Certificados;
- Eventos de gestión del ciclo de vida del dispositivo criptográfico (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 CPS;
- Aprobación y rechazo de solicitudes de certificados;
- Emisión de Certificados; y
- Generación de listas de revocación de certificados y entradas OCSP.

Eventos de seguridad, que incluyen:

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

7.4.2 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.

7.4.3 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.

7.4.4 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.

7.4.5 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.

7.4.6 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.

7.4.7 NOTIFICACIÓN AL SUJETO CAUSA DEL EVENTO

No se estipula.

7.4.8 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.

7.5 ARCHIVO DE REGISTROS

7.5.1 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.

7.5.2 PERIODO DE CONSERVACIÓN

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

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

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.

7.5.3 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.

7.5.4 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.

7.5.5 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 7.8. Sellado de tiempo, todos los registros deben tener datos que indiquen el momento en que ocurrió el evento.

7.5.6 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 6.

7.5.7 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).

7.6 CAMBIO DE CLAVES DE UNA EC

GlobalSign puede cambiar periódicamente el material clave para las ECs Emisoras de acuerdo a la sección 7.3.2. 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.

7.7 RECUPERACIÓN EN CASO DE COMPROMISO Y DESASTRE

7.7.1 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.

7.7.2 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.

7.7.3 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.

7.7.4 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 6.7.1. Los sistemas de información del estado del certificado deben ser desplegados para proporcionar disponibilidad las 24 horas del día, 365 días al año.

7.8 CESE DE UNA EC O ER

Antes de su finalización, la ER 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 ER que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección:
https://digilink.pe

8 CONTROLES TÉCNICOS DE SEGURIDAD

- GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES
- GENERACIÓN DEL PAR DE CLAVES DE LA EC

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:

1. Genera las claves en un entorno físicamente seguro como se describe en la Sección 5.1 y

   5.2.2. de la Política de Certificación y / o Declaración de Prácticas de Certificación;

2. Genera las claves de CA utilizando personal en roles confiables bajo los principios de control de múltiples personas y conocimiento dividido;
3. Generar 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;
4. Registre sus actividades de generación de claves de CA; y

Mantenga 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

8.1 GENERACIÓN DEL PAR DE CLAVES DEL SUSCRIPTOR

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.

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

8.2 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.

8.3 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.

8.4 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).

8.5 TAMAÑO DE LAS CLAVES

GlobalSign sigue la publicación especial NIST 800-133 Revisión 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 RS 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.

8.5.1 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.

8.5.2 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.

8.6 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.

8.6.1 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.

8.6.2 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).

8.6.3 CUSTODIA DE LA CLAVE PRIVADA

GlobalSign no custodia las claves privadas por ningún motivo.

8.6.4 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.

8.6.5 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.

8.6.6 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.

8.6.7 ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO

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

8.6.8 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.

8.6.9 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.

8.6.10 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.

8.6.11 EVALUACIÓN DEL MÓDULO CRIPTOGRÁFICO

Ver Sección 7.2.1.

8.7 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

8.7.1 ARCHIVO DE LA CLAVE PÚBLICA

GlobalSign archiva las claves públicas de los certificados.

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

Los certificados de Globalsign, emitidos a través de Digilink, tienen un periodo de validez limitado. Los certificados de la CA raíz tienen un periodo de validez máximo de 40 años; los certificados de las CA subordinadas, como máximo 17 años; los certificados de persona natural, persona jurídica y de agente automatizado, como máximo 2 años; y los certificados de sellado de tiempo, hasta 11 años.
GlobalSign cumple con los requisitos básicos con respecto al periodo de validez máximo.

8.8 DATOS DE ACTIVACIÓN

8.8.1 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.

8.8.2 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.

8.8.3 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.

8.9 CONTROLES DE SEGURIDAD INFORMÁTICA

8.9.1 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 incluyenlas 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;
- Proporcionar autoprotección para el sistema operativo.

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

8.9.2 EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

No se estipula.

8.10 CONTROLES TÉCNICOS DEL CICLO DE VIDA

8.10.1 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.

8.10.2 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.

8.10.3 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.

8.11 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.

8.12 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.

8.12.1 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 emitido 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 CPS.

9 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.

9.1 FRECUENCIA O CIRCUNSTANCIAS DE LOS CONTROLES

Digilink se somete anualmente a las auditorías programadas por el INDECOPI.
GlobalSign, en calidad de proveedor de infraestructura de DIGILINK, 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.

9.2 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

9.3 RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

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

9.4 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.

9.5 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.

9.6 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/

10 CONFORMIDAD

Esta Política de Seguridad ha sido aprobada por el Responsable de la EC de DIGILINK. Cada vez que se genere un cambio en este documento, se procederá a informar previamente a INDECOPI y al dar conformidad, será nuevamente aprobada por el Responsable de la EC.

11 PUBLICACIÓN

La versión vigente del presente documento se encuentra disponible en la página web de Digilink https://digilink.pe para conocimiento del personal de Digilink y del público en general.

12 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

Firmado por: JOSE ENRIQUE CAMARENA MEJIA
DNI:08083238
RUC:20606433507
Motivo: FIRMA DIGITAL