POLÍTICA Y PLAN DE SEGURIDAD

Entidad de Registro

Información del documento	
Nombre de documento: **Política y Plan de Seguridad de la Entidad de Registro de DIGILINK**	
Nombre de documento: **DL-PPSREG-01**	
Versión: **1.2**	Aprobado por: **Responsable de la Entidad de Registro**
Año: **2024**	Dirigido a: **INDECOPI**

Control de versiones		
Versión	**Fecha**	**Descripción**
1.0	03-01-2022	Elaboración de documento inicial.
1.1	15-09-2023	Se realizaron cambios en el formato. Se ha incluido el logo y el código en la cabecera del documento.
1.2	25-01-2024	Cambio de Representante Legal de la empresa.

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 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas de seguridad que utiliza DIGILINK para la administración de sus servicios como Entidad de Registro o Verificación – ER, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Registros o Verificación (ER)" establecida por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre los sistemas de registro que utiliza DIGILINK en la entrega de sus servicios, y que son proporcionados por la Entidad de Certificación de DIGILINK.

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.
Política de Certificación	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, 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 acreditadas, es una persona jurídica privada que presta indistintamente servicios relacionados con las funciones de infraestructura de clave pública (PKI) como el registro de suscriptores, producción, emisión, renovación, gestión, cancelación u otros servicios inherentes a la certificación digital.

4.1.2 ENTIDAD DE REGISTRO 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 re-emisión y renovación (a veces denominadas como nueva clave) de certificados.

4.1.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL E INFRAESTRUCTURA

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de 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.

Actualmente, los servicios de registro digital que ofrece DIGILINK son provistos por la EC de DIGILINK.

Los servicios de certificación digital que ofrece DIGILINK son provistos en un contrato de tercerización por 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 RPS de DIGILINK.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por DIGILINK como prestadores de servicios de la misma, conforme a lo establecido en la Política de Certificación.

4.1.5 SUSCRIPTOR

Conforme a la IOFE, el Suscriptor es el 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 CPS 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 DIGILINK. 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 ALCANCE

La presente política es de cumplimiento obligatorio para el personal contratado por DIGILINK que participan de las operaciones críticas de los servicios de registro descritos en la Declaración de Prácticas de Registro.

6 SERVICIOS DE CERTIFICACIÓN DIGITAL

DIGILINK, brinda los servicios de verificación y registro de usuarios que solicitan la emisión, revocación y distribución de los certificados digitales provistos por su Entidad de Certificación.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritos en la Declaración de Prácticas y las Políticas de Certificación de DIGILINK que se encuentran en su página web.

7 RESPONSABILIDADES

GLOBALSIGN, como proveedor de infraestructura y responsable de la gestión de operaciones de los servicios de la EC de DIGILINK, asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital provistos por la EC de DIGILINK.

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por DIGILINK.

DIGILINK es responsable de exigir y supervisar las operaciones de los servicios de la EC que son administrados por el proveedor de infraestructura y responsable de la gestión de operaciones.

Como Entidad de Registro, DIGILINK es responsable de la correcta identificación de las personas naturales o jurídicas y de la seguridad en la entrega de certificados digitales, siempre que esta sea realizada por los Operadores de Registro autorizados.

Las peticiones, quejas o reclamos sobre los servicios prestados por DIGILINK o de su proveedor de infraestructura son recibidas directamente por la EC o ER de DIGILINK. La línea telefónica es permanente para la atención a suscriptores y terceros debido a consultas relacionadas con el servicio que dispone DIGILINK. Asimismo, pueden acercase hacia la oficina de ER de DIGILINK indicando que presenta una queja, reclamo o petición. El suscriptor recibirá un mensaje de correo electrónico, cuando el reclamo o apelación sea resuelto.

8 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La ER de DIGILINK tiene como objetivo de seguridad, garantizar la autenticidad e integridad de la información crítica de los procesos de registro, mediante la gestión de riesgos de seguridad y la aplicación de políticas y estándares que regulen las actividades críticas de las operaciones de validación y registro, por parte del personal y terceros subcontratados, en cumplimiento de las obligaciones de la ER en los ámbitos legales, regulatorios y contractuales.

Los controles son definidos en base a la identificación y valoración de los activos que forman parte de las operaciones de registro, así como la identificación de amenazas y vulnerabilidades de estos activos críticos, la evaluación del impacto de los riesgos, y el tratamiento de los riesgos de impacto grave y moderado que puedan presentarse en los procesos de registro contemplados por la ER de DIGILINK.

9 PLAN DE SEGURIDAD DE LA INFORMACIÓN

A fin de dar cumplimiento a los objetivos de seguridad indicados, DIGILINK ha implementado una serie de controles de seguridad que se describen en adelante.

9.1 SEGURIDAD FÍSICA

9.1.1 UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

La ubicación y diseño de las instalaciones de la ER de DIGILINK prevé el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre.

9.1.2 SEGURIDAD FÍSICA DEL PERSONAL Y EL EQUIPAMIENTO

A fin de proteger al personal y el equipamiento en las instalaciones de la ER de DIGILINK, se implementaron los siguientes controles:

a) Señalización de zonas seguras
b) Provisión de extinguidores contra incendios
c) Cableado eléctrico no expuesto
d) Uso de estabilizadores y supresores de picos

9.1.3 PERÍMETROS DE SEGURIDAD Y CONTROL DE ACCESO FÍSICO

Las áreas de archivo de documentos en papel y archivos electrónicos, se encuentran protegidas constantemente contra acceso no autorizado:

a) Solo ingresa personal autorizado
b) Los terceros y el personal de limpieza pueden ingresar con autorización del Responsable de Seguridad, deben ser previamente identificados y deben ser registrados y supervisados durante su estancia en el área
c) Cuando sea asignado un personal nuevo se deberán verificar sus antecedentes

Las operaciones de validación y registro pueden realizarse en las instalaciones de DIGILINK o en las instalaciones del cliente o cualquier otro lugar definido por él en presencia del Operador de Registro, el cual será responsable de proteger la información proporcionada por el cliente.

9.1.4 PROTECCIÓN CONTRA INCENDIOS

Las instalaciones poseen las siguientes medidas para la prevención y protección contra incendios:

a) Está prohibido fumar o generar cualquier fuente de humo o fuego dentro de las áreas de archivo y en las instalaciones de la ER de DIGILINK.
b) Se cuenta con un extinguidor visible, destinado a extinguir fuego sobre equipos electrónicos y documentos en papel.
c) Una copia de los documentos y archivos electrónicos, que poseen las solicitudes de los servicios de registro y los contratos de los titulares y suscriptores se encuentra guardada en un lugar de contingencia protegida por el Responsable de la ER, contra acceso no autorizado

9.1.5 ARCHIVO DE MATERIAL

Los archivos se almacenan de manera electrónica y se encuentran protegidos en el repositorio ALFRESCO y su acceso está restringido a personal autorizado.

9.1.6 GESTIÓN DE RESIDUOS

Los archivos tanto electrónicos (contratos de suscriptores y solicitudes de los servicios de registro) y el material distintivo (formatos membretados propios de la ER), que requieran ser eliminados o su soporte electrónico requiera ser desechado, serán borrados o destruidos de manera irrecuperable.

9.2 GESTIÓN DE ROLES

9.2.1 ROLES DE CONFIANZA

Los roles de confianza son definidos de la siguiente manera:

- Responsable de la ER
- Responsable de Seguridad y de Privacidad
- Operadores de Registro
- Auditor interno

Estos roles son asignados formalmente por el Responsable de la ER de DIGILINK.

La descripción de los roles incluye las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que son puestas de manifiesto a las personas que ejercen dichas funciones. Se cuenta con constancia por escrito del conocimiento de las mismas.

9.2.2 NÚMERO DE PERSONAS REQUERIDAS POR LABOR

Los cambios en los documentos normativos requieren de la autorización del Responsable de la ER y el Responsable de Seguridad y Privacidad. Dichos roles no son incompatibles y pueden ser asumidos por un mismo cargo.

El Auditor interno será siempre una persona independiente de las operaciones de registro.

9.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Los roles de confianza emplean controles de acceso físico para el acceso a las áreas de archivo, así como lógicos para las comunicaciones con la EC. Los controles de acceso a

los sistemas de Registro dependen de la configuración de los sistemas de cada EC y no de la ER de DIGILINK.

9.2.4 ROLES QUE REQUIEREN FUNCIONES POR SEPARADO

El auditor asignado por el INDECOPI deberá ser siempre una persona independiente de las operaciones de registro.

9.3 GESTIÓN DEL PERSONAL

9.3.1 ACUERDOS DE CONFIDENCIALIDAD

Los empleados y contratistas deben ser requeridos de cumplir términos de confidencialidad y provisiones de no revelación de información confidencial o privada, así como la legislación que rige a las transacciones que se realizan bajo el marco de la IOFE, la legislación relativa al régimen de los trabajadores y cualquier otra legislación relevante, de conformidad con la Norma Marco sobre Privacidad presentada en el anexo 6 de la Guía de Acreditación de ER.

Esta información debe ser entregada por escrito a sus empleados y contratistas, debiéndose obtener declaración por escrito por parte de estas personas respecto al conocimiento de toda esta información.

Esta información debe ser incorporada en todos los contratos de trabajo o servicio.

9.3.2 CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS

Los roles de confianza cuentan con conocimiento y entrenamiento en las operaciones de registro digital, la Política y Plan de Seguridad de la Información, y la Política y Plan de Privacidad. Asimismo, cuentan con experiencia relacionada a los temas de certificación digital.

9.3.3 PROCEDIMIENTO PARA VERIFICACIÓN DE ANTECEDENTES

Se verifican los antecedentes de todos los candidatos a empleados en concordancia con las leyes vigentes y normatividad pertinente, que participan y tienen acceso a las operaciones y sistemas de registro, incluyendo:

- Verificación de antecedentes penales
- Verificación de antecedentes policiales

Las personas que desempeñan roles de confianza tienen en claro el nivel de sensibilidad y valor de los bienes y transacciones protegidos por la actividad de la cual ellas son responsables.

9.3.4 REQUISITOS DE CAPACITACIÓN

Todos los empleados de la organización que participan de los servicios de registro reciben las capacitaciones apropiadas y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral:

- El equipo y software requerido para operar.
- Los aspectos de la Declaración de Prácticas y Política de Registro, Política y Plan de Seguridad, Política de privacidad, Plan de privacidad y otra documentación relevante que afecte sus funciones.
- Requisitos legislativos en relación a sus funciones.
- Sus roles en relación al Plan de Contingencias.

9.3.5 FRECUENCIA Y REQUISITOS DE LAS RE-CAPACITACIONES

Las sesiones de capacitación y entrenamiento serán llevadas a cabo anualmente y cuando existan cambios significativos en los elementos tratados en la capacitación inicial y cada vez que se adhiera, sustituya o rote al personal encargado.

9.3.6 FRECUENCIA Y SECUENCIA DE LA ROTACIÓN EN EL TRABAJO

No se implementará rotación de los trabajadores.

9.3.7 SANCIONES POR ACCIONES NO AUTORIZADAS

Se llevará a cabo un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad, una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza. Dicha persona será inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.

Dichas sanciones se encuentran establecidas en los contratos de cada empleado y/o contratista.

9.3.8 REQUERIMIENTOS DE LOS CONTRATISTAS

El personal contratado para fines específicos dentro de las operaciones de la ER de DIGILINK, será evaluado respecto de sus antecedentes criminales, conocimiento y experiencia. Asimismo, no deberá tener acceso sin supervisión a las áreas de archivo y no tendrá acceso a los sistemas de registro brindados por la EC.

9.3.9 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL

Se entregará al personal la documentación necesaria para el desempeño de sus funciones:

- Una declaración de funciones y autorizaciones.
- Manuales para los equipos de software que deben de operar.
- Aspectos de la Declaración de Prácticas y Política de Registro, Política y Plan de Seguridad, Política de privacidad, Plan de privacidad y otra documentación relevante en relación a sus funciones.
- Legislación aplicable a sus funciones.
- Documentación respecto a sus roles frente a plan de contingencia.

9.4 PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS

9.4.1 TIPOS DE EVENTOS REGISTRADOS

Los sistemas de información sensible son provistos por la EC, por lo que la ER de DIGILINK sólo puede acceder vía web. En este sentido, los logs de auditoría son administrados y definidos por la EC.

Se guardarán los contratos de los titulares y suscriptores, así como las solicitudes de los procesos de registro, como evidencia de las transacciones realizadas y para efectos de auditoría.

La ER de DIGILINK genera reportes de los siguientes eventos:

- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.

El registro de auditoría de eventos debe registrar la hora, fecha e identificadores software/hardware.

9.4.2 FRECUENCIA DEL PROCESAMIENTO DEL REGISTRO

Los registros de auditoría deben ser procesados y revisados una vez al mes como mínimo con el fin de buscar actividades sospechosas o no habituales.

El procesamiento de los registros de auditoría debe incluir la verificación de que dichos registros no hayan sido manipulados.

9.4.3 PERIODO DE CONSERVACIÓN DEL REGISTRO DE AUDITORÍAS

Como mínimo los contratos de suscriptores y titulares, así como las solicitudes de los procesos de registro se conservarán por un periodo de diez (10) años.

9.4.4 PROTECCIÓN DEL REGISTRO DE AUDITORÍA

Las áreas de archivo donde se almacenan los contratos de los suscriptores y los titulares, así como las solicitudes de los procesos de registro estarán protegidos contra acceso no autorizado y los ingresos y salidas de personal serán registrados.

La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años.

9.4.5 COPIA DE SEGURIDAD DEL REGISTRO DE AUDITORÍA

Todas las solicitudes y contratos físicos serán generados con copia y los documentos electrónicos tendrán una copia por los Operadores de Registro. Las copias serán almacenadas en un lugar diferente como contingencia, protegidas contra acceso no autorizado por el Responsable de la ER de DIGILINK.

9.4.6 AUDITORÍA

Las auditorías internas se llevarán a cabo al menos una vez al año en la ER de DIGILINK.

Las evaluaciones técnicas del INDECOPI se llevarán llevarse a cabo una vez al año y cada vez que el INDECOPI lo requiera.

9.4.7 NOTIFICACIÓN AL TITULAR QUE CAUSA UN EVENTO

Las notificaciones automáticas dependen de los sistemas de la EC, para todos los eventos relacionados con el uso de los certificados por parte de un titular.

9.4.8 VALORACIÓN DE VULNERABILIDAD

Los sistemas de registro son administrados por cada EC, por lo que la protección perimetral de redes corresponde a la infraestructura de la EC.

9.5 ARCHIVO

9.5.1 PROTECCIÓN DEL ARCHIVO

El archivo físico está protegido con controles de acceso físico para impedir el acceso a personas no autorizadas. Los documentos se firman de manera manuscrita y digital respectivamente para prevenir cualquier modificación.

El ingreso y salida de documentos físicos y digitales se registra para impedir la pérdida o destrucción no autorizada.

Se considera la posibilidad de re-firmado de los archivos cuando los avances en las tecnologías generen potencialmente una posibilidad de afectación a los mismos o la generación de microformas según Decreto Legislativo 681.

Los datos archivados consignarán la fecha y hora, y la firma digital de la organización que genera dichos datos según la RFC 3161 (Time Stamping), o pueden ser protegidos de cualquier otra forma que pueda demostrar que los datos corresponden a la organización que los ha generado.

9.5.2 PROCEDIMIENTO PARA OBTENER Y VERIFICAR LA INFORMACIÓN DEL ARCHIVO

Mensualmente, la integridad del archivo debe ser verificada.

9.6 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

9.6.1 PLAN DE CONTINGENCIAS

La ER de DIGILINK mantiene un plan de contingencias que define acciones, recursos y personal para el restablecimiento y mantenimiento de las operaciones registro de los procesos de atención de solicitudes de emisión y revocación, en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

El plan asegura que los servicios de registro para los procesos de emisión y revocación, puedan ser asumidos dentro de un plazo máximo de 24 horas

Los planes son evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad o asesores, conjuntamente con la información respecto a las acciones correctivas que pudieran ser necesarias.

La recuperación de los sistemas administrados por la EC, incluyendo la disponibilidad de los sistemas de registro, que permiten la comunicación entre la ER y la EC, es responsabilidad de la EC. En esos casos, la ER de DIGILINK informará a los titulares y suscriptores el hecho mediante un mensaje de correo electrónico.

9.6.2 COMPROMISO DE LA CLAVE PRIVADA

En el caso de compromiso de la clave privada de un empleado que cumpla un rol de confianza, el certificado deberá ser revocado y se deberá solicitar la emisión de un nuevo certificado.

9.7 CONFIDENCIALIDAD DE INFORMACIÓN DE LA ER

9.7.1 INFORMACIÓN CONSIDERADA CONFIDENCIAL

La ER de DIGILINK mantiene de manera confidencial la siguiente información:

Material comercialmente reservado de la ER: planes de negocio y diseños e información de propiedad intelectual, e información que pudiera perjudicar la normal realización de sus operaciones.

- Información de los suscriptores y titulares, incluyendo contratos, información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores y titulares;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores y titulares.

9.7.2 INFORMACIÓN QUE PUEDE SER PUBLICADA

- Información respecto de la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión, la publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.
- Información de certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) y su estado.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confíen.

10 DERECHOS DE PROPIEDAD INTELECTUAL

Se prohíbe la reproducción, divulgación, comunicación pública y transformación de cualquiera de los elementos contenidos en el documento Política y Plan de Seguridad, que son propiedad exclusiva de DIGILINK sin su autorización expresa.

11 RESPONSABLE DE SEGURIDAD

El Responsable de Seguridad gestiona la implementación y vela por el cumplimiento del presente documento, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

12 CONFORMIDAD

Este documento ha sido aprobado por el Responsable de la ER 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.