POLÍTICA

Política y Plan de Seguridad en la Entidad de Registro

Norma(s) que Aplican	Referencia Normativa	Área Proceso	Código
INDECOPI - SID	3.2.11 Auditoría	PE: Perú	PE-PL-304-0001
INDECOPI - ER	3.2.8 Gestión de la seguridad		

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Alfredo Guardiola	26-12-2023	06-05-2026	06-05-2026	1	01-11-2023

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
Responsable de Seguridad	Responsable de Seguridad	Gerente General	Chief Technology Officer	Público

Firma electrónica avanzada
IGNACIO ENRIQUE VASQUEZ FLORES
2026.05.13 18:04:07 -0400

CONTENIDO

1 INTRODUCCIÓN

ECERTLA S.A.C., que en adelante llamaremos “ECERT", es una empresa peruana fundada en el año 2023 con el objetivo de brindar servicios basados en soluciones y firma digitales, firma electrónica e identidad digital en Latinoamérica.

Como parte de los servicios relacionados a la firma digital, ECERT es una Entidad de Registro, y un Prestador de Servicios de Valor Añadidos (SVA) acreditado ante el INDECOPI para su debido ejercicio.

En calidad de Entidad de Registro brinda los servicios de verificación de sus clientes, tanto para personas naturales, personas jurídicas, como paso previo a la emisión de certificados digitales.

ECERT brinda los servicios de firma digital a través de plataformas o de terceros que se interconectan al SID portal empresas. Entre los tipos de certificados digitales que se brindan para realizar las transacciones de firma se encuentran:

- Certificado Digital de Persona Natural para Persona Natural;
- Certificado Digital de Persona Jurídica para Representante Legal;
- Certificado Digital de Persona Jurídica de Pertenencia a Empresa (Conocido también como certificado de Atributo o certificado de Empleados o Certificados profesional colegiado);
- Certificado Digital de Persona Jurídica para Agente Automatizado.

Los certificados emitidos son provistos por la Entidad de Certificación de BIT4ID S.A.C., la cual forma parte de los Prestadores de Servicios de Certificación Digital acreditados por el INDECOPI.

En calidad de Prestador de Servicios de Valor Añadido – SVA como Sistema de Intermediación Digital “ECERT” provee la plataforma Portal Empresas, la cual mantiene las funcionalidades necesarias para regular y controlar la gestión de usuarios y el intercambio seguro de información, la gestión de las bolsas de firmas contratadas, así como la generación y protección de registros auditables de las transacciones realizadas. Para realizar esto de

manera más segura y automatizada, Portal Empresas se conecta a los servicios de registro, y automatiza los procesos de recojo de evidencias y validación de identidad, utilizando para ello, herramientas de biometría facial interconectada con el servicio de Consulta en Línea del RENIEC.

2 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas de seguridad que utiliza ECERT 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 ALCANCE

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

4 OBJETIVO DE LA ACREDITACIÓN

El alcance de la acreditación cubre los sistemas de registro que utiliza ECERT en la entrega de sus servicios, y que son proporcionados por la Entidad de Certificación BIT4ID.

5 DEFINICIONES Y ABREVIACIONES

- ER - Entidad de Registro: 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.
- EC- Entidad de Certificación: Entidad que presta servicios de emisión y revocación de certificados digitales en el marco de la regulación establecida por la IOFE.
- PSVA - Prestador de Servicios de Valor Añadido: Entidad que presta servicios que implican el uso de firma digital en el marco de la regulación establecida por la IOFE.

- SVA - Servicios de valor añadido: Servicios compuestos por tecnología y sistemas de gestión que utilizan certificados digitales garantizando la autenticidad e integridad de los mismos durante su aplicación.
- Política de servicios de valor añadido: Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
- INDECOPI: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual: Es la Autoridad Nacional de Protección del Consumidor que fomenta en el mercado mejores decisiones de consumo, garantizando la protección de la salud y seguridad de los consumidores. Además de promover mecanismos para la prevención y solución de conflictos a nivel nacional.
- CPS - Declaración de Prácticas de certificación: Declaración de los procedimientos y controles que adopta en cada etapa de los servicios y sistemas que brinda a sus clientes para la emisión de certificados digitales (BIT4ID).
- RPS - Declaración de Prácticas de registro: Procedimientos y controles que se adopta en cada etapa de los servicios y sistemas que se brinda a los clientes de acuerdo con lo establecido por INDECOPI.
- DPSVA - Declaración de Prácticas de Servicios de Valor Añadido: Procedimientos y controles que se adopta en cada etapa de los servicios y sistemas que se brinda a los clientes de acuerdo con lo establecido por INDECOPI.
- SID - Sistema de Intermediación Digital: Plataforma de gestión necesario para regular y controlar la gestión de usuarios y el intercambio seguro de información, así como la generación y protección de registros auditables de las transacciones realizadas.
- Titular: Entidad que requiere los servicios provistos por las EC y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
- Suscriptor: Entidad que requiere los servicios provistos por la SVA de ECERT 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 firmada digitalmente y que confía en la validez de las transacciones realizadas.
- IOFE- Infraestructura Oficial de Firma Electrónica: es el Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente (INDECOPI).
- SUNARP: Superintendencia Nacional de los Registros Públicos del Perú: Institución en Perú encargada de la administración y supervisión de los registros públicos, como el registro de propiedades, empresas y personas.
- SUNAT: Superintendencia Nacional de Aduanas y de Administración Tributaria: Entidad peruana encargada de la administración y control de los impuestos, aduanas y tributos en el país.
- RENIEC: Registro Nacional de Identificación y Estado Civil: Entidad encargada de organizar y mantener el registro único de identificación de las personas naturales e inscribir los hechos y actos relativos a su capacidad y estado civil.

6 PARTICIPANTES DE LA PKI

6.1 Entidad de registro ECERT

ECERT brinda los servicios de Entidad de Registro, 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 posterior registro.

6.2 Entidad de certificación BIT4ID

BIT4ID, en su papel de Entidad de Certificación acreditada, es una persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

6.3 Proveedor de servicios de certificación digital

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Registro de ECERT, 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 ECERT son provistos por ECERT CHILE.

6.4 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 ECERT.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por BIT4ID como prestadores de servicios de ECERT conforme a lo establecido en la Política de Certificación.

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 del 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 corresponderá a la persona jurídica. La atribución de responsabilidad del suscriptor, para tales efectos, corresponde a la misma persona jurídica.

6.5 Suscriptor

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

6.6 Solicitante

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo la CPS de BIT4ID.

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

6.7 Tercero que confía

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar las transacciones de firma digital y confiar en los certificados digitales emitidos por la Entidad de Certificación de BIT4ID. El Tercero que confía a su vez puede ser o no titular de un certificado.

6.8 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.

7 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La ER de ECERT 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 ECERT.

8 PLAN DE SEGURIDAD DE LA INFORMACIÓN

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

8.1 Seguridad Física

8.1.1 Ubicación y construcción del local

La ubicación y diseño de las instalaciones de la ER de ECERT 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, manteniendo vigente su acreditación ante el Instituto Nacional de Defensa Civil.

8.1.2 Seguridad física del personal y el equipamiento

A fin de proteger al personal y el equipamiento en las instalaciones de la ER de ECERT, 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

8.1.3 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. Se encuentra en ambientes separados de las áreas públicas de registro.
b. Solo ingresa personal autorizado
c. El ingreso y salida del personal debe ser registrado

d. 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
e. El ingreso y salida de documentos debe ser registrada
f. Debe estar cerrada bajo llave cuando no esté siendo usada
g. Cuando sea asignado un personal nuevo se deberán verificar sus antecedentes

Las operaciones de validación y registro pueden realizarse en las instalaciones de ECERT 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.

8.1.4 Protección contras la exposición al agua

Las instalaciones se encuentran protegidas contra exposición al agua, en particular las áreas de archivo se encuentran distantes de zonas de filtración de agua o humedad, ya sea en el techo o en las paredes colindantes.

8.1.5 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 ECERT.
b. Se cuenta con un extinguidor visible destinado a controlar el 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.

8.1.6 Archivo de material

Los archivos tanto electrónicos como de papel (contratos de suscriptores y solicitudes de los servicios de registro y el material distintivo (formatos membretados propios de la ER) se encuentran protegidos en las áreas de archivo en contenedores de protección contra fuegos y se sitúan en diversas dependencias para eliminar riesgos asociados a una única ubicación.

El acceso a estos contenedores está restringido a personal autorizado.

8.1.7 Seguridad de residuos

Los archivos tanto electrónicos como de papel (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.

8.1.8 Copia de seguridad externa

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 es guardada en un lugar de contingencia protegida por el responsable de la ER contra acceso no autorizado.

8.2 Gestión de Roles

8.2.1 Roles de Confianza

Los roles de confianza son definidos de la siguiente manera:

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

Estos roles son asignados formalmente por el responsable de la ER de ECERT.

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 y se cuenta con constancia por escrito del conocimiento de las mismas.

8.2.2 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.

8.2.3 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 ECERT.

8.2.4 Roles que requieren funciones por separado

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

8.3 Gestión del Personal

8.3.1 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 de conocimiento de toda esta información.

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

8.3.2 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.

8.3.3 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.

8.3.4 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 con sus funciones.
- Sus roles en relación con el Plan de Contingencias.

8.3.5 Frecuencia y requisitos de las 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.

8.3.6 Frecuencia y secuencia de la rotación en el trabajo

No se implementará rotación de los trabajadores.

8.3.7 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.

8.3.8 Requerimientos de los contratistas

El personal contratado para fines específicos dentro de las operaciones de la ER de ECERT, 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.

8.3.9 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 con sus funciones.
- Legislación aplicable a sus funciones.
- Documentación respecto a sus roles frente a plan de contingencia.

8.4 Procedimiento de Registros de Auditorías

8.4.1 Tipo de eventos registrados

Los sistemas de información sensible son provistos por la EC por lo que la ER de ECERT 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 ECERT 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.

8.4.2 Frecuencias 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.

8.4.3 Período 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.

8.4.4 Protección del registro de auditorías

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.

8.4.5 Copia de seguridad del registro de auditorías

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 ECERT.

8.4.6 Auditorías

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

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

8.4.7 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.

8.4.8 Valoración de vulnerabilidades

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

8.5 Archivo

8.5.1 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.

8.5.2 Procedimiento para obtener y verificar información del archivo

Mensualmente, la integridad del archivo debe ser verificada.

8.6 Recuperación Frente al Compromiso y Desastre

8.6.1 Plan de contingencias

La ER de ECERT 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 reasumidos 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 ECERT informará a los titulares y suscriptores el hecho mediante un mensaje de correo electrónico.

8.6.2 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 un nuevo certificado.

8.7 Confidencialidad de Información de la ER

8.7.1 Información considerada confidencial

La ER de ECERT 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.

8.7.2 Información que puede ser publicada

- Información respecto de la revocación de un certificado, sin revelar la causal que motivó dicha revocación, 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 confían.

9 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 ECERT sin su autorización expresa.

10 PERSONA DE CONTACTO

- Datos del responsable de Seguridad de la información:
- Nombre: Ignacio Vasquez
- Dirección Perú: Calle K n° 120, distrito de Miraflores, Provincia y Departamento de Lima, Perú.
- Dirección Chile: Monjitas 395, Piso 17, Santiago de Chile

- Correo electrónico: ivasquez@ecertla.com
- Página Web: https://www.ecertla.com/peru/

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 ECERT 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.

13 DE GOBIERNO

Respecto de esta Práctica las responsabilidades de los principales roles son las que se describen a continuación:

13.1 Gerente General

- Asegurar el establecimiento de esta Práctica, así como de su adecuación a los procesos de negocio.
- Revisar al menos una vez al año esta Práctica, revisión que debe ser aprobada por el mismo Gerente General.
- Informar al Directorio y los ejecutivos de la empresa, por sí mismo o por quién éste designe.

13.2 Comité de Sistema de Gestión

- Asegurar la implementación de esta Política, para lo cual le corresponde hacer seguimiento de la gestión de riesgos y oportunidades en cada sesión.
- Informar al Gerente General y a la plana ejecutiva de los riesgos asociados a esta Política y su implementación, así como resolver respecto de las medidas de mitigación.

13.3 Propietario del Proceso, del Riesgo o del Activo de la Información

El Propietario del Proceso, del Riesgo o del Activo de Información, debe:

- Asegurar la aplicación y seguimiento de Práctica y los documentos relacionados.
- Planificar sus procesos, objetivos e indicadores, de forma coherente con la presente Práctica, con la finalidad de minimizar los riesgos, gestionar las oportunidades, verificar el desempeño y optimizar los resultados de la organización en su conjunto.

14 REFERENCIAS NORMATIVAS

- Guía de Acreditación de Prestadores de Servicio de Valor Añadido, INDECOPI
- Ley de Firmas y Certificados Digitales - Ley 27269
- Decreto Supremo 052-2008
- Decreto Supremo 070-2011

15 PUBLICACIÓN

La Declaración de Prácticas de Registro - RPS de ECERT, la Política de seguridad, Política y Plan de Privacidad, y otra documentación relevante son publicados en la página web de ECERT:

- https://www.ecertla.com/peru/

Todas las modificaciones relevantes 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 ECERT antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

16 SENSIBILIZACIÓN Y CAPACITACIÓN

- El Gerente General de ECERT reconoce como tareas prioritarias la sensibilización, capacitación y entrenamiento del personal, en materias de las indicadas en la presente Política.
- Los ejecutivos de ECERT deben crear mecanismos para que esta política, las normas y sus procedimientos, sean conocidos y considerados permanentemente por todos los integrantes de la organización, asegurándose que los colaboradores asumen y comprenden sus responsabilidades. Estas acciones estarán contenidas en las actividades de capacitación anual al personal de ECERT.
- Los ejecutivos de ECERT deben asegurar que todos los colaboradores cuenten con una inducción y sean capacitados en materias de esta política, manteniendo un canal de comunicación formal para informar a toda la organización respecto a los avances, logros y novedades en la materia, con el objetivo de crear una cultura de calidad dentro de la Organización.

17 INCUMPLIMIENTO

Ante la ocurrencia de algún incumplimiento a las medidas orientadas a resguardar la presente política, el usuario que lo detecte debe informar a la brevedad a su jefatura directa y al Comité Sistema de Gestión, quienes analizarán el incumplimiento y deben gestionar las medidas necesarias para minimizar los potenciales daños a la empresa y lograr el cumplimiento integral de esta política, evitando que se reiteren situaciones similares.

Todo colaborador tiene la obligación de notificar cualquier actividad o situación que afecte o pueda afectar lo dispuesto en la presente Política. Dicha notificación se debe registrar conforme al Procedimiento Gestión de Incidentes (SGI-P-104-0008).

Los incumplimientos graves, es decir, aquellos que afecten a los clientes y/o que manifiesten como quejas del cliente o de INDECOPI deben ser informados al Gerente General y al Directorio de ECERT.

18 SANCIONES

a) Al colaborador que contravenga lo indicado en esta Política y/o los documentos relacionados a la misma, se le debe aplicar lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad (SGI-F-301-0019), en cuanto a sanciones y multas.

b) Con relación al personal externo y/o proveedores que no cumplan con lo indicado en esta Práctica, dependiendo del tipo de incumplimiento se debe amonestar o rescindir el contrato.

19 CONTROL DE VERSIONES

Control de versiones		
Versión	**Fecha**	**Descripción**
1	07-04-2023	• Elaboración de documento inicial.
2	11-01-2024	• Se elimina la palabra "enrolados", reemplazándola por la palabra "persona natural o jurídica". • Se agrega dirección y número de teléfono en Perú. • Se homologa el certificado profesional colegiado como persona jurídica, tal como lo tiene BIT4ID.
0	29-10-2025	• Se crea documento en nuevo gestor documental IS Contacto
1	07-04-2026	• 5. Se actualizan las definiciones. • 10. y 15 Se actualiza página web.

Fin del documento

Una copia impresa de este documento es válida sólo por el día en que se imprimió.

Cualquier modificación y/o copia total o parcial, por cualquier medio, queda totalmente PROHIBIDA.