GRAMD.COM

ENTIDAD DE REGISTRO O VERIFICACION

DECLARACION DE PRÁCTICAS Y POLÍTICAS DE REGISTRO DE GRAMD PERUANA S.A.C. VERSIÓN 1.1

Elaborado y aprobado por:	Gerencia de Registro Digital de la ER GRAMD
Dirigido a:	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)
Tipo de Documento:	Declaración de Prácticas y Políticas de Registro
Versión:	1.1
Fecha de elaboración:	04/12/2019

CONTROL DE CAMBIOS

Version	Motivo de Version	Descripcion del cambio	Autor del Cambio	Fecha del Cambio
1.0	Original	Creacion del documento	Gerencia de Registro Digital de la ER GRAMD	27/11/2017
1.1	Actualizacion	Todo	Gerencia de Registro Digital de la ER GRAMD	04/12/19

ÍNDICE

1. INTRODUCCIÓN

Gramd Peruana S.A.C. (en adelante GRAMD) es una empresa privada reconocida en el mercado nacional que brinda el servicio de Identidad Digital, Comunicaciones Seguras, Venta Licencias de Certificados Digitales destinado a organizaciones, software, servidores y personas juridícas como representantes legales de empresas, de ser el caso, con el soporte de BIT4ID SAC quien es una Entidad de Certificación reconocida por el Indecopi.

En virtud de un Convenio de Prestación de Servicios, se regulan las condiciones y modalidades de la prestación de servicios por parte de:

- **BIT4ID S.A.C.** (Prestadora de Servicios de Certificación Digital, debidamente acreditada por el INDECOPI), que es una sociedad peruana que pertenece a la sociedad BIT4ID GROUP. (en adelante BIT4ID), y
- **GRAMD PERUANA S.A.C.**, que presta los servicios de registro o verificación, de personas jurídicas, en la demarcación de Lima y otras ciudades del Perú, conforme a lo establecido en la Declaración de Prácticas de Certificación, las Políticas de Certificación de BIT4ID S.A.C., sus procedimientos y documentos técnicos, así como la Ley N° 27269, y su Reglamento.

Entre los tipos de certificados digitales que GRAMD provee se encuentran: Certificados digitales para persona jurídica.

2. OBJETIVO

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

3. DEFINICIONES Y ABREVIACIONES

Entidad de Certificación (EC):	Persona jurídica o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.
Entidad de Registro o Verificación (ER):	Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, comprobación de estos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
Declaración de Prácticas de Certificación (CPS):	Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual se define sus Prácticas de Certificación.
Declaración de Prácticas de Registro o Verificación (RPS):	Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación.
Identificador de Objeto (OID):	Es una cadena de números, formalmente definida usando el estándar ASN.1 (ITU-T Rec. X.660 ISO/IEC 9834 series), que identifica de forma única a un objeto. En el caso de la certificación digital, los OIDs se utilizan para identificar a los distintos objetos en los que ésta se enmarca (por ejemplo, componentes de los Nombres Diferenciados, CPS, etc.).
Infraestructura Oficial de Firma Electrónica (IOFE)	Sistema confiable, acreditado, regulado y supervisado por el INDECOPI, provisto de instrumentos legales y técnicos que

	permiten generar firmas electrónicas y proporcionar diversos niveles de seguridad respecto a: 1) la integridad de los mensajes de datos y documentos electrónicos; 2) la identidad de su autor, lo que es regulado conforme a la Ley. El sistema incluye la generación de firmas electrónicas, en las que participan entidades de certificación y entidades de registro o verificación acreditadas ante el INDECOPI incluyendo a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), las Entidades de Certificación para el Estado Peruano (ECEP) y las Entidades de Registro o Verificación para el Estado Peruano (EREP).
Operador de Registro de Datos:	Persona responsable de representar a GRAMD en calidad de ER de BIT4ID en las actividades de recepción, validación y procesamiento de solicitudes.
Prácticas de Registro o Verificación:	Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una ER.
Registro Nacional de Identificación y Estado Civil (RENIEC):	Es un organismo autónomo del Estado Peruano, encargado de la identificación de los peruanos, otorgando el Documento Nacional de Identidad (DNI), registrando hechos vitales como nacimientos, matrimonios, defunciones, divorcios y otros que modifican el estado civil. Durante los procesos electorales, proporciona el Padrón Electoral que se utilizará en las elecciones.
Superintendencia Nacional de los Registros Públicos (SUNARP):	Es un organismo autónomo del Estado Peruano, tiene como función la planificación y organización de las inscripciones y publicidades de actos y contratos en los registros de los derechos y titularidades.

4. DIFERENCIACIÓN DE LOS PARTICIPANTES

4.1 ENTIDAD DE CERTIFICACIÓN - BIT4ID

La empresa BIT4ID SAC, en su calidad de Entidad de Certificación acreditada, presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios vinculados a la certificación digital. Los servicios ofrecidos por BIT4ID comprenden aquellos orientados a la gestión del ciclo de vida de los certificados digitales, de acuerdo a lo especificado en su correspondiente Declaración de Prácticas de Certificación (RPS).

4.2 ENTIDAD DE REGISTRO – ER GRAMD

GRAMD, en su calidad de Entidad de Registro, se encarga de validar la información suministrada por un solicitante de certificado digital; mediante la comprobación de sus datos, identificación y autenticación, para su posterior registro. Dentro de estas funciones se debe tener presente la gestión interna ante BIT4ID a fin de que aquella genere o cancele el certificado digital emitido a nombre de un solicitante de certificado digital.

4.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL (BIT4ID S.A.C.[1])

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Registro – ER GRAMD, cuando ésta entidad así lo requiere y garantizan la continuidad del servicio a los suscriptores y/o titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

Los servicios de certificación digital que ofrece GRAMD son provistos en un contrato de tercerización por la Entidad de Certificación de BIT4ID.

[1] Prestador de Servicios de Confianza (TSP)

4.4 TITULAR DE CERTIFICADO DIGITAL

Un titular de certificado digital, es aquella persona natural que representa una organización y que se conoce como persona jurídica, dicha persona se le atribuye un certificado digital proveniente de una Entidad Certificadora "BIT4ID" que previante paso por un proceso de validacion de identidad a cargo de una Entidad de Registro "GRAMD".

4.5 SUSCRIPTOR DE CERTIFICADO DIGITAL

Un suscriptor de certificado digital, es aquella persona natural responsable de la generación y 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 sea una persona natural, sobre la misma 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. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

4.6 SOLICITANTE DE CERTIFICADO DIGITAL

Se entenderá por Solicitante, aquella persona natural que representa una organización y que se conoce como persona jurídica, la persona solicita un certificado digital aceptando previamente lo establecido en la CPS de Entidad Certificadora "BIT4ID" como tambien la RPS de la Entidad de Registro "GRAMD".

4.7 TERCERO QUE CONFÍA O TERCER USUARIO

Se considerará como Tercero que Confía a personas naturales y/o jurídicas que confían en el contenido y la aplicación de un certificado digital, los terceros que confían pueden ser todas aquellas personas naturales y jurídicas que requieren evaluar la validez de un certificado para proceder con sus respectivas transacciones electrónicas, incluyendo entidades de otras infraestructuras además de la IOFE.

4.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR DE CERTIFICADO DIGITAL

Se considerará como Entidad a la cual se encuentra vinculado el Titular de un Certificado Digital, a la persona jurídica u organización que mantiene un vínculo con el Titular de un certificado digital.

5 RESPONSABILIDAD LEGAL

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de tales usos quedan a cargo del "El Suscriptor"/Titular. En ningún caso podráÍ "El Suscriptor" ni los terceros perjudicados reclamar a la EC y/o "GRAMD" compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados digitales.

6 USO DEL CERTIFICADO DIGITAL

6.1 USOS ADECUADOS DEL CERTIFICADO DIGITAL

El uso de los certificados digitales, está determinado en la CPS de BIT4ID.

En términos generales, se admiten los certificados para los siguientes usos:

- **Identificación del Titular**: El Titular del certificado puede autenticar, frente a otro individuo, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública.

- **Identidad del documento firmado**: La utilización del certificado otorga plena seguridad de que el documento firmado es integro. Vale decir, que no fue alterado o modificado, después de que el Titular lo firmó.
- **No repudio:** Con el uso de este certificado, se garantiza además, que el individuo que firma el documento no podrá repudiarlo. Vale decir, que el Titular que firmó este documento no podrá negar su autoría, o la integridad del mismo.

Cada política de certificación está identificada por un único identificador de objeto (OID) que además incluye el número de versión.

- **Los certificados que emitimos :**
  - Certificado de Perteneciente a una persona juridica.
  - Certificado para Facturacion electronica.

6.2 USOS PROHIBIDOS / NO AUTORIZADOS, Y EXONERACIÓN DE RESPONSABILIDAD

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos en cada caso, y que vienen descritos en las políticas de certificación correspondientes (CPS de BIT4ID).

Se consideran indebidos aquellos usos que no están definidos en la CPS de BIT4ID y en consecuencia para efectos legales, tanto BIT4ID como GRAMD, quedan exonerados de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de certificados digitales.

7 INFORMACIÓN DE CONTACTOS

Datos de la Entidad de Certificación y Prestadora de Servicios:

Nombre:	BIT4ID S.A.C.
Dirección:	Av. Antonio Miroquesada, Nº 360 - Oficina 04-112 – Distrito de Magdalena del Mar, Provincia y Departamento de Lima.
Teléfono:	01-242 9994
Correo electrónico:	jga@bit4id.com
Página Web:	https://www.bit4id.com

Datos de la Entidad de Registro o Verificación:

Nombre:	GRAMD PERUANA S.A.C.
Dirección:	Av. República de Panamá N° 3418, Of. 301, Distrito de San Isidro, Provincia y Departamento de Lima.
Teléfono:	01-7390900 / 0800-7-1500
Correo electrónico:	countryoffice-pe@gramd.com
Página Web:	https://www.gramd.com.pe/

8 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE RPS

Los documentos relacionados con la presente RPS, y demás documentos normativos son administrados por GRAMD, y verificados periódicamente por BIT4ID, cada nueva versión será presentada al INDECOPI, y luego de su aprobación, será debidamente publicada en la siguiente dirección url: https://www.gramd.com.pe/

Para mayor detalle al respecto se podrá consultar a la siguiente persona:

- Razon Social : Gramd Peruana Sac
- Ruc: 20535708798
- Nombre: Ing. Roberto Augusto Castañeda Chávez/ Rosa Cecilia Santos Vasquez
- Cargo: Responsable de la Entidad de Registro o Verificación – ER GRAMD.
- Dirección de correo electrónico: acastaneda@gramd.com / cecilia.santos@gramd.com

9 RESPONSABILIDADES DE LOS TITULARES Y/O SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por GRAMD son responsables de revisar el presente documento, la CPS y las Políticas de Certificación de BIT4ID, a fin de tener conocimiento de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

10 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS Y OTROS DOCUMENTOS

La Declaración de Prácticas de Registro (RPS), así como la Política de Seguridad, Política y Plan de Privacidad de la Entidad de Registro o Verificación - ER GRAMD, y otra documentación relevante son publicadas en la siguiente dirección:
https://www.gramd.com.pe/

Asimismo, la Declaración de Prácticas y Políticas de Certificación de la Entidad de Certificación –BIT4ID y otra documentación relevante son publicadas en la siguiente dirección:
http://www.bit4id.com

Todas las modificaciones relevantes en la documentación de GRAMD, serán comunicadas a INDECOPI y deben ser publicadas tan pronto como razonablemente sea posible, debiendo tener cuidado de cumplir con los requisitos que fueren necesarios para la aprobación de dichas modificaciones y las nuevas versiones del documento serán publicadas en el sitio web descrito.

El presente documento es firmado por el Responsable de la ER GRAMD antes de ser publicado, comprometiéndose dicho responsable de controlar las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

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

11 IDENTIFICACIÓN Y AUTENTICACIÓN

11.1 NOMBRES

11.1.1 TIPOS DE NOMBRES

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.2 PSEUDÓNIMOS

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.3 REGLAS UTILIZADAS PARA INTERPRETAR VARIOS FORMATOS DE NOMBRES

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.4 UNICIDAD DE LOS NOMBRES

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.5 RECONOCIMIENTO, AUTENTICACIÓN Y FUNCIÓN DE LAS MARCAS REGISTRADAS

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.6 MÉTODOS DE PRUEBA DE LA POSESIÓN DE LA CLAVE PRIVADA

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.7 AUTENTICACIÓN DE LA IDENTIDAD DE UN INDIVIDUO, LA ENTIDAD Y SU VINCULACIÓN

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

12 SOLICITUD DE EMISIÓN DE CERTIFICADOS DIGITALES

Los procedimientos, requisitos de solicitud y responsabilidades en el uso de los certificados, pueden variar de acuerdo a lo establecido en la Política de Certificación y Declaración de Prácticas de BIT4ID, los mismos que son publicados en la siguiente dirección web:
http://www.BIT4ID.com

El ciclo de vida de un certificado digital no debe exceder de Tres (03) años conforme lo estipulado por la IOFE.

12.1 SOLICITUD DE CERTIFICADOS DE PERSONA JURÍDICA

12.1.1 SERVICIOS BRINDADOS POR GRAMD

La ER GRAMD brinda los siguientes servicios a personas jurídicas:

- Atención de solicitudes de emisión, revocación de certificados de atributos para personas jurídicas públicas o privadas, constituidas en el Perú, para ser usados por representantes legales, funcionarios y personal específico.
- Atención de solicitudes de emisión, revocación de certificados de atributos para personas jurídicas públicas o privadas, constituidas en el extranjero, para ser usados por representantes legales, funcionarios y personal específico.
- Atención de solicitudes de emisión, revocación de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el Perú, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
- Atención de solicitudes de emisión, revocación de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el extranjero, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados brindados por la ER GRAMD corresponden a BIT4ID y dicha información se encuentra publicada en la siguiente dirección:
http://www.bit4id.com

12.1.2 PERSONAS AUTORIZADAS PARA REALIZAR LA SOLICITUD

La solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de Datos de la ER GRAMD, la documentación legal que acredite sus facultades como representante.

12.1.3 FORMAS DE ATENCIÓN

La solicitud deberá ser realizada mediante un contrato de adquisición de certificado digital ("Contrato de Venta de Licencia(s) de Certificado Digital y Suscriptor", en adelante "El Contrato"), que puede ser celebrado de las siguientes formas:

- ✓ De manera presencial en las instalaciones de la ER GRAMD.
- ✓ De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER GRAMD.
- ✓ De efectuarse de manera remota, deberá suscribirse electrónicamente el contrato de adquisición de certificado digital, con la firma digital del representante asignado por la persona jurídica.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro de Datos en la ER GRAMD utilizando un certificado digital contenido en un dispositivo criptográfico seguro reconocido por el INDECOPI.

12.1.4 SOLICITUD DE CERTIFICADOS DE ATRIBUTOS

En el caso de certificados de persona jurídica se considera como titular del certificado y los empleados vienen a ser los suscriptores.
El solicitante deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado, diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el representante legal o una persona asignada por él.

Un mismo suscriptor podrá efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera.

12.1.5 RECONOCIMIENTO, AUTENTICACIÓN Y FUNCIÓN DE LAS MARCAS REGISTRADAS

Los solicitantes de certificados de personas jurídicas no deben incluir nombres en las solicitudes que puedan suponer infracción de derechos de terceros. La ER GRAMD podrá rechazar una solicitud de certificado a causa de conflicto de nombres, en vista que no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

A través de la verificación de la documentación e información que figura en Registros Públicos o la embajada correspondiente, la ER GRAMD determinará la validez del nombre de la persona jurídica. Sin embargo, no le corresponde a ésta última, determinar si a un solicitante le asiste algún tipo de derecho sobre el nombre que figura en una solicitud de certificado, asimismo, no es competencia de la ER GRAMD, la resolución de cualquier disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

12.1.6 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA JURÍDICA

El solicitante deberá acreditar la existencia de la persona jurídica y su vigencia mediante los documentos públicos expedidos por los Registros Públicos, o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. La información brindada por los

solicitantes será validada a través de la consulta a la Superintendencia Nacional de los Registros Públicos (SUNARP).

En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

12.1.7 CONTRATO DE SUSCRIPTOR

El representante legal de la persona jurídica o una persona asignada por él, debidamente acreditada (a través de una declaración jurada), deberá firmar "El Contrato".

Mediante este documento, el titular y/o suscriptor deberá declarar tener pleno conocimiento de los términos y condiciones aplicables a los certificados.

La celebración de dicho documento, deberá realizarse antes de la emisión de los certificados.

12.1.8 VERIFICACIÓN DEL SUSCRIPTOR

Los solicitantes de un certificado digital, deben ser validados en cualquiera de las siguientes formas:

- ✓ De manera presencial en las instalaciones de la ER GRAMD.
- ✓ De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER GRAMD.

A fin de verificar sus identidades debe cumplir los requerimientos establecidos en el presente documento respecto de la autenticación de personas naturales.

Cuando una persona solicite la emisión de un certificado digital que sirva para acreditar el ejercicio de un cargo en concreto, la ER GRAMD requerirá a este solicitante la documentación legal que evidencie su cargo, incluyendo las facultades para realizar dicho proceso.

Asimismo, está en la obligación de presentar el original de su propio documento oficial de identidad.

La solicitud deberá ser realizada mediante "El Contrato" que puede ser celebrado de las siguientes formas:

- ✓ De manera presencial en las instalaciones de la ER GRAMD.
- ✓ De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER GRAMD.
- ✓ De efectuarse de manera remota, deberá suscribirse electrónicamente el contrato de adquisición de certificado digital, con la firma digital del representante asignado por la persona jurídica.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro de Datos de la ER GRAMD utilizando un certificado digital reconocido por el INDECOPI.

A través de dicho acuerdo, el suscriptor declara conocer los términos y condiciones aplicables a los certificados digitales. Su celebración deberá realizarse antes de la emisión del certificado digital.

13 PROCESAMIENTO DE LA SOLICITUD

13.1 RECHAZO DE LA SOLICITUD DE EMISION DE UN CERTIFICADO

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

- ✓ En el caso de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los documentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

Así como en el supuesto que, el resultado de la validación realizada por la ER fuese negativo, conforme a lo establecido en este documento.

GRAMD, en su calidad de Entidad de Registro o Verificación, tiene la facultad de establecer en su RPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, asumiendo las consecuencias que podría acarrear tal decisión.

13.2 APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

Para aprobar una solicitud, la ER GRAMD realizará lo siguiente:

- Comunicar a la BIT4ID SAC su aprobación para le emisión del certificado, a través de un sistema web con control de acceso, y la protección de un canal SSL. Este sistema será brindado por la Entidad de Certificación BIT4ID SAC.
- Será necesaria la firma del "El Contrato".

13.3 REGISTRO DE DOCUMENTOS

La ER GRAMD registrará y archivará la solicitud, "El Contrato", y demás documentación legal presentada por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

13.4 MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor.

Los módulos criptográficos distribuidos y proporcionados por BIT4ID SAC cuentan con la certificación FIPS 140-2 o Common Criteria o equivalente.

Es preciso señalar, que únicamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Luego, se realizará la petición segura del certificado a la respectiva EC en el formato PKCS#10 (CSR), realizando con ello la prueba de la posesión de la clave privada.

13.5 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Cuando la información ha sido validada y aprobada por un Operador de Registro de Datos de la ER GRAMD, ésta enviará a BIT4ID SAC la autorización de la emisión del certificado, inmediatamente.

El máximo tiempo de respuesta para la emisión del certificado será de 03 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo, en la cuenta bancaria de GRAMD, por el servicio brindado.

13.6 EMISIÓN DEL CERTIFICADO

La emisión del certificado será realizada virtualmente, vale decir a través del correo electrónico proporcionado por el suscriptor en su solicitud.

13.7 APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

A fin de que una solicitud sea aprobada, la ER GRAMD realizará lo siguiente:

- ✓ Comunicar a la EC BIT4ID SAC su aprobación para la emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por BIT4ID SAC.
- ✓ Se requerirá la firma del contrato del suscriptor.

13.8 REGISTRO DE DOCUMENTOS

La ER GRAMD tiene la obligación de registrar y archivar la solicitud, el "Acuerdo del Suscriptor", y los documentos de sustento presentados por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

13.9 MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA

Como parte de la Política de Seguridad de GRAMD, la generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor.

Los módulos criptográficos distribuidos y proporcionados por BIT4ID SAC cuentan con la certificación FIPS 140-2 o Common Criteria o equivalente.

Sin embargo, solamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Luego, se realizará la petición segura del certificado a BIT4ID SAC en el formato PKCS#10 (CSR), realizando con ello la prueba de la posesión de la clave privada.

13.10 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Cuando la información ha sido validada y aprobada por un Operador de Registro de Datos de la ER GRAMD, ésta enviará a la respectiva EC la autorización de la emisión del certificado, inmediatamente.

El máximo tiempo de respuesta para la emisión del certificado será de 03 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo, en la cuenta bancaria de GRAMD, por el servicio brindado.

14 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

14.1 SITUACIONES PARA REALIZAR LA SOLICITUD

A efectos de una solicitud de revocación, el titular y suscriptor de un certificado digital, bajo su responsabilidad, pueden realizar la mencionada solicitud, al tener conocimiento de la ocurrencia de cualquiera de las siguientes situaciones:

- ✓ Por exposición, puesta en peligro o uso indebido de la clave privada.
- ✓ Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- ✓ Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica privada o pública.
- ✓ Cuando la información contenida en el certificado ya no resulte correcta.
- ✓ Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- ✓ Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE, a través de lo estipulado en el "Acuerdo del Suscriptor".
- ✓ Por decisión de la legislación respectiva.
- ✓ Por resolución administrativa o judicial que lo ordene.

14.2 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

14.2.1 SERVICIOS BRINDADOS POR GRAMD

La ER GRAMD brinda los siguientes servicios a personas jurídicas y naturales:

- Atención de solicitudes de revocación de certificados para personas naturales de nacionalidad peruana.
- Atención de solicitudes de revocación de certificados de atributos para personas naturales de nacionalidad extranjera.
- Atención de solicitudes de revocación de certificados de atributos para personas jurídicas públicas o privadas, constituidas en el Perú, para ser usados por representantes legales, funcionarios y personal específico.
- Atención de solicitudes de revocación de certificados de atributos para personas jurídicas privadas o públicas, constituidas en el extranjero.
- Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el Perú, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
- Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el extranjero, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados digitales provienen de la Entidad de Certificación BIT4ID SAC.

14.2.2 PERSONAS AUTORIZADAS PARA REALIZAR LA SOLICITUD

Conforme a lo establecido por la Ley, el tipo de personas que pueden solicitar la revocación de un certificado son las siguientes:

- ✓ El titular del certificado.
- ✓ El suscriptor del certificado.
- ✓ La EC o ER que emitió el certificado.
- ✓ Un Juez que conforme a Ley decida revocar el certificado.

En el supuesto que como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER GRAMD, será suficiente con presentar su solicitud firmada de forma

manuscrita (previa presentación de su documento oficial de identidad) o con firma digital al Operador de Registro de Datos.

14.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS SOLICITANTES

En el supuesto que la solicitud sea presencial:

- ✓ Los suscriptores deben demostrar su documento oficial de identidad.
- ✓ El representante legal de la persona jurídica debe presentar la documentación que acredite su representación.
- ✓ Los terceros (diferentes de la EC, el suscriptor y el titular), deberán presentar pruebas fehacientes a la ER GRAMD, del uso indebido del certificado, conforme a lo estipulado por la Ley, junto a la orden judicial respectiva.

14.2.4 FORMAS DE ATENCIÓN

La solicitud deberá ser realizada por los titulares y suscriptores de las siguientes formas:

- ✓ De manera presencial en las instalaciones de la ER GRAMD.
- ✓ De manera presencial en alguna locación señalada por estos, en presencia de un representante de la ER GRAMD.
- ✓ De efectuarse de manera remota, mediante documento o correo electrónico firmado digitalmente por el representante legal de la persona jurídica o por el suscriptor. El certificado digital a emplear no debe ser el que se desea revocar.
- ✓ De manera remota en una comunicación directa con la EC BIT4ID, mediante un control de acceso o contraseña brindados al suscriptor en el momento de la solicitud de emisión del certificado.

Los demás actores, diferentes a los suscriptores y titulares, deberán realizar la solicitud de manera presencial en las instalaciones de la ER GRAMD.

La EC BIT4ID no requerirá efectuar la solicitud a la ER GRAMD en los casos que el suscriptor haya infringido las obligaciones descritas en su contrato, o en caso sea necesario por revocación del certificado de la EC. Una EC puede revocar los certificados que ha emitido, siempre y cuando los motivos de revocación estén determinados en su CPS y se encuentren conforme a la Ley.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro de Datos de la ER GRAMD, utilizando un certificado digital reconocido por el INDECOPI.

15 PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

15.1 RECHAZO DE LA SOLICITUD DE REVOCACIÓN

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las formas de solicitud o que el solicitante no se encuentre debidamente autorizado conforme a lo descrito en el presente documento.

Adicionalmente, la solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

- ✓ Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los documentos legales respectivos, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en el presente documento.

Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, las cuales serán asumidas por la ER GAMD.

15.2 APROBACIÓN DE LA SOLICITUD DE REVOCACIÓN

Para que la ER GRAMD apruebe una solicitud de revocación, se deberá cumplir con lo siguiente:

- ✓ Comunicar a la EC BIT4ID su aprobación para la revocación del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por BIT4ID.
- ✓ Una copia de dicha solicitud firmada será enviada a la EC BIT4ID o almacenada por la ER GRAMD, teniendo en cuenta su vinculación.

15.3 REGISTRO DE DOCUMENTOS

La ER GRAMD registrará y archivará la solicitud y los documentos de sustento presentados por el solicitante dejando constancia de la persona que efectúa la solicitud, la relación que tiene ésta con el titular, las razones de la solicitud, las acciones tomadas para la verificación de la veracidad de la solicitud, fecha y hora de la revocación y de la notificación de la misma BIT4ID, sus suscriptores y los terceros que confían.

En cumplimiento de la Política de Seguridad de la ER GRAMD, toda la documentación será protegida contra acceso no autorizado y destrucción.

En caso que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

15.4 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER GRAMD COMUNICARÁ a BIT4ID, por vía electrónica la revocación del certificado de manera inmediata.

El máximo tiempo de respuesta para la revocación del certificado dependerá de lo establecido en la CP y CPS de la EC.

15.5 REVOCACIÓN DEL CERTIFICADO

La revocación del certificado será comunicada al suscriptor y titular mediante el correo electrónico del suscriptor, registrado en su solicitud.

16 CONTROLES DE LAS INSTALACIONES, DE LA GESTIÓN Y CONTROLES OPERACIONALES

De acuerdo a los lineamientos establecidos por el INDECOPI, la presente sección describe de forma genérica las medidas que ha implementado GRAMD, en su calidad de ER, con la finalidad de garantizar los requerimientos que en materia de seguridad, sostienen los servicios de registro o verificación de datos. El

detalle de las medidas de seguridad adoptadas para proteger los activos críticos que sostienen los mencionados servicios, están establecidas en la Política de Seguridad de la ER GRAMD.

En las sub secciones siguientes se reseña las medidas adoptadas más relevantes:

16.1 CONTROLES FISICOS

En esta sub sección se describen los controles que se aplicarán a los recursos físicos que comprenden las instalaciones de la ER GRAMD, lo cual incluye la infraestructura física y su acondicionamiento, el acceso físico a ésta, así como su protección y seguridad.

16.1.1 UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

Las instalaciones de la ER GRAMD se encuentran resguardadas físicamente con las medidas de protección necesarias para salvaguardar el desarrollo de las actividades de prestación de servicios como ER.

16.1.2 ACCESO FÍSICO

En los ambientes donde se desarrollan las actividades y operaciones de la ER GRAMD se han establecido perímetros de seguridad e implementado controles de acceso, de modo que solo el personal autorizado y acreditado puede acceder a los mismos. Estos controles de acceso aplican para el personal de la ER, visitantes o proveedores.

16.1.3 ENERGÍA Y AIRE ACONDICIONADO

Las instalaciones donde se encuentran los servidores que brindan soporte a las operaciones de la ER GRAMD cuenta con un equipo de apoyo que suministra energía temporal en caso de caídas del sistema eléctrico principal, protegiendo a los equipos frente a fluctuaciones eléctricas que los pudieran dañar.

El ambiente donde se encuentran situados los equipos de tratamiento y almacenamiento de información, dispone de un sistema de aire acondicionado que dota al entorno de operaciones de una humedad y temperatura adecuada y constante consiguiendo la protección de los equipos y un óptimo funcionamiento de los mismos.

El equipo de apoyo que suministra energía eléctrica, así como el equipo de aire acondicionado, cuenta con mantenimientos preventivos periódicos a fin de garantizar su correcto funcionamiento.

16.1.4 EXPOSICIÓN AL AGUA

La ER GRAMD ha tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado, disponiendo de controles de humedad.

16.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

La ER GRAMD ha adoptado controles que permiten prevenir y extinguir incendios u otras exposiciones dañinas como llamas o humo en todas sus instalaciones; en tal sentido, los ambientes de la ER GRAMD, cuentan con detectores de humo, así como extintores que permiten detectar y sofocar un eventual siniestro respectivamente.

16.1.6 ARCHIVO DE MATERIAL

La ER GRAMD ha establecido lineamientos para la clasificación de la información, así como su tratamiento y condiciones de almacenamiento de acuerdo a la criticidad de esa información y en concordancia con el proceso de certificación digital, las leyes y regulaciones vigentes.

Toda información contenida en formato papel, relacionada con una solicitud de un certificado digital, se almacenará en las instalaciones de la ER GRAMD, las cuales cuentan con adecuados controles de acceso físico para limitar el acceso solo a personal autorizado, así como proteger dicha información de algún deterioro o daño accidental (ejemplo: agua, incendio, etc.).

Respecto a la información que ingresa en formato electrónico, ésta es almacenada en los equipos (servidores) ubicados en las instalaciones de la ER GRAMD, en un ambiente que cuenta con controles de acceso físico y lógico para limitar el acceso sólo al personal autorizado. Así también, se protege dicha información de algún daño o destrucción deliberada o accidental (ejemplo: robo, alteración no autorizada, agua, incendio y electromagnetismo).

16.1.7 GESTIÓN DE RESIDUOS

La información contenida en formato papel, así como en soportes magnéticos u ópticos, antes de ser eliminada, es destruida tanto física como lógicamente a fin de evitar la posibilidad de recuperación de dicha información desde los formatos que la contuvieren.

Este procedimiento es efectuado de acuerdo a la legislación vigente y las políticas y prácticas de la ER GRAMD.

Se almacenaran los registros y/o documentos por un mínimo de 10 años.

16.1.8 COPIA DE SEGURIDAD EXTERNA

Las copias de seguridad de la información correspondiente a la ER GRAMD, son almacenadas en una plataforma virtual de propiedad de GRAMD, denominada IDENTITY PKI.

16.2 CONTROLES PROCESALES

16.2.1 ROLES DE CONFIANZA

La ER GRAMD ha definido y comunicado las funciones a su personal, así mismo se ha determinado los roles de confianza y los procedimientos de control adecuados para el cumplimiento de las obligaciones establecidas en el presente documento. Estos roles son los siguientes:

1. **Gerente de Registro Digital de la ER GRAMD:**

    1. Es el encargado de supervisar las labores de todo el personal interno, y asignar roles y funciones.
    2. Es el responsable de coordinar con el Analista de Control Externo de BIT4ID, el desarrollo de las auditorías internas a intervalos planificados o cuando ocurran cambios significativos en la puesta en marcha de la seguridad.
    3. Implementará todas las políticas establecidas en la Declaración de Prácticas y Políticas de Registro, Política de Seguridad, Política de Privacidad y Plan de Privacidad. Así como, asignar las distintas responsabilidades del personal interno, respecto a la seguridad de la información.
    4. Es el encargado de aprobar la Política de Seguridad, elaborada en conjunto por el Administrador y Oficial de Seguridad de Información de la ER

GRAMD, y por el Supervisor y Coordinador de Información de la ER GRAMD.

2. Administrador y Oficial de Seguridad de Información de la ER GRAMD:

1. Es el encargado de asegurar el cumplimiento de la calidad de servicio de la ER GRAMD.
2. Autoriza la emisión de los certificados digitales ante la EC BIT4ID, para lo cual cumplirá y hará cumplir los plazos establecidos para los trámites realizados.
3. Controla el cumplimiento de las disposiciones legales, reglamento interno, RPS y otras que correspondan a las actividades dentro de la IOFE y; administrará los recursos y bienes que le han sido asignados.
4. Es responsable de la elaboración de la Declaración de Prácticas y Políticas de Registro, Política de Seguridad, Política de Privacidad y Plan de Privacidad; de la supervisión del cumplimiento de la normativa sobre protección de datos personales; y la implementación de las acciones respectivas.
5. Supervisará las estrategias, programas, políticas, procedimientos y controles relacionados a la seguridad de la información en el ámbito de la ER GRAMD.

3. Supervisor y Coordinador de la ER GRAMD:

1. Es el encargado de velar por el cumplimiento de las funciones de los Operadores de Registro de Datos, y distribuir la carga de trabajo entre dichas personas.
2. Autoriza la emisión de los certificados digitales ante la EC BIT4ID, para lo cual cumplirá y hará cumplir los plazos establecidos para los trámites realizados.
3. Controla el cumplimiento de las disposiciones legales, Declaración de Prácticas y Políticas de Registro, Política de Seguridad, Política de Privacidad y Plan de Privacidad, y otras que correspondan a las actividades dentro de la IOFE.
4. Reportará las fallas e interrupciones de los sistemas y servicios tanto de la ER GRAMD como de la EC BIT4ID.
5. Supervisará y apoyará el cumplimiento de las metas de la ER GRAMD.
6. Es responsable de la elaboración de la Política de Seguridad conjuntamente con el Administrador y Oficial de Seguridad de Información de la ER GRAMD.
7. Es responsable de implementar las políticas de planificación de respuesta a incidentes declarada en la Política de Seguridad, conjuntamente con el Gerente de Registro Digital de la ER GRAMD.

4. Jefe de Cuentas de la ER GRAMD:

1. Es el encargado de realizar la supervisión del correcto manejo de la cuenta del cliente.
2. Desarrollará los procedimientos comerciales para la adquisición de certificados digitales.
3. Es responsable del contacto directo con la EC BIT4ID.
4. Supervisará al Ejecutivo de Cuentas y Operador de Registro de Datos.
5. Tendrá pleno conocimiento de los servicios de registro de datos de suscriptores y/o titulares, y venta de certificados digitales.

5. Ejecutivo de Cuentas:

1. Es el encargado de orientar al cliente sobre el proceso de adquisición de certificados digitales.
2. Gestionará el soporte técnico y administrativo del cliente.
3. Organizará y supervisará el correcto manejo de los documentos requeridos al cliente.
4. Tendrá pleno conocimiento de los servicios de registro de datos de suscriptores y/o titulares, y venta de certificados digitales.

6. Operador de Registro de Datos:

1. Tendrá acceso a los sistemas de validación de identidad de los clientes.
2. Es responsable del correcto manejo y acceso a la información del suscriptor.
3. Es responsable del correcto registro de datos para la adquisición de los certificados digitales.
4. Tendrá pleno conocimiento de las políticas y prácticas de la ER y la EC.

7. Analista de Control Externo-BIT4ID:

1. Es el encargado de coordinar con las personas involucradas en el proceso de registro o verificación de datos, a fin de establecer la frecuencia y los recursos necesarios para ejecutar las auditorías internas en el Plan Anual de Auditoria Interna declarado en la Política de Seguridad.
2. Tendrá pleno conocimiento de las políticas y prácticas de la EC. Teniendo en cuenta que este Analista trabaja para la EC BIT4ID.

8. Asesor Externo Especialista en Recursos Humanos:

1. Es responsable de implementar lo estipulado en la Política de Seguridad con respecto a la contratación, renovación, y despido de personal y prestadores de servicios vinculados con la ER GRAMD.
2. Es responsable de controlar los procesos de servicios en la administración de personal, a objeto de dar cumplimiento a los planes y programas sobre los beneficios establecidos por la ER GRAMD.
3. Llevará el registro de los pasivos laborales del personal activo (vacaciones, anticipos de prestaciones sociales, etc.) y liquidaciones de prestaciones sociales, a objeto de cumplir con los procedimientos establecidos por la ER GRAMD.
4. Elaborará y controlará los procesos de nómina a fin de garantizar el depósito oportuno de los empleados y prestadores de servicios de la ER GRAMD.

16.2.2 NÚMERO DE PERSONAS REQUERIDAS POR LABOR

La ER GRAMD mantiene una política rigurosa para asegurarla separación de funciones basado en responsabilidades de trabajo.

La aprobación de la emisión de un certificado digital lo llevarán a cabo mínimo dos personas. Primero el Operador de Registro de Datos, quién verificará y/o autenticará la identidad del solicitante, aprobando o rechazando la solicitud correspondiente, y luego el Supervisor de Registro Digital de la ER GRAMD quién autorizara la emisión del certificado comunicándolo a la EC BIT4ID, según lo señalado en el procedimiento de trámite de emisión y entrega del certificado digital.

16.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN POR CADA ROL

El personal que opera el sistema administrativo de la ER GRAMD está autorizado para acceder a la misma previa autenticación de su identidad, mediante el uso de credenciales digitales como

usuario, contraseña y certificado digital personal de autenticación almacenado en un dispositivo criptográfico.

16.3 CONTROLES DE PERSONAL

En esta sub sección se establecen los controles implementados por la ER GRAMD en relación con el personal que desempeña funciones, comprenden entre otros, los requisitos a cumplir para su incorporación, la forma como éstos deben ser comprobados, la capacitación a los que estarán sujetos y las sanciones por acciones no autorizadas. Estos controles alcanzan al personal a cargo de terceros y contratistas que realicen labores por tiempo determinado en las instalaciones de la ER GRAMD.

16.3.1 CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS

Los procedimientos y requisitos dispuestos por GRAMD para la gestión del personal que desarrolla funciones en la ER GRAMD buscan asegurar que se acredite de manera suficiente y fehaciente las calificaciones y experiencia profesional.

En tal sentido, las prácticas de selección y reclutamiento del personal se lleva a cabo a través de un Asesor Externo especialista en Recursos Humanos, tomando en cuenta los perfiles fijados por la Gerencia General de GRAMD.

La definición de los puestos de trabajo y sus funciones, se encuentran detalladas en los contratos de trabajo respectivos.

En el caso del personal a cargo de terceros, será responsabilidad del contratista acreditar la formación y experiencia de aquellos, de acuerdo con los requerimientos fijados por la Gerencia General de GRAMD, debiendo presentar la documentación que evidencie el cumplimiento de dicho aspecto.

16.3.2 PROCEDIMIENTO PARA VERIFICACIÓN DE ANTENCEDENTES

Es política de GRAMD verificar la documentación aportada por el personal aspirante a realizar labores en la ER GRAMD. Para tal efecto, el Asesor Externo especialista en Recursos Humanos, ejecuta los siguientes controles mínimos:

- ✓ Verificación de la identidad personal.
- ✓ Confirmación de las referencias.
- ✓ Confirmación de empleos anteriores.
- ✓ Revisión de referencias profesionales.
- ✓ Confirmación de grados académicos obtenidos.
- ✓ Verificación de antecedentes penales y policiales, entre otros.

En caso de personal a cargo de terceros, corresponde al contratista realizar la verificación de los antecedentes respectivos de sus empleados.

16.3.3 REQUISITOS DE CAPACITACIÓN

Es política de GRAMD que toda persona que desarrolla funciones en la ER GRAMD, reciba desde su ingreso una instrucción- inducción acorde con la función a desempeñar. Dicho personal se encontrará sujeto a un plan de capacitación continuo, a fin que las responsabilidades asumidas como parte de los servicios de certificación digital se desarrollen en forma competente.

El contenido de los programas de capacitación se controla y refuerza periódicamente por la Gerencia de Registro Digital, en coordinación con el Administrador de la ER GRAMD, llevándose un registro y archivo de las materias impartidas para los efectos de las re-capacitaciones.

El plan de capacitación, adecuado a las funciones a desempeñar en la ER GRAMD, contiene como mínimo los siguientes conceptos básicos:

- ✓ Uso y operación del hardware y software empleado.
- ✓ Aspectos relevantes de la "Declaración de Prácticas y Políticas de Registro", "Política de Seguridad", "Política de Privacidad", "Plan de Privacidad", y otra documentación que comprenda sus funciones.
- ✓ Marco regulatorio de la prestación de los servicios de certificación digital.
- ✓ Procedimientos en caso de contingencias.
- ✓ Procedimientos de operación, administración y seguridad para cada rol específico.

La Gerencia de Registro Digital de la ER GRAMD, conjuntamente con la Administración de la ER GRAMD, cuando estimen conveniente o por disposición legal expresa, podrá incluir otros temas en la capacitación con la finalidad de lograr una apropiada formación y alcanzar un adecuado proceso de mejora continua de la capacitación del personal.

16.3.4 FRECUENCIA Y REQUISITOS DE LAS RE-CAPACITACIONES

La re-capacitación se efectuara necesariamente cuando el personal sea sustituido o rotado, así como cuando se realicen cambios en los procedimientos de operaciones o en la "Declaración de Prácticas y Políticas de Registro", "Política de Seguridad", "Política de Privacidad", y "Plan de Privacidad", o en cualquier otro documento que resulte relevante para la ER GRAMD y que comprometa los aspectos funcionales de las labores del personal.

16.3.5 FRECUENCIA Y SECUENCIA DE LA ROTACIÓN EN EL TRABAJO

La ER GRAMD, en caso determine la conveniencia, podrá implementar rotaciones de trabajo entre los distintos roles, con el objeto de incrementar la seguridad y asegurar la continuidad de las actividades. La rotación es comunicada al personal con el documento pertinente.

16.3.6 SANCIONES POR ACCIONES NO AUTORIZADAS

Le es aplicable a todo el personal el Reglamento Interno de GRAMD, independientemente de la modalidad de contratación.

Con relación a las operaciones de la ER GRAMD, se considerarán acciones no autorizadas, aquellas realizadas por el personal de manera negligente o malintencionada y que contravengan la presente "Declaración de Prácticas y Políticas de Registro", "Política de Seguridad", "Política de Privacidad", y "Plan de Privacidad", así como las directivas, guías de procedimientos, reglamento interno, y demás documentos afines.

La ER GRAMD apenas tome conocimiento de la acción no autorizada o de su potencial ejecución, suspenderá el acceso a todos los sistemas de información a aquel personal que se encuentre involucrado en el hecho.

Con la confirmación del hecho, el Administrador de la ER GRAMD, informará a la Gerencia General de Gramd, a fin de que ésta autorice al Área Legal para que inicie el procedimiento sancionador correspondiente, y de ser el caso se inicien las acciones legales para el resarcimiento por los daños y perjuicios en lo que pudiera verse afectado GRAMD.

16.3.7 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL DE GRAMD

La ER GRAMD suministra a todo su personal, en función a los cargos y roles que desempeñe, la documentación mínima siguiente:

- ✓ Manual de funcionamiento de equipos y software que debe operar en la ER GRAMD.
- ✓ "Declaración de Prácticas y Políticas de Registro", "Política de Seguridad", "Política de Privacidad", y "Plan de Privacidad".
- ✓ Normas legales y marco regulatorio aplicables a sus funciones en la ER GRAMD.
- ✓ Documentación aplicable en caso de contingencias.
- ✓ Otra documentación relevante en relación a sus funciones en la ER GRAMD.

17 RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

Se establece un plan de contingencias que permita el restablecimiento y mantenimiento de las operaciones de la ER. Este plan debe contemplar las acciones a realizar, los recursos a utilizar y el personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.

Dicho plan debe asegurar que los aspectos básicos del negocio, tales como servicios de validación o revocación, puedan ser reasumidos dentro de un plazo máximo de 24 horas, el cual constituye el plazo máximo para la emisión de las listas de revocación de certificados.

Los planes deben ser 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, juntamente con la información respecto a las acciones correctivas que pudieran ser necesarias.

17.1 PROCEDIMIENTOS EN CASO DE COMPROMISO DE LA CLAVE PRIVADA DE LA ENTIDAD

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.

18 GESTIÓN DE OPERACIONES

18.1 MÓDULO CRIPTOGRÁFICO

La generación de claves de los suscriptores debe ser realizada en módulos criptográficos FIPS 140-2 o Common Criteria.

Los módulos criptográficos usados por los Operadores de Registro deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 o Common Criteria EAL 4 como mínimo.

i. RESTRICCIONES DE LA GENERACIÓN DE CLAVES

Las claves pueden ser generadas solamente por los propios suscriptores.

ii. ENTREGA DE LA CLAVE PÚBLICA

Cuando un suscriptor genera su propio par de claves o par de claves del titular, las claves públicas correspondientes deben ser entregadas al emisor del certificado de manera tal que se asegure la autenticidad de dicho suscriptor.

En los casos en que las ERs acepten las claves públicas en representación de los emisores de los certificados, éstas deberán ser entregadas a dicho emisor de manera tal que se asegure el mantenimiento de la asociación que debe existir entre el titular y la clave.

iii. DEPÓSITO DE LA CLAVE PÚBLICA

La ER GRAMD no genera copias de las claves privadas de los suscriptores ni de los Operadores de Registro en ninguna modalidad.

iv. DATOS DE ACTIVACIÓN

Los datos de activación del módulo criptográfico serán administrados por los suscriptores. En caso de obtener módulos criptográficos de GRAMD se brindará la información correspondiente para realizar la asignación de los de activación por canales seguros.

19 AUDITORÍAS

a. FRECUENCIA DE AUDITORÍAS

La ER GRAMD, efectuará auditorías internas al menos una vez al año.

Las evaluaciones técnicas del INDECOPI se llevarán cada vez que la Autoridad Administrativa Competente lo requiera.

b. CALIFICACIONES DE LOS AUDITORES

La selección de los auditores depende del INDECOPI.

c. RELACIÓN DEL AUDITOR CON LA ER GRAMD

Los auditores o asesores deben ser independientes de la ER GRAMD.

20 MATERIAS DE NEGOCIO Y LEGALES

a. TARIFAS

Las tarifas por los servicios de registro y certificación digital serán proporcionadas a los clientes, a través de los Ejecutivos de Ventas de la ER GRAMD. Directamente, mediante correo electrónico.

b. POLÍTICAS DE REEMBOLSO

Las políticas de reembolso por los servicios de registro serán definidas en “El Contrato”.

c. COBERTURA DE SEGURO

GRAMD proporciona a sus clientes servicios de registro amparados por la cobertura del Seguro de Responsabilidad Civil de la Entidad de Certificación BIT4ID.

d. PROVISIONES Y GARANTÍAS

Las garantías por los servicios de registro y certificación digital serán definidas en “El Contrato”, en relación a errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de certificado o de revocación y protección de datos personales provistos.

e. EXCEPCIONES DE GARANTÍAS

La ER GRAMD no se responsabiliza en casos de compromiso de la clave en manos del suscriptor, o cualquier solicitud no realizada según los procedimientos definidos en el presente documento.

f. OBLIGACIONES DE LOS SUSCRIPTORES Y TITULARES

Las obligaciones de los suscriptores y titulares se definen en sus respectivos contratos.En particular los suscriptores y titulares tienen la responsabilidad de solicitar la revocación desuscertificados en casos de compromiso de su clave privada.

g. OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

La ER referencia provisiones de garantía y responsabilidad en relación a errores u omisiones, incluyendo limitaciones y exclusiones, términos, condiciones, incluyéndolas en los contratos con los suscriptores, y haciéndolos disponibles para los terceros que confían.

Los suscriptores y/o titulares están obligados a cumplir las obligaciones establecidas en el CP y CPS de la EC vinculada a la ER "GRAMD"

h. INDEMNIZACIÓN

Los casos de indemnización están establecidos en "El Contrato".

i. NOTIFICACIONES

Los medios de notificación están establecidos en "El Contrato".

j. ENMENDADURAS Y CAMBIOS

Las enmendaduras y cambios serán comunicadas al INDECOPI y luego de su aprobación serán publicadas en el repositorio y notificadas a los titulares y suscriptores, conforme a los medios especificados en sus contratos.

k. RESOLUCIÓN DE DISPUTAS

El procedimiento de resolución de disputas está establecido en "El Contrato".

l. CONFORMIDAD CON LA LEY APLICABLE

La ER GRAMD se compromete a cumplir la Ley aplicable a las operaciones de registro: las Guías de Acreditación de Entidades de Registro o Verificación del INDECOPI, la Ley de Firmas y Certificados Digitales y su Reglamento.

m. SUBROGACIÓN

La ER GRAMD no delega sus responsabilidades respecto de las operaciones de registro sobre terceros no autorizados por la IOFE. Todos los casos de responsabilidad de otros participantes como las EC son especificados en este documento.

n. FUERZA MAYOR

Las cláusulas de fuerza mayor están establecidas en "El Contrato".

o. DERECHOS DE PROPIEDAD INTELECTUAL

Todos los derechos de propiedad intelectual incluyendo los que corresponden a las aplicaciones o software desarrollado para las actividades de la ER GRAMD, OIDs, la presente "Declaración de Prácticas y Políticas de Registro", "Política de Seguridad", "Política de Privacidad", y "Plan de Privacidad", así como cualquier otro documento, electrónico o de cualquier otro tipo, son propiedad de GRAMD. Por tanto, se prohíbe cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son de titularidad de GRAMD.

Las claves privadas y las claves públicas son propiedad del titular del certificado digital.

21 FINALIZACIÓN DE LA ER GRAMD

Antes de su finalización, la ER GRAMD informará al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.

Todas las solicitudes y contratos de suscriptores y titulares serán transferidos al INDECOPI o a otro PSC designado por éste.

En caso de una operación de transferencia de titularidad, por el periodo establecido por la AAC de 10 años luego de generado el registro, los nuevos dueños u operadores solicitarán la evaluación de cumplimiento al INDECOPI para garantizar que se mantienen los requisitos de acreditación.

Se advertirá a todos los suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por una EC que finaliza o transfiere sus operaciones a traves de una comunicación a la AAC con 60 dias de anticipacion, mediante un comunicado publicado en la siguiente dirección:

22 BIBLIOGRAFIA

En la redacción de la presente RPS, se utilizó:

- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo N° 052-2008-PCM, y sus modificatorias, el Decreto Supremo N° 070-2011-PCM, y Decreto Supremo N° 105-2012-PCM.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Guía de Acreditación de Entidad de Registro, Versión 3.3 - INDECOPI.
- Norma Marco sobre Privacidad para los países integrantes del APEC, aprobada en la 16° Reunión Ministerial del APEC, Santiago de Chile, 17 y 18 de noviembre de 2004.