GRAMD

POLÍTICA DE SEGURIDAD

POLÍTICA DE SEGURIDAD DE GRAMD PERUANA S.A.C. VERSIÓN 1.0

Elaborado por:	Administrador y Oficial de Seguridad de Información de la ER GRAMD
Revisado por:	Supervisor y Coordinador de Seguridad de Información de la ER GRAMD Comité para la Acreditación de la ER GRAMD
Aprobado por:	Gerente 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:	Política de Seguridad
Versión:	1.0
Fecha de elaboración:	27/11/2017

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 naturales así como representantes legales de empresas, de ser el caso, con el soporte de una Autoridad Certificadora reconocida mundialmente como CAMERFIRMA.

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

- **CAMERFIRMA PERÚ S.A.C.** (Prestadora de Servicios de Certificación Digital, debidamente acreditada por el INDECOPI), que es una sociedad peruana que pertenece a la sociedad AC CAMERFIRMA S.A. (en adelante CAMERFIRMA), y
- **GRAMD PERUANA S.A.C.**, que presta los servicios de registro o verificación, tanto de personas naturales como 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 CAMERFIRMA PERÚ 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 de persona jurídica clase III.

2. OBJETIVO

Establecer el marco general y los lineamientos para la seguridad de la información que administra la Entidad de Registro o Verificación – ER GRAMD; a fin de garantizar la disponibilidad, confidencialidad e integridad de la información durante el desarrollo de las operaciones y acciones que ésta realiza.

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 CAMERFIRMA 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. PARTICIPANTES

4.1 ENTIDAD DE CERTIFICACIÓN - EC CAMERFIRMA

La EC CAMERFIRMA, 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 la EC CAMERFIRMA 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 la EC CAMERFIRMA 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 (AC CAMERFIRMA S.A.[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 CAMERFIRMA.

4.4 TITULAR DE CERTIFICADO DIGITAL

Un titular de certificado digital, es aquella persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

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, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado esta 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 cual deberá ser dueña del agente automatizado. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

4.6 SOLICITANTE DE CERTIFICADO DIGITAL

Se entenderá por Solicitante de un certificado digital, a aquella persona natural o jurídica que solicita un certificado digital, aceptando previamente lo establecido en la CPS de CAMERFIRMA, así como en la RPS de GRAMD.

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

4.7 TERCERO QUE CONFÍA O TERCER USUARIO

Se considerará como Tercero que Confía o Tercer Usuario, a aquellas personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

[1] Prestador de Servicios de Confianza (TSP)

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. ADMINISTRACIÓN DEL DOCUMENTO

5.1 ORGANIZACIÓN QUE ADMINISTRA EL DOCUMENTO

Razón Social:	Gramd Peruana S.A.C.
R.U.C.:	20535708798
Dirección:	Av. República de Panamá N° 3418, Of. 301, Urb. Limatambo, Distrito de San Isidro, Provincia y Departamento de Lima.
Teléfonos:	(+511) 7390900 / 0800-7-1500

5.2 PERSONA DE CONTACTO

Oficial de Seguridad de Información - Gerente de Registro Digital

Teléfono:	(+511) 7390900, Ext. 121
Correo electrónico:	acastaneda@gramd.com

6. BASE LEGAL

- ✓ Ley N° 27269, Ley de Firmas y Certificados Digitales.
- ✓ Ley N° 27310, Ley que modifica el artículo 11, de la Ley N° 27269.
- ✓ Ley N° 28403, que dispone la recaudación de un aporte por supervisión y control anual por parte de Indecopi de la Entidades de Certificación y de Verificación.
- ✓ Decreto Supremo 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
- ✓ Decreto Supremo N° 026-2016-PCM, que aprueba medidas para el fortalecimiento de la IOFE y la implementación progresiva de la firma digital en el sector público y privado.
- ✓ Guía de Acreditación de Entidades de Registro o Verificación
- ✓ Ley N° 29733, Ley de Protección de Datos Personales.

7. ALCANCE

7.1 ÁREAS DE ALCANCE

El contenido de la presente política así como las reglas o normas y procedimientos que se deriven de ella, serán de cumplimiento obligatorio para el personal de la ER GRAMD, que participen en la ejecución de las actividades que son parte del proceso de registro o verificación de datos y su posterior certificación digital.
La presente política así como las reglas o normas y procedimientos que se deriven de ella, también serán de cumplimiento obligatorio para los proveedores de servicios o terceros de la ER GRAMD.

7.2 SERVICIOS DE ALCANCE

La presente Política de Seguridad aplica para los siguientes servicios de la ER GRAMD:

Comprende los servicios de registro o verificación, tanto de personas naturales como jurídicas, en la demarcación de Lima y otras ciudades del Perú, conforme a lo establecido en la Declaración de Prácticas y Políticas de Registro, así como la protección de los documentos sustentatorios y su archivo ya sean en formato físico o digital.

7.3 INCLUSIONES DE ESTE DOCUMENTO

El presente documento incluye los siguientes aspectos: la evaluación de riesgos, control de acceso, seguridad de personal, seguridad física, seguridad de comunicaciones y redes, mantenimiento de equipos y su desecho, control de cambios y configuración, planificación de contingencias, respuesta a incidentes, auditorías y detección de intrusiones, y medios de almacenamiento de datos; todos ellos dentro del ámbito de las actividades que la ER GRAMD realiza.

8. RESPONSABLES

8.1 RESPONSABLE DE APROBAR Y APOYAR LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA ER GRAMD

- La Gerencia de Registro Digital de la ER GRAMD.

8.2 RESPONSABLES DE ELABORAR, EFECTUAR REVISIONES PERIÓDICAS, PROPONER Y APOYAR LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA ER GRAMD

- El Administrador y Oficial de Seguridad de Información de la ER GRAMD.
- El Supervisor y Coordinador de Seguridad de Información de la ER GRAMD.
- El Comité para la Acreditación de la ER GRAMD.

8.3 RESPONSABLES DE IMPLEMENTAR LA POLÍTICA DE SEGURIDAD DE LA ER GRAMD.

- Las personas que estén involucradas en el proceso de certificación digital, en los aspectos que les correspondan (Jefe de Cuentas, Ejecutivos de Cuentas, Operadores de Registro, Analista de Control Externo-Camerfirma, Asesor Externo Especialista Recurso Humanos).

8.4 RESPONSABLES DE SUPERVISAR EL CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DE LA ER GRAMD.

- El Administrador y Oficial de Seguridad de Información de la ER GRAMD.
- El Supervisor y Coordinador de Seguridad de Información de la ER GRAMD.
- Cada persona involucrada en el proceso de certificación digital.

9. GLOSARIO DE TÉRMINOS

- ✓ Activo: Algo que tenga valor para la organización
- ✓ Análisis de riesgos: Uso sistemático de la información para identificar orígenes y estimar el riesgo.
- ✓ Amenaza: Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.
- ✓ Control: Herramienta de la gestión de riesgos, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.

- ✓ Evaluación de riesgo: Proceso general de análisis y evaluación del riesgo.
- ✓ Evento de seguridad de la información: Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.
- ✓ Gestión de riesgo: Actividades coordinadas para dirigir y controlar una -. organización considerando el riesgo.
- ✓ Identidad digital: Es el reconocimiento de la identidad de una persona en un medio digital (como por ejemplo Internet) a través de mecanismos tecnológicos seguros y confiables, sin necesidad de que la persona esté presente físicamente.
- ✓ Incidente de seguridad de la información: Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocio y de amenazar la seguridad de la información.
- ✓ Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.
- ✓ Seguridad de la Información: Preservación de la confidencialidad, disponibilidad o integridad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, veracidad o confiabilidad también pueden ser consideradas.
- ✓ Tratamiento del riesgo: Proceso de selección e implementación de medidas o controles para modificar el riesgo.
- ✓ Vulnerabilidades: Debilidades de seguridad asociadas con los activos de información.

10. POLÍTICAS

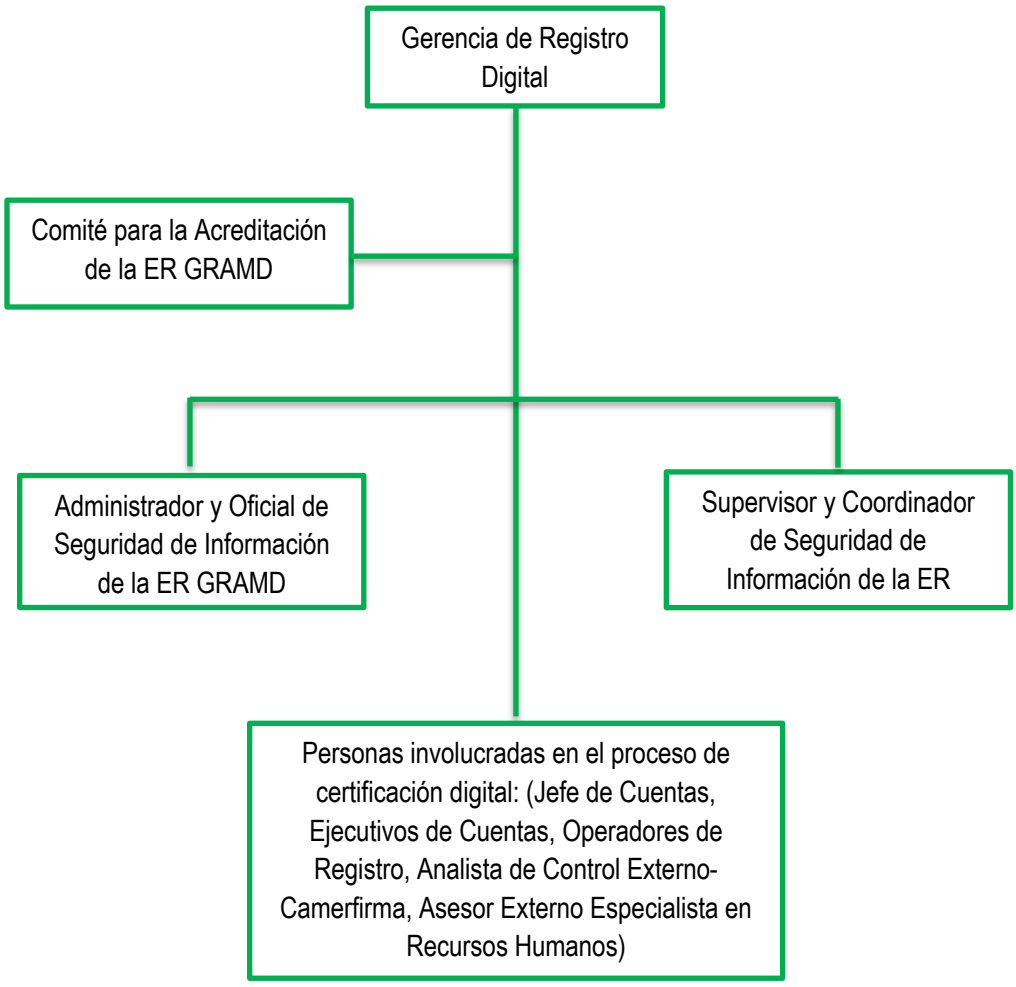
10.1 GENÉRICA

Gramd Peruana S.A.C. en su calidad de Entidad de Registro o Verificación, reconoce como su activo principal a la información resultante del proceso de registro o verificación de datos, que permite la posterior emisión de certificados digitales; en tal sentido, se efectúa el análisis y evaluación de los riesgos, la aplicación de controles y la toma de conciencia en el personal, de modo que nos permita mantener la confidencialidad, integridad y disponibilidad de la misma, así como dar cumplimiento a los requisitos técnicos y legales vigentes.

10.2 ESPECIFICA

10.2.1 ORGANIZACIÓN

Gramd Peruana S.A.C. ha establecido la siguiente estructura de gestión registro o verificación de datos, que permite la posterior emisión de certificados digitales, de la seguridad de la información en su calidad de ER, con la finalidad de implementar en el proceso de controles que permitan asegurar la confidencialidad, integridad y disponibilidad de la información.



Esquema 1: Estructura de gestión de la Seguridad de la Información en la ER GRAMD.

El Administrador y Oficial de Seguridad de Información, y el Supervisor y Coordinador de Seguridad de Información de la ER GRAMD, tienen entre sus funciones la elaboración de la Política de Seguridad, asimismo, después de la aprobación de esta política por la Gerencia de Registro Digital, esta será publicada a través de la Intranet para conocimiento de todo el personal que interviene en el proceso de certificación digital.

La Gerencia de Registro Digital también tiene entre sus responsabilidades coordinar el desarrollo de las auditorías internas a intervalos planificados o cuando ocurran cambios significativos en la puesta en marcha de la seguridad; así mismo, asignará las distintas responsabilidades respecto a la Seguridad de la Información a las personas involucradas en el proceso de registro o verificación de datos, y posterior certificación digital. Con la finalidad de garantizar la disponibilidad, confidencialidad e integridad de la información, coordinará la ejecución de revisiones y actualizaciones periódicas de la Política de Seguridad en concordancia con los riesgos identificados, requerimientos de la entidad, leyes y regulaciones.

Para asegurar la Protección de Datos Personales, el Administrador y Oficial de Seguridad de la Información, es también responsable de la supervisión del cumplimiento de la

normativa sobre protección de datos personales y la implementación de las acciones respectivas.
Para la supervisión de la Seguridad de la Información, el Administrador y Oficial de Seguridad de Información, asumirá la responsabilidad de supervisar la implementación de la visión de seguridad de la información, así como de las estrategias, programas, políticas, procedimientos y controles relacionados a la seguridad de la información en el ámbito de la ER GRAMD.

Para la planificación y ejecución de las auditorías internas a la ER GRAMD, la Gerencia de Registro Digital cuenta con un Analista de Control Externo, quien en coordinación con las personas involucradas en el proceso de registro o verificación de datos y posterior certificación digital, establecerá la frecuencia y los recursos necesarios para ejecutar las auditorías internas en el Plan Anual de Auditoria Interna.

10.2.2 EVALUACIÓN DE RIESGOS

Para cada proceso vital o crítico que se desarrolla en el ámbito de la ER GRAMD, se deberá efectuar el análisis y evaluación de riesgos, teniéndose en consideración tanto las amenazas internas como las externas; asimismo, se identificarán, evaluarán e implementarán las opciones de tratamiento del riesgo que permitan mitigar el impacto en los activos de información involucrados en el proceso de registro o verificación de datos y posterior emisión del certificado digital. La evaluación y tratamiento del riesgo se realizará de acuerdo a la Metodología de Análisis y Tratamiento del Riesgo definida por la ER GRAMD.

Corresponderá a la Gerencia de Registro Digital, decidir si se acepta el riesgo o se brinda las facilidades necesarias para implementar las opciones de tratamiento que permita evitar o mitigar el impacto de estos riegos.

10.2.3 CONTROL DE ACCESOS

Se controlará el acceso a la información confidencial generada durante el proceso del certificado digital, en concordancia con lo establecido en el Plan de Privacidad de la ER GRAMD, así como la información reservada de ésta misma, y los resultados de la evaluación de riesgos.

La administración del acceso a los usuarios considerará que:

- Toda solicitud de acceso físico y lógico, así como la administración de las cuentas de usuario a los activos de información deberá ser realizada conforme a los procedimientos establecidos.
- Sólo se asignará cuentas de acceso individuales, si por razones de operación se requiere el uso de una misma cuenta para más de un usuario, lo que deberá ser de conocimiento del Administrador y Oficial de Seguridad de Información de la ER GRAMD y aprobado por la Gerencia de Registro Digital.

El personal que reciba una cuenta de usuario para el acceso a los activos de información de la ER GRAMD, deberá hacer uso adecuado de sus contraseñas de acceso manteniendo la confidencialidad de la misma, no dejando su ambiente de trabajo desatendido, solicitando su cambio de contraseña si tiene algún indicio de su vulnerabilidad y seleccionando una contraseña que tenga un nivel adecuado de complejidad; es responsabilidad del supervisor

del personal el informar a éste sobre el cumplimiento estas disposiciones y el verificar su cumplimiento.
Es responsabilidad de los propietarios de los activos de información de la ER GRAMD, clasificar la información (física o digital) de acuerdo a lo indicado en los lineamientos definidos para la clasificación de información. Asimismo, identificar y agrupar a los usuarios, considerando su necesidad de información para el desarrollo de sus funciones o labores que realizan, con la finalidad de establecer los niveles de acceso a la base de datos, sistemas y/o aplicativos, centros de datos, infraestructura de procesamiento de información, archivos físicos y electrónicos, de acuerdo con el resultado de la evaluación de riesgos y los requerimientos de la organización.

Con respecto a los accesos de entidades, organizaciones o instituciones externas que requieran acceder a los servicios de la ER GRAMD, se deberá controlar los accesos lógicos proporcionados a dichas entidades estableciendo interfaces seguras entre la red de datos de la ER GRAMD, y la red de datos de la entidad externa.

Previo al acceso a los servicios de la ER GRAMD, dichas entidades externas deberán firmar un acuerdo de confidencialidad y un compromiso a salvaguardar la integridad, disponibilidad y confidencialidad de la información que utilice o sea de su conocimiento.

10.2.4 SEGURIDAD DEL PERSONAL

Cada área debe asegurar que el personal, contratista y terceros reciban y comprendan sus responsabilidades respecto al uso y tratamiento de los activos de información relacionados al proceso registro o verificación de datos y posterior certificación digital, con la finalidad de reducir el riesgo de hurto, fraude o mal uso de la información. Así mismo, deberán asegurar la implementación de controles de seguridad relacionados al personal, antes, durante y finalizado el empleo o servicio brindado a la ER GRAMD.

Antes del empleo o servicio:

- Los perfiles de los puestos deberán ser definidos en base a las funciones que se van a desarrollar y las responsabilidades que les competan.
- El Asesor Externo Especialista en Recursos Humanos debe implementar controles para la selección y contratación del personal, a fin de verificar la veracidad de los datos proporcionados por los postulantes, así como sus antecedentes penales y policiales.
- Para los servicios efectuados por terceros, la verificación de los datos la efectuará el proveedor del servicio. La ER GRAMD, se reserva el derecho de verificar dicha documentación.
- Cada una de las personas que presta servicios en la ER GRAMD deben firmar un Contrato de Confidencialidad y un documento de compromiso para salvaguardar la integridad, disponibilidad y confidencialidad de la información que utilice, o sea de su conocimiento.

Durante el empleo o servicio:

- Toda persona que presta servicios en la ER GRAMD, recibirá charlas de inducción en materia de Seguridad de la Información.
- Se deben desarrollar actividades de capacitación continua dirigidas a mantener actualizados los conocimientos del personal respecto al uso y reserva de la información, así como a las políticas y procedimientos relevantes para sus funciones. Estas

actividades de capacitación así como los responsables de efectuarlas estarán definidas en el Plan de Capacitación.

- Para los casos de tercerización de servicios se informará al prestador del servicio cuáles son los criterios que deberá considerar para la seguridad de la información, así como también, se monitoreará y revisará su cumplimiento.
- Todo incumplimiento de la Política de Seguridad de parte del personal o proveedores, deberán ser informadas, por el personal que tome conocimiento del hecho, al Administrador y Oficial de Seguridad de Información de la ER GRAMD para su análisis, evaluación y comunicación al Asesor Externo Especialista en Recursos Humanos, a fin de que éste proceda a la sanción que corresponda en concordancia con los procedimientos internos, en el caso de los proveedores para su comunicación a la Gerencia General para la sanción que corresponda de acuerdo a la legislación vigente.

Finalización del empleo o servicio:

- Todo cambio o finalización de funciones deberá realizarse de acuerdo a los procedimientos de la ER GRAMD, incluyendo la entrega de los bienes asignados al personal. De igual modo, cada encargado o supervisor deberá solicitar el retiro de accesos a la información o servicios de todo personal que ya no labore en la empresa.

El Asesor Externo Especialista en Recursos Humanos, la Gerencia General, y el personal de confianza que conforman la ER GRAMD, son los responsables de implementar lo estipulado en la Política de Seguridad con el personal y proveedores, respectivamente.

10.2.5 SEGURIDAD FÍSICA

La ER GRAMD debe implementar controles de seguridad física con la finalidad de prevenir accesos no autorizados a los ambientes en que se procesa o resguarda información confidencial, así mismo, evitar el daño o perdida de los activos de información críticos que intervienen en el proceso de certificación digital.

Se deben delimitar los perímetros del ambiente en que se resguarda la información sensible, y se establecerán los controles físicos de entrada y salida.

Los ambientes serán diseñados e implementados adecuadamente para la seguridad de los recursos que albergan y del personal. Se deberá, asimismo, establecer controles de acceso a los ambientes, al uso de las llaves de los mismos, y asignar a los responsables respectivos. Así mismo, se debe definir e implementar un plan de evacuación en casos de desastre.

Estas políticas de seguridad física se deben considerar también para los ambientes de contingencia. Es responsabilidad de la Gerencia de Registro Digital, el implementar las políticas de seguridad física.

10.2.6 SEGURIDAD DE COMUNICACIONES Y REDES

Se deben establecer responsabilidades y procedimientos documentados de operación asociado al procesamiento de información y recursos de comunicaciones, con el objetivo de evitar daños, accesos no autorizados, mal uso de los activos de información, garantizar la seguridad de los datos y la disponibilidad de los servicios utilizados a través de la red de la ER GRAMD y del internet.

Es responsabilidad de la Gerencia de Registro Digital, el implementar las políticas de seguridad de comunicaciones y redes.

10.2.7 MANTENIMIENTO DE EQUIPOS Y SU DESECHO

Se debe asegurar la disponibilidad e integridad de los equipos a través de un adecuado plan de mantenimiento. Antes de su desecho o reúso, se revisará que toda información sensible haya sido removida, con la finalidad de prevenir el acceso no autorizado a información sensible.

El reemplazo, decomiso, manipulación y desecho, tanto del hardware como del software, se realizarán de acuerdo a los criterios establecido por la ER GRAMD, para el correcto uso de los equipos. La Gerencia de Registro Digital, será la responsable de implementar las políticas de mantenimiento de equipo y su desecho.

10.2.8 PLANIFICACIÓN DE CONTINGENCIAS

La ER GRAMD, implementará un Plan de Contingencias a nivel de servicios, que le permita reaccionar ante una posible interrupción en las actividades críticas del proceso de registro o verificación de datos, en un tiempo prudencial; en cuanto a la certificación digital, la EC CAMERFIRMA cuenta con su propio plan de contingencias, según se puede apreciar en su CPS.

Para establecer el Plan de Contingencias se identificarán procesos críticos para el servicio prestado por la ER GRAMD, los eventos que pueden ocasionar interrupciones en estos procesos, y los planes o acciones que se deberán efectuar para mantener y recuperar las operaciones, así como el periodo en que estos deberán recuperarse. La Gerencia de Registro Digital, será la responsable de implementar las políticas de planificación de contingencias.

10.2.9 RESPUESTA A INCIDENTES

Se deberá clasificar, comunicar y atender los incidentes de manera rápida, eficaz y sistemática, a fin de garantizar el restablecimiento del servicio en el menor tiempo posible.

Para el caso de los incidentes que afecten la seguridad de la información, se deberá establecer que toda persona (personal o proveedor) que presta servicios en la ER GRAMD deberá comunicar oportunamente al Administrador y Oficial de Seguridad de Información o persona designada, cuando se haya detectado o tomado conocimiento del incidente. Adicionalmente, el Supervisor y Coordinador de Seguridad de la Información deberá llevar un registro de los incidentes de seguridad ocurridos en su ámbito de alcance, monitoreando la implementación de las acciones correctivas o preventivas que ameriten.

Corresponde a la Gerencia de Registro Digital, y al Supervisor y Coordinador de Seguridad de la Información, implementar las políticas de planificación de respuesta a incidentes.

10.2.10 AUDITORIAS Y DETECCIÓN DE INTRUSIONES

Se programarán como mínimo auditorías anuales, las cuales se ejecutarán de acuerdo al Plan Anual de Auditoria. Al término de la auditoria el área o persona auditada deberá implementar en el menor tiempo posible las acciones correctivas y preventivas identificadas. Corresponde a la Gerencia de Registro Digital elaborar el Plan Anual de Auditoría Interna.

10.2.11 MEDIOS DE ALMACENAMIENTO

Se asegurará la protección de los documentos, medios informáticos, datos de entrada o salida y documentación del proceso de registro o verificación de datos y su posterior certificación digital, de las ocurrencias como daño, modificación, robo o acceso no autorizado.

La ER GRAMD debe establecer el procedimiento para la administración de los medios de almacenamiento de información, y los controles de seguridad requeridos para el almacenamiento, uso y protección de la información. La Gerencia de Registro Digital tendrá bajo su responsabilidad la implementación de la Política de Medios de Almacenamiento.

11. CONFIDENCIALIDAD DE INFORMACIÓN DE LA ER GRAMD

11.1 INFORMACIÓN CONSIDERADA CONFIDENCIAL

La ER GRAMD mantiene de manera confidencial la siguiente inform6ación:

- ✓ 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.

11.2 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 suscriptores, titulares o terceros que confían.
- ✓ Información de certificados (siempre que el suscriptor lo autorice en el “Contrato de Suscriptor y Licencias de Certificados Digitales Personales”) y su estado.

La publicación puede estar limitada a suscriptores, titulares o terceros que confían. La Gerencia de Registro Digital, será la responsable de implementar las políticas de manejo de información confidencial.

12. REFERENCIAS

- La Norma ISO/IEC 17799 "Information technology - Code of practice for information security management" y la Norma ISO/IEC TR13335 "Information technology - Guidelines for the management of IT Security".
- La Norma ISO/IEC 27001:2005 "Information technology - Security techniques - Information security managementsystems - Requirements".
- La Norma ISO/IEC 15408 "Information technology - Security techniques - Evaluation criteria for IT security".