PERUSECURITY

POLÍTICA DE SEGURIDAD V.1.0

Entidad de Registro Peru Media Security SAC

POLÍTICA DE SEGURIDAD ER

PERU MEDIA SECURITY SAC

Generales			
Propietario del Documento	*Carlos Torres*	**Clasificación**	*Información Pública*
Aprobado por:	*Carlos Torres*	**Fecha aprobación**	*07/03/2023*

Historial de Versiones			
Versión	**Fecha**	**Autor**	**Resumen de Cambios**
1.0	*15/02/2023*	*Carlos Torres*	*Documento Inicial*

PERU SECURITY

INDICE

POLÍTICA DE SEGURIDAD ER

1. INTRODUCCIÓN

PERU MEDIA SECURITY SAC. se constituye como Entidad de Registro o Verificación de la Entidad de Certificación AC CAMERFIRMA PERÚ S.A.C. y brinda servicios de recepción de solicitudes de emisión, de revocación y re-emisión de los certificados digitales, tanto para el caso de personas jurídicas como personas naturales respecto de los servicios brindados por esta Entidad de Certificación.

2. OBJETIVO

PERU MEDIA SECURITY SAC., como Entidad de Registro o Verificación, tiene como objetivo asegurar la confiabilidad de la identidad del solicitante de los servicios de emisión, revocación y re-emisión de los certificados digitales, registrando y verificando la información entregada por los solicitantes antes de comunicar a la Entidad de Certificación la aprobación de una solicitud. Al ser ER para AC CAMERFIRMA PERÚ S.A.C. también debe dar cumplimiento a las normas, políticas y directrices establecidos por esta EC para sus Entidades de Registro a nivel internacional.

Este documento tiene como objetivo la descripción de operaciones y prácticas de seguridad de la información que cumple PERU MEDIA SECURITY SAC para la administración de sus servicios como Entidad de Registro (ER) en el marco del cumplimiento de los requerimientos de las Guías de Acreditación establecidas por el INDECOPI.

3. DEFINICIONES Y ABREVIACIONES

Entidades de Certificación	EC: Es la persona jurídica pública 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.
Entidades de Registro o Verificación	ER: Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así

	como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
Declaración de Prácticas de Registro	RPS: Conjunto de declaraciones sobre políticas y prácticas de la Entidad de Registro, que sirve para comunicar el cumplimiento legal y regulatorio a los suscriptores y terceros que confían.
Operador de Registro	Persona responsable de representar a PERU MEDIA SECURITY SAC. en calidad de ER de AC CAMERFIRMA S.A. en las actividades de recepción, validación y procesamiento de solicitudes.
Prácticas de Registro	Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.
Roles de confianza	Roles que tienen acceso a la información crítica de las operaciones de registro de PERU MEDIA SECURITY SAC. en calidad de ER de AC CAMERFIRMA S.A..
Suscriptor	Es la 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 digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.
Tercero que confía	Se refiere a las 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.
Titular	Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

4. ALCANCE

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

5. EVALUACIÓN DE RIESGOS

Es crucial identificar y valorar los activos que corresponden y evaluar el riesgo de impacto grave o moderado en los procesos de registro contemplados por la ER. Por lo tanto, se identifican las amenazas y vulnerabilidades de los activos críticos y evalúan el impacto de los riesgos para prevenir incidentes negativos que puedan afectar significativamente el servicio de certificación digital.

Para lograr esto, la metodología de riesgo se convierte en una herramienta fundamental que permite priorizar la inversión de recursos en el tratamiento de riesgos y en los requerimientos de los activos críticos que sostienen las operaciones del servicio de certificación digital. En este sentido, PERU MEDIA SECURITY SAC ha utilizado parte de la metodología MAGERIT para identificar y tratar los riesgos de impacto grave y moderado que puedan presentarse en los procesos de registro contemplados por la ER.

De esta manera, se asegura que los activos críticos de la ER sean protegidos y que el servicio de certificación digital pueda seguir operando de manera segura y confiable para sus usuarios. La utilización de la metodología de riesgo es esencial para el éxito de cualquier proceso, y en el caso de la ER, es especialmente importante debido a la naturaleza sensible y crítica de sus operaciones.

PERU MEDIA SECURITY cuenta con los siguientes documentos relacionados a la evaluación de riesgos:

- MATRIZ DE RIESGO

6. POLÍTICA DE CONTROL DE ACCESO

A continuación, se detallan los controles de acceso implementados para la protección de la información sensible, considerando el acceso a equipos informáticos, software, lectura y escritura de documentos tanto físicos como electrónicos. Asimismo, se consideran los controles de acceso a los ambientes donde se encuentra la información sensible. Todos los controles implementados están basados en los resultados de la evaluación de riesgos.

Se establece que el personal de PERU MEDIA SECURITY SAC y terceros deben acogerse a los controles de seguridad establecidos.

6.1 CONTROL DE ACCESO

6.1.1 Ubicación y construcción del local

La ubicación y diseño de las instalaciones de PERU MEDIA SECURITY SAC. en calidad Entidad de Registro de AC CAMERFIRMA PERU S.A.C prevee el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre, manteniendo vigente su acreditación ante el Instituto Nacional de Defensa Civil.

6.1.2 Perímetros de seguridad y control de acceso físico

El primer nivel de control es el ingreso al edificio:

a) Al llegar al edificio custodiado, la persona deberá acercarse al área de recepción donde se encuentra el guardia de seguridad.
b) La persona deberá presentarse de manera cordial y entregar su identificación, como el DNI o pasaporte, para que el guardia de seguridad pueda verificar su identidad.
c) El guardia de seguridad tomará nota del nombre de la persona, la hora de llegada y el motivo de su visita en un registro de ingreso.
d) A continuación, el guardia de seguridad llamará a la oficina o al departamento al que la persona desea ingresar para verificar si tiene permiso para hacerlo. Si se trata de una visita programada, es posible que se solicite el nombre de la persona que se va a visitar.
e) La persona será informada de que hay una cámara de seguridad en el timbre de la oficina que permite a los ocupantes ver a la persona que llega antes de permitir su ingreso.
f) Si se le permite ingresar, el guardia de seguridad le indicará la dirección de la oficina o departamento al que desea ingresar.

g) La persona deberá dirigirse al lugar indicado y tocar el timbre para que se le permita ingresar.
h) Si los ocupantes de la oficina o departamento verifican que la persona tiene permiso para ingresar, le permitirán el ingreso al edificio. De lo contrario, se le negará el acceso.

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

a) Están en ambientes separados de las áreas públicas de registro.
b) Sólo ingresa personal autorizado.
c) El ingreso y salida del personal es registrado.
d) Los terceros y el personal de limpieza ingresan sólo con autorización del responsable de Seguridad, asimismo son previamente identificados, registrados y supervisados durante su estancia en el área.
e) El ingreso y salida de documentos es registrado.
f) Está cerrada bajo llave cuando no esté siendo usada.
g) Cuando sea asignado un personal nuevo se verifican sus antecedentes.

6.2 GESTIÓN DE LOS DERECHOS DE ACCESO PRIVILEGIADOS

El Administrador de Sistemas será el encargado de hacer la gestión con el Oficial de Seguridad de la Información a fin de otorgar el acceso a los sistemas de información y servicios a los empleados y terceros, esto por requerimiento del jefe del área donde labora el empleado o tercero.

a) Los sistemas de información de PERUMEDIA SECURITY SAC proveen la gestión y administración de los usuarios (internos, externos), crear, editar e inactivar perfiles de acuerdo a lo requerido para el desarrollo de sus funciones. Así mismo los privilegios que tienen dentro de los mismos.

b) Para el acceso a los sistemas de información, los usuarios hacen buen uso de sus claves de acceso asignadas que serán gestionadas en AWS por el Gerente general y el Administrador de Sistema.

6.3 RESTRICCIONES DE ACCESO A LA INFORMACIÓN

PERU MEDIA SECURITY mantiene un perímetro de seguridad para proteger las áreas que contienen la información, teniendo en cuenta los niveles de clasificación y ubicación, para lo cual realiza asignación de los responsables de los activos de información indicados en el 6.1

7. SEGURIDAD DEL PERSONAL

A fin de proteger al personal y al equipamiento en las instalaciones de PERU MEDIA SECURITY SAC., en calidad de Entidad de Registro de AC CAMERFIRMA PERÚ, S.A.C. implementa los siguientes controles:

a) El personal ingresa a la oficina principal mediante factor de autenticación dactilar y seguidamente son controlados por la recepcionista.
b) El personal de PERU MEDIA SECURITY SAC solo ingresa a aquellas áreas donde se encuentre autorizado.
c) Existen implementos de seguridad contra amenazas físicas (incendios, inundaciones; etc) extintores; etc.
d) Señalización de zonas seguras.
e) No existe cableado eléctrico expuesto.
f) Uso de estabilizadores y supresores de picos.
g) Se emplea infraestructura de files rotulados que se guardan en archiveros con llaves para almacenar documentos con información confidencial.
h) Se emplea infraestructura virtual para almacenar los activos de información en formato digital.

8. SEGURIDAD FÍSICA

PERU MEDIA SECURITY SAC aplica protección física contra los daños que puedan ocurrir por fuego, inundación, terremotos, disturbios y otros causados por el hombre.

Se consideran los siguientes lineamientos para evitar los daños por incidentes mencionados:

8.1 Protección contra la exposición al agua (inundación)

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

8.2 Protección contra incendios

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

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

Se consideran los siguientes lineamientos para evitar los daños por incidentes mencionados:

- El equipo de reemplazo se ubica a una distancia segura para evitar el daño de un desastre que afecte el local principal.
- Se proporciona equipo contra incendios ubicado adecuadamente.
- Cuenta con respaldo de toda la información alojada en la nube esto a fin de asegurar que esta no se pierda en caso ocurra un desastre natural de gran envergadura.

Se describen los métodos de verificación de datos y antecedentes, así como los perfiles considerados para la selección tanto del personal que ocupa roles de confianza, incluyendo al responsable de Seguridad. Se detallan las responsabilidades del personal, así como los medios y mecanismos de comunicación y capacitación.

9. SEGURIDAD DE COMUNICACIONES Y REDES

Se describen las medidas de seguridad en el tema de comunicaciones y redes tanto a nivel interno como a nivel externo. También se establecen los requerimientos de seguridad que deben cumplirse cuando existe una relación con otros medios de comunicación. Cabe recalcar que los sistemas de registro son administrados por cada EC, por lo que la protección perimetral de redes corresponde a la infraestructura de cada EC.

El Jefe de sistemas garantiza la seguridad de los datos y los servicios conectados en las redes de la empresa, contra el acceso no autorizado consideran los siguientes lineamientos:

- Implementación de firewalls
- Sistemas de detección de intrusos
- Control de acceso y autenticación para acceder a la red
- Cifrado de información a través de SSL
- Establecimiento de políticas de contraseñas

10. MANTENIMIENTO DE EQUIPOS Y SU DESECHO

Se describen las normas y procedimientos que aseguran la correcta utilización de los equipos informáticos, así como su mantenimiento.
También se detallan las normas y procedimientos cuando el equipo es reemplazado, decomisado, manipulado, desechado (hardware y software). Descripción del tipo de personal que está autorizado para el mantenimiento del equipo.

10.1 Plan de mantenimiento preventivo: Este plan debe incluye actividades como limpieza de hardware, actualización de software, y revisión de hardware.

10.2 Política de actualización de software: Asegurarse de que todos los programas y sistemas operativos instalados en los equipos estén actualizados. Esto ayuda a garantizar la seguridad y estabilidad del sistema.

10.3 Política de uso adecuado de los equipos: Esta incluye recomendaciones como no comer o beber cerca de los equipos y evitar moverlos sin autorización para evitar daños innecesarios.

10.4 Respaldo de datos: Respaldo de datos semanales para evitar la pérdida de información en caso de fallos de hardware o software. Incluye la creación de copias de seguridad en un servidor o en un dispositivo de almacenamiento externo.

10.5 Política de desecho de equipos: Este proceso asegura de que los equipos sean desechados de manera segura y responsable al final de su vida útil, incluyendo la eliminación de datos personales y la disposición adecuada de los componentes.

10.6 Política de cumplimiento de las regulaciones ambientales: Es importante cumplir con las regulaciones ambientales locales y nacionales para el manejo y desecho de equipos electrónicos, ya que pueden contener sustancias tóxicas y peligrosas.

11. PROCEDIMIENTOS DE REGISTRO DE AUDITORÍAS

11.1. Tipos de eventos registrados

Los sistemas de información sensible son provistos por la EC, por lo que PERU MEDIA SECURITY SAC. en calidad Entidad de Registro de AC CAMERFIRMA PERU S.A.C. sólo puede acceder vía web. En este sentido, los logs de auditoría son administrados y definidos por la EC.

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

La ER de PERU MEDIA SECURITY SAC. genera reportes de los siguientes eventos:

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

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

11.2. Frecuencia del procesamiento del registro

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

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

11.3. Periodo de conservación del registro de auditorías

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

11.4. Protección del registro de auditoría

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

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

11.5. Copia de seguridad del registro de auditoría

Todas las solicitudes y contratos físicos son generados con copia y los documentos electrónicos tienen una copia por los Operadores de Registro. Las copias serán almacenadas en un lugar diferente como contingencia, protegidas contra acceso no autorizado por el Responsable de PERU MEDIA SECURITY SAC. en calidad Entidad de Registro de AC CAMERFIRMA PERU S.A.C.

11.6. Auditorías

Se establecen los objetivos de las auditorías. Su frecuencia y sistemas implicados. PERU MEDIA SECURITY SAC cuenta con los siguientes documentos relacionados a las auditorias:

- PROCEDIMIENTO DE AUDITORÍAS INTERNAS (PAI)
- FORMATO DE AUDITORÍA INTERNA

11.7. Notificación al titular que causa un evento

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

11.8. Valoración de vulnerabilidad

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

12. PLAN DE CONTINGENCIAS

Se describe la relación entre la valoración de riesgos y las acciones que se deben tomar como contingencia. PERU MEDIA SECURITY SAC cuenta con los siguientes documentos relacionados con la planificación de contingencias:

- MATRIZ DE RIESGO
- PLAN DE CONTINGENCIAS Y RECUPERACION DE DESASTRES

13.RESPONSABILIDADES

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

13.1 PERSONA DE CONTACTO

Nombre: Fiorella Favarato Hurtado

Correo electrónico: entidad.registro@perusecurity.com.pe

Teléfono: (51 1) 500 54 41

14.CONFORMIDAD

Este documento ha sido aprobado por el responsable de PERU MEDIA SECURITY SAC. en calidad Entidad de Registro de AC CAMERFIRMA PERÚ S.A.C. (Declaración de Practicas de Registro de la ER – 3.2.1) y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.