
# PLAN DE PRIVACIDAD V.1.0

Entidad de Registro Peru Media Security SAC

# PLAN DE PRIVACIDAD

## PERU MEDIA SECURITY SAC

| Generales | | | |
|---|---|---|---|
| **Propietario del Documento** | *Carlos Torres* | **Clasificación** | *Información Pública* |
| **Aprobado por:** | *Carlos Torres* | **Fecha aprobación** | *17/02/2023* |

| Historial de Versiones | | | |
|---|---|---|---|
| **Versión** | **Fecha** | **Autor** | **Resumen de Cambios** |
| *1.0* | *17/02/2023* | *Carlos Torres* | *Documento Inicial* |

## INDICE

# PLAN DE PRIVACIDAD

## 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. En tal sentido, cumple con los requisitos, procedimientos y auditorias exigidas en las Políticas de Certificación de AC CAMERFIRMA PERÚ, S.A.C.

## 2. PARTICIPANTES

- **Entidades de Certificación:** Entidades emisoras de certificados digitales, las cuales utilizan los servicios de registro de PERU MEDIA SECURITY SAC.

  Las jerarquías y Entidades de Certificación que gestiona AC CAMERFIRMA PERÚ, S.A.C. se encuentran definidas en el documento Declaración de Prácticas de Certificación. http://www.camerfirma.com.pe/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

  AC CAMERFIRMA PERÚ, S.A.C. gestiona los sistemas de registro que son utilizados por PERU MEDIA SECURITY SAC. para gestionar las solicitudes de los servicios de certificación digital, por lo que la responsabilidad de la disponibilidad y seguridad de estos sistemas depende de AC CAMERFIRMA PERÚ, S.A.C.

  AC CAMERFIRMA PERÚ, S.A.C. cuenta con las certificaciones ISO 27001 y se somete al proceso de acreditación de la Autoridad Administrativa competente, INDECOPI.

- **Entidades de Registro o Verificación**: PERU MEDIA SECURITY SAC. se somete al proceso de acreditación del INDECOPI, en calidad de Entidad de Registro o Verificación

PERU MEDIA SECURITY SAC. es ER de AC CAMERFIRMA PERÚ, S.A.C. Las comunicaciones entre PERU MEDIA SECURITY SAC. y AC CAMERFIRMA PERÚ, S.A.C. se realizan vía web de manera ininterrumpida, según los niveles de disponibilidad y recuperación brindados y declarados. La ER tiene procedimientos de contingencia para acceder a los sistemas en casos de corte del servicio de Internet. La disponibilidad del servicio web de registro es provisto por cada EC y es responsabilidad de la EC el mecanismo de contingencia utilizado.

- **Titulares de certificados:** El Titular del certificado es el responsable de los efectos jurídicos generados por la utilización de una firma digital. Tratándose de personas naturales, éstas son firmantes/titulares del certificado y de las firmas digitales que se generen a partir de aquél. En el caso de personas jurídicas, son éstas las titulares del certificado digital, y sus representantes o personas vinculadas, los suscriptores poseedor y responsable de la generación y uso de las claves, salvo el caso de las firmas digitales que generen a través de agentes automatizados para las cuales las personas jurídicas son titulares de los certificados y de las firmas digitales generadas a partir de éstos

- **Suscriptor:** Conforme a la IOFE, el Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.
  En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.
  En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad del suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad del suscriptor, para tales efectos, corresponde a la misma persona jurídica.

- **Tercero que Confía o Parte usuaria:** En esta Política se entiende por Parte Usuaria a la persona que voluntariamente confía en los certificados emitidos bajo esta política y se sujeta a lo dispuesto en ella por lo que no se requerirá acuerdo posterior alguno. La Parte Usuaria también puede denominarse como “Tercero que Confía”.

- Solicitante: Se entenderá por Solicitante, la persona natural o jurídica que solicita un certificado emitido bajo esta RPS. En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

## 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 PERÚ, S.A.C. 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 PERÚ, S.A.C.. |
| 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

El plan 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. OBJETIVO

El presente documento contiene los controles de privacidad de la información implementados por la Entidad de Registro de PERU MEDIA SECURITY S.A.C.

## 6. PERSONA DE CONTACTO

Nombre: Fiorella Favarato Hurtado

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

Teléfono: (51 1) 500 54 41

## 7. INFORMACIÓN RECOLECTADA Y PROTEGIDA

Como parte de las operaciones de registro, PERU MEDIA SECURITY SAC. en calidad de ER de AC CAMERFIRMA PERÚ, S.A.C. recolecta información de los suscriptores y titulares del siguiente tipo:

- Datos de identificación personal, incluyendo la fotografía que aparece en su documento de identidad.
- Contrato de solicitud de servicios.

# 8. TRATAMIENTO DE LOS DATOS PERSONALES

## 8.1 DATOS CONSIDERADOS PRIVADOS

Se considera como información privada, la siguiente:

- De conformidad con lo establecido por la Norma Marco sobre privacidad del APEC, se considera información personal, cualquier información relativa a un individuo identificado o identificable.
- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los usuarios de los servicios de certificación digital.
- En todos los casos, se determina que en el plan de Privacidad que el titular o suscriptor brinda su consentimiento para el tratamiento y almacenamiento de estos datos.

La información personal considerada como privada únicamente será divulgada en caso que exista consentimiento previo y por escrito firmado para tales efectos por el titular de dicha información o medio una orden judicial o administrativa que así lo determine.
Cualquier violación a la privacidad de esta información por parte del personal de la ER de PERU MEDIA SECURITY S.A.C. o de los terceros subcontratados, será sujeto de sanción.

## 8.2 DATOS CONSIDERADOS NO PRIVADOS

Se considera como información no privada, la siguiente:

- Información personal públicamente disponible.

En estos casos no será requerida autorización del usuario para dar publicidad a esta información.

# 9. PREVENCION DEL DAÑO DE DATOS PERSONALES

Se toman las siguientes medidas para prevenir el uso indebido de la información adoptando lo establecido por el APEC a través de la Norma Marco sobre Privacidad respecto de los principios que deben ser observados siempre que se realice algún tipo de labor o función

que involucre la recolección, posesión, procesamiento, uso, transferencia o revelación de información personal.

- Se restringe el acceso a los datos personales a los Operadores de Registro.
- Estos datos son protegidos contra acceso no autorizado.
- Se concientiza al personal para no divulgar o exponer de manera accidental datos personales de los usuarios
- Se implementan procedimientos para documentar las prácticas en lo que respecta a la información personal que se recolecta durante las actividades de operación, las mismas que deben informar sobre:
    i. El hecho de que se está recolectando información personal.
    ii. Los propósitos para los cuales se recolecta dicha información personal.
    iii. Los tipos de personas u organizaciones a las que dicha información podría ser revelada.
    iv. La identidad y ubicación del responsable de la información personal, Incluyendo información respecto a la forma de contactarlo en razón a sus prácticas y manejo de la información personal.
    v. Las opciones y medios que ofrece el responsable de la información personal a los individuos para limitar el uso y revelación, así como los mecanismos para el acceso y corrección de su información.
    vi. Se toman todos los pasos razonablemente necesarios, a fin de asegurar que se provee tal información, sea antes o en el mismo momento en que se está efectuando la recolección de la información personal. Caso contrario, deberá proveerse esta información tan pronto como sea factible.
- No es apropiado exigir que los responsables de la información personal provean información respecto a la recolección y uso de información que se encuentra públicamente disponible.

## 10. LIMITACIONES A LA RECOLECCIÓN

La recolección de información personal se encuentra limitada a la información que es relevante para el propósito para el cual se está recolectando y esta información es obtenida

de manera legal y apropiada, y, en la medida de lo posible, con la debida información o consentimiento del individuo al cual pertenece.

## 11. USO DE LA INFORMACIÓN PERSONAL

La información personal recolectada es usada en estricto cumplimiento de los propósitos de la recolección o aspectos relativos a los mismos, excepto:

- que exista consentimiento del individuo al que pertenece la información personal recolectada;
- que esta información es necesaria para la provisión de un servicio o producto solicitado por el individuo; o
- que la recolección está permitida por mandato de ley u otros instrumentos legales o exista algún tipo de pronunciamiento con efectos legales que lo autorizara.

## 12. ELECCIÓN

Cuando corresponda, los individuos cuentan con mecanismos claros, destacados, fáciles de comprender, accesibles y económicos que les permitan tomar decisiones sobre la recolección, uso y divulgación de su información personal.

Es posible que no sea necesario que los responsables de la información proporcionen estos mecanismos en los casos de recolección de información que ya sea de dominio público. Para verificar si este es el caso, se puede consultar el sitio web del Ministerio de Justicia y Derechos Humanos a través del siguiente enlace: https://prodpe.minjus.gob.pe/prodpe_web/BancoDato_verResultado

Es importante asegurarse de que los mecanismos proporcionados sean comprensibles para los individuos y les permitan ejercer control sobre su información personal de manera efectiva. De esta forma, se respeta la privacidad y se promueve el uso responsable y ético de la información personal recolectada.

## 13. INTEGRIDAD DE LA INFORMACIÓN PERSONAL

La información personal es exacta, completa y se mantiene actualizada en el extremo que fuere necesario para los propósitos de su empleo.

## 14. SALVAGUARDAS A LA SEGURIDAD

Los responsables de la información personal son capaces de proteger la información personal que mantienen, a través de salvaguardas apropiados contra riesgos tales como pérdida de la información o acceso indebido a la misma, así como contra la destrucción, uso, modificación o revelación no autorizada o cualquier otro abuso. Estas salvaguardas son proporcionales a la naturaleza y gravedad del daño potencial, la sensibilidad de la información y el contexto en que ésta es mantenida, y son sometidas a revisiones y reevaluaciones periódicas.

## 15. ACCESO Y CORRECCIÓN

Los individuos son capaces de:

- obtener del responsable de la información personal, la confirmación respecto a si mantiene o no información personal que les concierne;
- comunicar su información personal, luego de haber probado suficientemente su identidad, dentro de un periodo de tiempo razonable; por una tarifa, si es que la hubiera, la cual no debe ser excesiva; de una manera razonable; de un formato que sea razonablemente comprensible;
- y cuestionar la exactitud de la información que les concierne y de ser posible y apropiado, hacer que la información sea rectificada, completada, enmendada o borrada.

Se provee acceso y oportunidad para la corrección de la información, salvo cuando:

- la carga o costo de hacerlo sea indebido o desproporcional a los riesgos de la privacidad individual en el caso en cuestión;
- la información no pueda ser divulgada por razones legales o de seguridad o para proteger información comercial de carácter confidencial; o
- se podría violar la privacidad de la información de personas diferentes al individuo.

## 16. RENDICIÓN DE CUENTAS

PERU MEDIA SECURITY SAC está obligado a rendir cuentas sobre su cumplimiento con las medidas necesarias para dar efecto a los principios establecidos en el presente documento. Esto incluye la implementación adecuada de medidas de seguridad para proteger la información personal que manejan y asegurar que la transferencia de información, ya sea nacional o internacional, se realice de manera responsable y consciente.

Cuando se transfiera información personal, PERU MEDIA SECURITY SAC deberá obtener el consentimiento del titular o implementar medidas necesarias para garantizar que los receptores de la información protejan la información de manera consciente y responsable. Estas medidas deben ser proporcionales a la naturaleza de la información y el contexto en el que se maneja, y deben ser sometidas a revisiones y evaluaciones periódicas para garantizar su efectividad.

La rendición de cuentas y el cumplimiento responsable de los principios de protección de información son fundamentales para garantizar la privacidad y los derechos de los individuos y promover el uso ético y responsable de la información personal.

## 17. RESPONSABILIDADES

El responsable de Privacidad 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.

### 17.1 Persona de contacto

Nombre: Fiorella Favarato Hurtado

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

Teléfono: (51 1) 500 54 41

## 18. CONFORMIDAD

Este documento ha sido aprobado por el responsable de PERU MEDIA SECURITY SAC. en calidad de ER 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.