



Tinexta Infocert

PUB-2022-14-03
DECLARACIÓN DE PRÁCTICAS Y
POLÍTICA DEL SERVICIO DE VALOR
AÑADIDO – INFOCERT SIGN

Contenido

1. Tratamiento del documento	5
1.1. Control de actualizaciones	5
1.2. Control de cambios	5
1.3. Mantenimiento del documento	5
1.4. Validez	5
1.5. Tratamiento y confidencialidad	5
1.6. Distribución	5
2. Introducción	6
3. Objetivo del documento	6
4. Objeto de la acreditación	6
5. Definición y abreviaciones	7
6. Alcance	8
7. Participantes del SVA	8
7.1. Proveedores de servicios del SVA	8
7.2. Usuarios	8
7.3. Terceros que confían	8
8. Plataforma Infocert Sign	8
9. Responsabilidades	9
9.1. Responsabilidades de Camerfirma España	9
9.2. Responsabilidades de Camerfirma Perú	9
9.3. Responsabilidades de Tinexta Infocert	9
9.4. Responsabilidades del suscriptor del servicio	10
9.5. Responsabilidades del tercero que confía	10
9.6. Limitaciones de responsabilidades	10
10. Controles en las instalaciones, gestión y operaciones	11
10.1.	Cumplimiento
11	
10.2.	Controles físicos
11	
10.3.	Controles de procedimiento
14	
10.4.	Gestión de activos
14	
10.5.	Seguridad de los recursos humanos
14	

10.6.	Gestión de incidentes	
14		
10.7.	Continuidad del negocio después de un desastre	
14		
10.8.	Seguridad de la información – Antivirus/Software malicioso	
14		
10.9.	Ciclo de vida de la clave privada	
15		
10.10.	Controles de seguridad de la red	16
10.11.	Controles de ingeniería de los módulos criptográficos	16
10.12.	Controles de prueba de la posesión de la clave privada	16
10.13.	Autenticación	16
10.14.	Renovación de la clave	17
10.15.	Método de destrucción de la clave privada	17
10.16.	Evaluación de riesgos	17
10.17.	Procedimientos de auditoría de seguridad	17
10.18.	Controles de procedimiento	18
11.	Protección de datos personales	19
12.	Datos que se recogen	20
12.1.	Datos del cliente	
20		
12.2.	Datos de soporte	
20		
13.	Tratamiento de la información privada y confidencial	20
14.	Localización de los datos	21
15.	Política de reembolso	21
16.	Responsabilidad financiera, representaciones y garantías	21
17.	Enmendaduras	21
18.	Resolución de disputas	22
19.	Acuerdo íntegro, subrogación y divisibilidad	22
20.	Fuerza mayor y otras provisiones	22
21.	Tarifas	22
22.	Finalización del SVA	22
23.	Organización que administra la declaración de prácticas y política del SVA	23
24.	Publicación de la declaración de prácticas y otros documentos	23



Tinexta Infocert

PUB-2022-14-03
Página 4 de 24.

25.Conformidad con la ley aplicable	23
26.Bibliografía	23

1. Tratamiento del documento

1.1. Control de actualizaciones

VERSIÓN	FECHA	ELABORADO	APROBADO
1.0	Abril 2017	Ramiro Muñoz	Ramiro Muñoz
2.0	Abril 2024	Adrián Sastre	Adrián Sastre
3.0	Diciembre 2025	Adrián Sastre	Julio César Infante
4.0	Mayo 2025	Adrián Sastre	Julio César Infante

1.2. Control de cambios

DESCRIPCION DEL CAMBIO	APARTADOS QUE CAMBIAN RESPECTO A VERSIÓN ANTERIOR
AÑADIDO	
MODIFICADO	Actualización del nombre comercial del software.
ELIMINADO	

1.3. Mantenimiento del documento

Se requiere mantenimiento y/o revisión de este documento, cada vez que varíen algunas de las fases del proceso, las funciones del personal involucrado o las herramientas utilizadas en el mismo

1.4. Validez

Hasta su actualización.

Cualquier copia local se considera una **copia no controlada**. Es responsabilidad de quienes utilizan copias no controladas verificar su nivel de actualización.

1.5. Tratamiento y confidencialidad

Documento de uso público, pudiendo acceder a él todas las partes interesadas a través de la página web.

1.6. Distribución

Distribución pública.

2. Introducción

AC Camerfirma S.A. (Camerfirma España) es una empresa que fue creada en el año 1999 con domicilio en España, donde se establece como prestador de servicios de certificación al amparo de la LEY 59/2003, de 19 de diciembre, de firma electrónica en España. Asimismo desde la entrada en vigor del Reglamento (UE) N° 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, consta como Prestador Cualificado de Servicios de Confianza debidamente acreditado ante su órgano de Supervisión nacional y publicación de sus servicios de confianza cualificados en la TSL y EUTL.

Camerfirma España, como entidad líder española en la emisión de certificados empresariales en el sector privado tiene mucho que ofrecer en cuanto a conocimiento de esta tecnología a nivel europeo e incluso mundial. Camerfirma España desde el comienzo de su trayectoria como sociedad anónima en el año 2000, mantiene una estrecha relación con los mercados de Sudamérica y cuenta en su labor con numerosos proyectos de consultoría y de implantación de PKI con las Cámaras de Comercio sudamericanas.

En el año 2014, Camerfirma logró acreditarse como Entidad de Certificación en Perú a través de su sucursal CAMERFIRMA PERU S.A.C. (Camerfirma Perú). En el año 2017, se acreditó como prestador de servicios de emisión de Sellos de Tiempo (Timestamp), para brindar dichos servicios en Perú y dar cumplimiento a la regulación peruana establecida por la Autoridad Administrativa Competente (AAC), INDECOPI.

Como Prestador de Servicios de Valor Añadido – Sistema de Intermediación Digital, Camerfirma Perú dispone de la siguientes plataformas:

- **Infocert Sign:** Brindada y administrada por la empresa **Tinexta InfoCert**, la cual provee una plataforma de firma disponible desde la web, escritorio y dispositivos móviles. Facilitando el proceso de firma y la conservación de los documentos firmados. Asimismo, la infraestructura tecnológica y operativa de dicha aplicación es provista por **Tinexta InfoCert**.

La sucursal Camerfirma Perú es responsable de gestionar y mantener la acreditación de los servicios de Camerfirma España ante el INDECOPI, además de atender las solicitudes y reclamos por parte de sus clientes. En este sentido, nos referiremos a ambas de manera general como Camerfirma, a menos que sea necesario distribuir responsabilidades.

3. Objetivo del documento

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza Camerfirma Perú para la administración de sus servicios como Prestador de Servicios de Valor Añadido tipo Sistema de Intermediación Digital, en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Prestadores de Servicio de Valor Añadido (SVA)” establecida por el INDECOPI.

4. Objeto de la acreditación

El alcance de la acreditación del Sistema de Intermediación Digital de Camerfirma Perú cubre la Plataforma Infocert Sign en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)” establecida por el INDECOPI.

Camerfirma Perú es responsable de exigir el cumplimiento de los requisitos establecidos por la Autoridad Administrativa de la IOFE a sus proveedores y es responsable ante sus clientes de la calidad y seguridad de los servicios brindados.

Los proveedores por sí mismos no se encuentran amparados por la presente acreditación, sino solamente a través del control de calidad y seguridad que exige Camerfirma Perú a sus proveedores.

5. Definición y abreviaciones

DEFINICIÓN	ABREVIACIÓN
Prestador de Servicios de Valor Añadido	PSVA: Entidad que presta servicios que implican el uso de firma digital en el marco de la regulación establecida por la IOFE.
Servicios de Valor Añadido	SVA: Servicios compuestos por tecnología y sistemas de gestión que utilizan certificados digitales garantizando la autenticidad e integridad de los mismos durante su aplicación.
Declaración de Prácticas del Servicio de Valor Añadido	DPSVA: Procedimientos y controles que se adopta en cada etapa de los servicios y sistemas que se brinda a los clientes de acuerdo a lo establecido por INDECOPI.
Política de Servicios de Valor Añadido	Conjunto de reglas que indican el marco de la aplicabilidad de los servicios para una comunidad de usuarios definida.
Suscriptor	Entidad que requiere los servicios provistos por el SVA de Camerfirma Perú y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación electrónica generada durante la ejecución de los servicios de valor añadido, y que confía en la validez de las transacciones realizadas.
Titular	Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.
Roles de confianza	Roles que tienen acceso a la información crítica de las operaciones de Camerfirma.
ACC	Autoridad Administrativa Competente
IOFE	Infraestructura Oficial de Firma Electrónica
PSC	Prestador de Servicios de Certificación
CRL	Lista de Certificados Revocados
CPD	Centro de Procesamiento de Datos
SID	Sistema de Intermediación Digital
RGPD	Reglamento General de Protección de Datos
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la protección de la Propiedad Intelectual

6. Alcance

El presente documento es de carácter público y se encuentra dirigida a todas las personas naturales y jurídicas, solicitantes, clientes, terceros que confían y público en general.

7. Participantes del SVA

7.1. Proveedores de servicios del SVA

Los proveedores de servicios del SVA son terceros que prestan sus servicios tecnológicos y/o infraestructura a Camerfirma Perú y así poder garantizar:

- La protección de datos personales de los clientes.
- La continuidad del servicio de los SVA.
- La seguridad, disponibilidad de las operaciones de los SVA.

Los SVA que ofrece Camerfirma Perú, son provistos por sus proveedores de infraestructura tecnológica y operativa.

7.2. Usuarios

Camerfirma Perú brinda sus servicios de SVA a personas jurídicas del sector público y privado.

7.3. Terceros que confían

Son todas aquellas personas naturales y jurídicas que requieren evaluar la validez de una transacción electrónica, un documento firmado o un certificado utilizado o generado en los servicios brindados por Camerfirma Perú.

8. Plataforma Infocert Sign

Camerfirma Perú ofrece el siguiente Servicio de Sistema de Intermediación Digital:

- Infocert Sign es una plataforma de firma disponible desde la web, escritorio y dispositivos móviles.
- Infocert Sign cuenta con una interfaz simple e intuitiva, facilitando el proceso de firma. La conservación de documentos firmados está garantizada asegurando la compatibilidad con cualquier dispositivo digital.

Proporciona a los usuarios las funciones de creación y gestión de procesos de autorización típicas de los secretarios, las características de aprobación y firma que suelen utilizar los gestores y las funciones de configuración de usuarios y políticas de firma, típicas de un administrador de sistema.

- Secretary (Secretario): Crea y activa los procesos de firma que implican a uno o más gestores.
- Manager (Gestor): Recibe notificaciones sobre los procesos de firma en los que está involucrado.

- **Administrator (Administrador):** Crea y/o modifica los usuarios asociándolos a diferentes métodos de firma, y crea políticas de firma para la gestión de determinados procesos.

El expediente utilizado en los procesos de autorización puede estar compuesto por uno o más documentos, en cada uno de los cuales varios gestores pueden realizar diferentes acciones (vista, inicial, firma, etc.).

Seleccionando los campos individuales en la página de envío, es posible especificar:

- Los gestores implicados (destinatarios) y el proceso de autorización.
- Los documentos que componen el expediente y las acciones solicitadas.
- Los mensajes para enviar a los destinatarios.
- El nivel de privacidad del expediente.

También es posible seleccionar una política de firma predefinida. Por Política de Firma se entiende un conjunto de reglas que determina automáticamente, en base a uno o más atributos del documento, qué gestores deben firmar el documento y la secuencia en la que sus firmas deben aplicarse al documento. Cada documento puede leerse íntegramente y firmarse electrónicamente, cuando proceda. Los documentos antiguos, que hayan sido archivados por el secretario, seguirán estando siempre accesibles a través del Archivo de Documentos.

La aplicación está disponible para dispositivos iOS y Android.

Cada documento puede consultarse en su totalidad, y, finalmente, ser firmado digitalmente.

9. Responsabilidades

9.1.Responsabilidades de Camerfirma España

Camerfirma exige y supervisa que sus proveedores realicen la implementación de los controles de seguridad y privacidad necesarios para proteger la información de sus clientes, conforme a lo declarado en el presente documento.

9.2.Responsabilidades de Camerfirma Perú

La sucursal Camerfirma Perú es responsable de representar a Camerfirma España para la gestión y mantenimiento de la acreditación de los servicios de Camerfirma España ante el INDECOPI, además de atender las solicitudes y reclamos por parte de sus clientes.

9.3.Responsabilidades de Tinexta Infocert

En calidad de proveedor de infraestructura tecnológica y operativa, Tinexta InfoCert es responsable de la implementación de los controles de seguridad y privacidad necesarios para proteger la información de sus clientes, conforme a lo declarado en el presente documento.

9.4. Responsabilidades del suscriptor del servicio

El suscriptor es responsable de no reproducir, total o parcialmente, bajo ninguna forma de soporte, la información contenida en la aplicación de la plataforma.

Los servicios prestados por la plataforma, así como la información contenida en la misma, incluida la base de datos, sólo se podrá utilizar para el uso propio de la plataforma.

El usuario no podrá revender dichos servicios e información ni cederlos (tampoco gratuitamente) a terceros bajo ningún concepto. Está expresamente prohibido almacenar datos, direcciones, teléfonos o e-mails en cualquier tipo de soporte, ya sea físico o informático, y utilizarlo para fines distintos a los contemplados en este contrato, así como la revelación de los mismos a cualquier tercero.

- A no extraer o reutilizar datos fuera de lo expresamente autorizado por cada tipo de servicio contratado.
- No introducir información ficticia, contraria a la ley o a las buenas costumbres.
- Mantener la ética profesional en su relación con otras empresas usuarias de la Plataforma y con CAMERFIRMA.
- En caso de formalizar un contrato, realizar cualquier tipo de actuación u operación a través de los servicios ofrecidos por la Plataforma con CAMERFIRMA y/o con otros usuarios, se atenderá y respetará la normativa sobre el uso del servicio correspondiente que se publica en la web y la ética y buena fe contractual.

Cualquiera de los servicios facilitados por CAMERFIRMA a través de la plataforma no eximirá al Usuario de su responsabilidad por el cumplimiento de todas las obligaciones que se establecen legalmente en materia administrativa, fiscal, laboral, penal, civil y mercantil.

9.5. Responsabilidades del tercero que confía

El tercero que confía en los documentos generados por los servicios de la plataforma es responsable de lo siguiente:

- Verificar la validez de los certificados digitales de los documentos o información procesada por los sistemas de intermediación digital como Producto.
- Tomar en cuenta cualquier limitación en el uso de los sistemas considerados en la DPSVA.
- Tomar en cuenta cualquier otra precaución prescrita en los acuerdos u otra parte

9.6. Limitaciones de responsabilidades

Camerfirma Perú no será responsable cuando se encuentre ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por los usuarios o por los Terceros, o cualquier otro caso de fuerza mayor.
- Por el uso indebido o fraudulento del directorio de certificados y CRL's (Lista de Certificados Revocados) emitidos por la Autoridad de Certificación.
- Por el uso indebido de la información contenida en el Certificado o en la CRL.
- Por el contenido de los mensajes o documentos firmados o encriptados mediante los certificados.

- En relación a acciones u omisiones del Solicitante y Suscriptor:
- Falta de veracidad de la información suministrada para emitir el certificado.
- Retraso en la comunicación de las causas de suspensión
- Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- Uso del certificado fuera de su periodo de vigencia, o cuando se notifique la revocación de este.
- Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y en particular, superar los límites que figuren en el certificado digital en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas.
- En relación con acciones u omisiones del tercero que confía en el certificado: o falta de comprobación de las restricciones que figuren en el certificado digital en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o falta de comprobación de la pérdida de vigencia del certificado digital publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma digital

10. Controles en las instalaciones, gestión y operaciones

10.1. Cumplimiento

Los Servicios de Valor Añadido brindados por Camerfirma Perú cuentan con controles de seguridad física (ambiente físico, redes, sistemas, entre otros) y son sometidos a auditorías de terceros por parte de auditores reconocidos internacionalmente y autorizados.

10.2. Controles físicos

El Centro de Datos Principal como el Centro de Datos Secundario se encuentran en territorio italiano y están organizados y administrados de conformidad con la regulación europea sobre las medidas de seguridad.

Las medidas adoptadas proporcionan garantías de seguridad adecuadas con respecto a:

- Características del edificio y la construcción.
- Sistemas de prevención de robo de activos y pasivos.
- Control de acceso físico.
- Suministro de energía eléctrica y aire acondicionado.
- Protección contra incendios.
- Protección contra inundaciones.
- Métodos de almacenamiento de soporte magnético.
- Sitios de almacenamiento de soporte magnético.

Las medidas adoptadas proporcionan garantías de seguridad adecuadas con respecto a:

- Características del edificio y la construcción.
- Sistemas de prevención de robo de activos y pasivos.

- Control de acceso físico.
- Suministro de energía eléctrica y aire acondicionado.
- Protección contra incendios.
- Protección contra inundaciones.
- Métodos de almacenamiento de soporte magnético.
- Sitios de almacenamiento de soporte magnético

10.2.1.Ubicación de los centros de datos

Los centros de datos de Tinexta Infocert están ubicados en Italia y cuentan con áreas protegidas con los más altos niveles de seguridad, tanto físicos como lógicos.

- CPD InfoCamere: Corso Stati Uniti, 14 (Padova) - Italia
- CPD Wiit: Via Muzio Attendolo detto Sforza, 7 (Milán) - Italia

10.2.2.Acceso físico

El acceso al centro de datos está regulado por los procedimientos de seguridad de Tinexta InfoCert.

Hay un área de bunker dentro del Centro de Datos donde se ubican los sistemas de CA y para los cuales existe otro nivel de seguridad necesario.

10.2.3.Planta eléctrica y aire acondicionado

El sitio que alberga los centros de datos de Tinexta Infocert en Italia, aunque no están certificados, tienen las características de un centro de datos de nivel TIER 3.

Las salas técnicas están equipadas con un sistema de suministro de energía eléctrica diseñado para evitar cualquier anomalía que se pueda presentar.

La fuente de alimentación del sistema incluye los más moderna tecnología con miras a aumentar fiabilidad y garantizar la redundancia en las funciones esenciales para los servicios prestados.

La infraestructura de suministro de energía eléctrica incluye:

- UPS, equipados con acumuladores de CA.
- Voltaje de CA disponible (220 – 380 V CA).
- Armarios de fuente de alimentación redundantes con líneas protegidas.
- Servicio de generador de emergencia.
- Sistema de conmutación automática y sincronización entre generadores, red y baterías (STS)

Cada gabinete tecnológico instalado en el Centro de Datos utiliza dos líneas eléctricas que garantizan HA en caso de que una de las dos líneas disponibles se interrumpa.

El gabinete tecnológico se monitorea remotamente, se realizan controles continuos en el estado de las líneas eléctricas (encendido / apagado) y la energía eléctrica absorbida (cada carga no debe exceder el 50% de la capacidad de la línea).

El área técnica se mantiene normalmente entre 20° y 27° con un nivel de humedad relativa entre 30% y 60%.

Las plantas están equipadas con baterías de condensación, sistema de recolección y drenaje y controlado por sondas anti – inundación.

Todo el condicionamiento del sistema es servido por generadores de emergencia en caso de corte de energía.

La capacidad de enfriamiento del gabinete es garantizada con una carga máxima prevista de 10kw y un máximo de 15Kw.

10.2.4.Prevencción y protección contra inundaciones

El área donde se encuentran los centros de datos de Tinexta Infocert, no presenta riesgo ambiental.

Cuando se diseñó el edificio, se tomaron medidas específicas para aislar los edificios del peligro potencial, como los que albergan el generador eléctrico y planta de calefacción central.

El área que alberga el equipo está en la planta baja en una posición elevada en comparación con la carretera.

10.2.5.Prevencción y protección contra incendios

El centro de datos tiene un sistema de detección de humo administrado por una estación de energía analógica referida como NOTIFICADOR, con sensores ópticos colocados en la sala y el techo y sensores de muestra de aire instalados subterráneamente en los conductos de aire.

El sistema automático de detección de incendios está conectado a NAFS 125 automático y gas ecológico PF23, en ciertas salas cuentan con sistemas de extinción por aspersión.

Si los dos detectores se disparan en la misma área, la descarga de extinción se aplica área afectada. Cada compartimiento de extinción de incendios tiene una planta específica.

También hay extintores portátiles que cumplen con las regulaciones y leyes vigentes.

10.2.6.Medios de almacenamiento

En lo que respecta a la plataforma de almacenamiento, la solución proporciona el uso de Net App (FAS 8060) sistemas para la parte NAS.

Para la parte SAN, en cambio se utiliza una infraestructura basa en tecnología EMC2 que incluye VNX 7600, VNX 5200 y XtremIO, administrado a través del almacenamiento VPLEX como capa de virtualización.

Esta infraestructura se gestiona a través de ViPR.

10.2.7.Eliminación de residuos

Tanto Camerfirma como Tinexta Infocert cuenta con la certificación ISO 14001 para la gestión ambiental sostenible de su producción que incluye el reciclaje y la eliminación sostenible de residuos.

En cuanto al contenido de TI de electrónica los residuos están relacionados, todos los medios antes de su eliminación se limpian de acuerdo con lo establecido en los procedimientos, es decir, el uso de empresas de saneamiento certificadas.

10.2.8.Copia de seguridad fuera del sitio

Las copias de seguridad se realizan en el centro de datos secundario, con un dispositivo EMC Data Domain 4200.

10.3.Controles de procedimiento

10.3.1.Roles clave

Los roles clave los desempeñan personas con experiencia, profesionalismo y conocimientos técnicos necesarios y habilidades legales, que se verifican de manera anual.

10.4.Gestión de activos

Los activos son contabilizados y son asignados a un propietario. Se mantiene un inventario de los principales activos de hardware utilizados en los servicios que componen el SID.

10.5.Seguridad de los recursos humanos

El personal y los proveedores de Camerfirma Perú son requeridos a completar satisfactoriamente una verificación de antecedentes estándar como parte del proceso de su contratación a fin de validar el empleo anterior, educación, antecedentes penales.

El personal de los proveedores de Camerfirma Perú es requerido a tomar algún tipo de formación que se considere conveniente a los servicios que prestan y el rol que desempeñan.

10.6.Gestión de incidentes

Como parte de sus servicios, Camerfirma Perú realiza los procesos de detección e investigación de todas las incidencias reportadas por sus clientes.

10.7.Continuidad del negocio después de un desastre

Camerfirma Perú restablecerá los servicios críticos de los SVA dentro de las 24 horas posteriores a un desastre o emergencia imprevista, de acuerdo con el documento "Continuidad del negocio".

10.8.Seguridad de la información – Antivirus/Software malicioso

Los sistemas de los proveedores de Camerfirma Perú cuentan con software antivirus para asegurar la protección contra software malicioso común.

10.9.Ciclo de vida de la clave privada

10.9.1.Controles de desarrollo del sistema

Camerfirma Perú emplea sistemas fiables y productos con un nivel de seguridad suficiente para la funcionalidad y seguridad que se exige.

10.9.2.Gestión de seguridad

Camerfirma Perú realiza los esfuerzos que razonablemente estén a su alcance para confirmar que los procedimientos administrativos y de gestión son aplicados, son adecuados y se corresponden con los estándares reconocidos.

En particular:

- Camerfirma Perú es responsable por todos los aspectos relativos a la prestación de servicios de certificación, incluso si algunas de sus funciones han sido subcontratadas con terceras partes. Las responsabilidades de las terceras partes serán claramente definidas por Camerfirma Perú en los acuerdos concretos que Camerfirma Perú suscriba con esas terceras partes para asegurar que éstas están obligadas a implementar cualquier control requerido por Camerfirma Perú. Camerfirma Perú es responsable por la revelación de prácticas relevantes.
- Camerfirma Perú desarrolla las actividades necesarias para la formación y concienciación de los empleados en materia de seguridad.
- La información necesaria para gestionar la seguridad de Camerfirma Perú debe mantenerse en todo momento. Cualquier cambio que pueda afectar al nivel de seguridad establecido deberá ser aprobado por el foro de gestión de Camerfirma Perú.
- Los controles de seguridad y procedimientos operativos para las instalaciones de Camerfirma Perú, sistemas e información necesarios para los servicios de certificación son documentados, implementados y mantenidos.

Camerfirma Perú realiza los esfuerzos que razonablemente estén a su alcance para confirmar que se mantenga la seguridad de información cuando la responsabilidad respecto a funciones de Camerfirma Perú haya sido subcontratada a otra organización.

10.9.3.Depósito de la clave privada

La clave privada de Camerfirma Perú es almacenado en un medio seguro protegido criptográficamente y al menos bajo un control dual.

En ningún caso Camerfirma Perú podrá almacenar la clave privada de firma del suscriptor (key escrow).

10.9.4.Copia de seguridad de la clave privada

Camerfirma Perú realiza una copia de backup de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de esta de acuerdo con el apartado anterior.

Las copias de las claves privadas de los suscriptores se registrarán por lo dispuesto en el punto anterior

10.9.5.Gestión del ciclo de vida del hardware criptográfico

Camerfirma Perú realiza los esfuerzos que razonablemente estén a su alcance para confirmar la seguridad del hardware criptográfico a lo largo de su ciclo de vida. En particular, que:

- el hardware criptográfico de firma de certificados no se manipula durante su transporte.
- el hardware criptográfico de firma de certificados no se manipula mientras está almacenado.
- el uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.
- el hardware criptográfico de firma de certificados está funcionando correctamente; y
- la clave privada de firma de Camerfirma Perú almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo

10.9.6.Evaluación de la seguridad del ciclo de vida

La evaluación de la seguridad del ciclo de vida está supeditada a la metodología interna de Camerfirma Perú.

10.10.Controles de seguridad de la red

Los sistemas y redes de Tinexta Infocert están conectados a Internet de manera controlada por sistemas de firewall, que le permiten dividir la conexión en áreas progresivamente más seguras: red de Internet, DMZ (zona desmilitarizada) o perímetro de redes, redes internas.

10.11.Controles de ingeniería de los módulos criptográficos

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 3 de FIPS 140-2 o por un nivel de funcionalidad y seguridad equivalente.

10.12.Controles de prueba de la posesión de la clave privada

El envío del CSR por el suscriptor, constituye la garantía de que el suscriptor está en posesión de clave privada. Aunque Camerfirma Perú puede generar la clave privada y entregársela al suscriptor por un medio seguro.

10.13.Autenticación

10.13.1.Autenticación de la identidad de una organización

Los Certificados emitidos bajo la presente Política identifican a una entidad, por lo que se comprobará la identidad de esta y de los solicitantes mediante el acceso a bases de datos externas.

10.13.2.Requisitos de comprobación de CRL

Los Terceros que confían deberán comprobar el estado de los certificados en los cuales va a confiar, debiendo comprobar en todo caso la última CRL emitida.

10.13.3.Disponibilidad de comprobación on-line de la revocación

Se proporcionará un servicio on-line de comprobación de revocaciones, el cual estará disponible las 24 horas del día los 7 días de la semana. En caso de fallo del sistema, del servicio o de cualquier otro factor que no esté bajo el control de Camerfirma Perú.

Camerfirma Perú deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

10.14.Renovación de la clave

Camerfirma Perú debe informar al Firmante/Suscriptor antes de renovar de los términos y condiciones que hayan cambiado respecto de la anterior emisión. Camerfirma Perú en ningún caso emitirá un nuevo certificado conteniendo la anterior clave pública del Firmante/Suscriptor. (Reutilización de la clave).

10.15.Método de destrucción de la clave privada

Camerfirma Perú debe realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada de la CA no será usada una vez finalizado su ciclo de vida.

Todas las copias de la clave privada de firma de la CA deberán ser destruidas o deshabilitadas de forma que la clave privada no pueda ser recuperada.

10.16.Evaluación de riesgos

Anualmente, los proveedores de Camerfirma Perú llevan a cabo un análisis de riesgo de seguridad de la información. El análisis incluye:

- La identificación de las amenazas relacionadas con los procesos de intercambio de información y firma digital.
- Una estrategia aprobada de gestión para la mitigación de las amenazas significativas identificadas.

10.17.Procedimientos de auditoría de seguridad

10.17.1.Tipo de eventos registrados

Camerfirma Perú registra y guarda los logs de todos los eventos relativos al sistema de seguridad del SVA, incluyendo:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la SVA a través de la red.
- Intentos de accesos no autorizados a la red interna de la SVA.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la SVA
- Encendido y apagado de la aplicación de la SVA.
- Cambios en los detalles de la SVA y/o sus claves.
- Cambios en la creación de perfiles de certificados.

- Generación de claves propias.
- Eventos del ciclo de vida del certificado.
- Eventos asociados al uso del módulo criptográfico de la SVA.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de suscriptor, si se gestiona esa información.
- Posesión de datos de activación, para operaciones con la clave privada de las SVA

10.17.2.Frecuencia de registros de auditoría

Se revisarán los logs de auditoría por parte de la Autoridad Administrativa Competente de manera anual y en todo caso cuando se produzca una alerta del sistema.

10.17.3.Periodo de conservación de los registros de auditoría

Se almacena la información de los logs de auditoría durante 15 años para garantizar la seguridad del sistema.

10.17.4.Protección de los registros de auditoría

Los logs de los sistemas son manejados en todo momento por el personal autorizado.

10.17.5.Sistemas de recogida de información de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo.

10.18.Controles de procedimiento

10.18.1.Roles de confianza

Los roles de confianza de Camerfirma Perú son los que se describen en el “Diagrama Organizacional”, garantizando la segregación de funciones.

Los roles de confianza son:

- Responsable del SID
- Responsable de seguridad de la información y privacidad de datos personales
- Proveedores de servicios de certificación digital
- Equipo de desarrollo
- Equipo de soporte y atención de incidentes
- Auditor interno

10.18.2.Identificación y autenticación por rol

Cada rol solo controla los activos necesarios, asegurando así que ninguna persona acceda a recursos no asignados.

11. Protección de datos personales

Como Cliente o usuario de la Plataforma “Infocert Sign” de gestión de evidencias electrónicas, verán sus datos tratados por CAMERFIRMA PERÚ S.A.C. como “encargado” y por TINEXTA INFOCERT S.P.A como “sub – encargado” del tratamiento, conforme se indica a continuación:

EPÍGRAFE	INFORMACIÓN SOBRE PROTECCIÓN DE DATOS PERSONALES PARA USUARIOS DE LA PLATAFORMA INFOCERT SIGN
Responsable del tratamiento	El cliente
Encargados del tratamiento	CAMERFIRMA PERÚ S.A.C. TINEXTA INFOCERT S.p.A.
Afectados	Usuarios de la aplicación y titulares de certificado digital.
Tipos de datos	- De identificación del usuario: nombre, apellidos, email, NIF o equivalente, departamento, cargo, organización y otros, fecha y lugar de nacimiento. - De contacto del usuario: email, teléfono y otros. - Los incluidos en los certificados: nombre, apellidos, NIF, organización, cargo y otros (del usuario de la aplicación o de terceros). - Del uso del servicio por el usuario y de registro de auditoría: IP, URL, fecha de operación y otros. - Los contenidos en las evidencias. En caso de activación del servicio opcional de firma grafométrica: - Datos biométricos.
Tratamientos	Los tratamientos que se realizan sobre los datos son los que resulten necesarios para la prestación del servicio ofrecido al CLIENTE, entre otros: - Almacenamiento - Uso de los certificados - Gestión del servicio - Consultas realizadas por el usuario y por los usuarios administradores - Exportación de datos (listados) por el usuario y por los usuarios administradores - Registro y consulta de actividad de uso (informes y auditorías) - Elaboración de listados e informes para la gestión del servicio por parte del PROVEEDOR

	• Envío de avisos y comunicaciones relacionadas con la prestación del servicio En caso de activación del servicio opcional de firma grafométrica: • recopilación, registro, organización, almacenamiento, tratamiento, recuperación, utilización, borrado. El Sub-encargado TINEXTA INFOCERT, S.P.A, en este servicio, utiliza servicios internos de almacenamiento situados en Padova/Milán (Italia).
Finalidades	Crear cuentas de usuarios y recoger las evidencias electrónicas de las operaciones realizadas con los documentos enviados a través de la aplicación.

12. Datos que se recogen

12.1. Datos del cliente

Como se describe en los contratos de los clientes, Camerfirma Perú sólo utiliza los datos de los clientes para proporcionar los Servicios contratados.

12.2. Datos de soporte

Es la información que los clientes entregan cuando hacen una solicitud de asistencia, incluyendo información sobre el hardware, software, y otros detalles relacionados con el incidente de soporte.

El servicio de soporte puede ser provisto a través del teléfono, correo electrónico o chat en línea.

13. Tratamiento de la información privada y confidencial

Camerfirma Perú no revela datos de clientes o datos de soporte fuera de Camerfirma Perú o sus proveedores con excepción de lo que el cliente solicite expresamente en su contrato.

La información proporcionada a los proveedores se hace restringiendo el acceso a la información del cliente al mínimo que sea necesario para cumplir con el servicio contratado. Los proveedores están obligados a mantener la confidencialidad de la información los clientes de Camerfirma Perú y se les prohíbe utilizar dicha información para ningún fin distinto de aquel para el que están contratados.

No se revelan datos de los clientes a un tercero con excepción de lo que el cliente solicite a menos que sea requerido por la ley.

Asimismo, como parte de la Prestación del Servicio de Valor Añadido mantiene de manera confidencial la siguiente información:

- Material comercialmente reservado de los PSCs, de los suscriptores de la empresa y de los terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual;
- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores de empresa y los terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- Se debe asegurar la reserva de toda información que mantiene, la cual pudiera perjudicar la normal realización de sus operaciones.
- Se permite la publicación de información respecto a la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión.
- La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían

14.Localización de los datos

Los datos de sus servicios pueden ser transferidos, almacenados y procesados en Perú o cualquier otro país en el que Camerfirma Perú o sus proveedores de servicios tengan instalaciones, siempre que sea establecido en el contrato con el proveedor y debidamente informado a los usuarios.

15.Política de reembolso

Las condiciones de reembolso serán definidas con cada cliente en los respectivos contratos, de acuerdo con el tipo de servicio, contrato y cliente.

16.Responsabilidad financiera, representaciones y garantías

La cobertura de seguro, las provisiones de garantía y responsabilidad, así como las indemnizaciones son definidas en los contratos con los clientes, de acuerdo al tipo de servicio, contrato y cliente.

Los seguros son provistos por Camerfirma Perú y dan cobertura a sus servicios.

17.Enmendaduras

Los procedimientos para la resolución de enmendaduras podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo con el tipo de servicio, contrato y cliente.

18.Resolución de disputas

Los procedimientos para la resolución de disputas podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo con el tipo de servicio, contrato y cliente.

19.Acuerdo íntegro, subrogación y divisibilidad

Las cláusulas de acuerdo íntegro, subrogación y divisibilidad podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo con el tipo de servicio, contrato y cliente.

20.Fuerza mayor y otras provisiones

Las cláusulas de fuerza mayor y otras provisiones aplicables a la entrega de los servicios de valor añadido podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo con el tipo de servicio, contrato y cliente.

21.Tarifas

Las tarifas por los servicios serán definidas en los contratos con las organizaciones clientes, de acuerdo con el tipo de servicio, contrato y cliente.

22.Finalización del SVA

Antes de que el SVA termine sus servicios, o que la empresa que lo gestiona deje de existir, realizará las siguientes medidas:

- De ser aplicable, con 30 días de anticipación se informará a todos clientes y suscriptores, la finalización de las operaciones del SVA.
- Se pondrá a disponibilidad de todas las organizaciones cliente la información concerniente a su terminación y las limitaciones de responsabilidad.
- Se concluirán los permisos de autorización de funciones de todos los subcontratados para actuar en nombre del SVA.
- Se mantendrán o transferirán a los terceros que confían sus obligaciones de verificar los documentos generados.

Las provisiones sobre término y terminación, así como las cláusulas de supervivencia serán definidas en los contratos de los clientes. Además, las modificaciones realizadas deben ser comunicadas a los suscriptores, titulares y terceros que confían.

23.Organización que administra la declaración de prácticas y política del SVA

Camerfirma Perú administra los documentos de Declaración de Prácticas del SVA, y todos los documentos normativos del SVA.

Para cualquier consulta contactar:

- Nombre: Departamento de Compliance interno de Camerfirma.
- Dirección de correo electrónico: compliance@camerfirma.com

24.Publicación de la declaración de prácticas y otros documentos

La Declaración de Prácticas de los Servicios de Valor Añadido de Camerfirma Perú, así como la Política y Plan de Privacidad, la Política de Seguridad y otra documentación relevante que contiene información sobre los servicios de certificación digital acreditados por INDECOPI son publicados en la siguiente dirección:

<https://www.camerfirma.com.pe/>

Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones de los documentos serán publicadas en la página web. La auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

25.Conformidad con la ley aplicable

Camerfirma Perú es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales – Ley 27269, para el reconocimiento legal de los servicios de valor añadido emitidos bajo las directrices definidas en el presente documento.

26.Bibliografía

- Guía de Acreditación de Prestadores de Servicios de Valor Añadido, INDECOPI
- Ley de Firmas y Certificados Digitales –Ley 27269
- Decreto Supremo 052-2008
- Decreto Supremo 070-2011
- Decreto Supremo 105-2012



Tinexta Infocert

think next,
trust now