Camerfirma PERÚ

Tinexta Infocert

PUB-2025-14-02
POLÍTICA DE SEGURIDAD INFOCERT SIGN

Contenido

1. Tratamiento del documento

1.1. Control de actualizaciones

VERSIÓN	FECHA	ELABORADO	APROBADO
1.0	12/06/2020	Innovate DC	Ramiro Muñoz
2.0	01/07/2025	Adrián Sastre	Dpto. Jurídico
3.0	18/05/2026	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 Reglamente (UE) N o 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 siguiente plataforma:

- **Infocert Sign**: Brindada y administrada por la empresa Tinexta InfoCert, la cual provee una plataforma de firma y marca de tiempo 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. Objeto 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 las siguientes plataformas:

- **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. Definiciones y abreviaciones

Definiciones y abreviaciones	
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.
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
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la protección de la Propiedad Intelectual

6. Alcance

El presente documento es de cumplimiento obligatorio por los empleados y los proveedores de los Servicios de Valor Añadido del Sistema de Intermediación Digital de Camerfirma Perú.

7. Política de seguridad

Camerfirma Perú implementa los controles necesarios para garantizar la confiabilidad y autenticidad de la firma digital en los Servicios de Valor Añadido. Esto implica controles de acceso a las aplicaciones, verificación de estado del certificado, generación de registros de eventos y transacciones, evaluación de vulnerabilidades de las aplicaciones y asimismo se somete ante el INDECOPI, en su calidad de Autoridad Administrativa Competente de la IOFE, a auditorías anuales.

8. Controles en las instalaciones, gestión y operacionales

8.1. 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 de manera anual.

8.2. Infraestructura y seguridad de los centros de datos

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 italiana y europea sobre las medidas de seguridad.

8.2.1. Ubicación de los centros de datos

El Centro de datos de Tinexta InfoCert está ubicado en la sede operativa de Corso Stati Uniti 14, 35127 – Padua.

El Centro de datos secundario, se encuentra en Milán (Via Muzio Attendolo 7) y actualmente se encuentra conectado al Centro de datos mencionado anteriormente a través de un enlace MPLS dedicado y protegido a 1 Gbps actualizable hasta 100 Gbps.

8.2.2. Red

El Centro de datos de Tinexta InfoCert utiliza una conexión Gigabit Ethernet dual de fibra óptica en redes troncales operado por dos proveedores diferentes. Ambas líneas aseguran una velocidad máxima de 10 Gb / s. Estas conexiones están certificadas en POP separados, con rutas físicas redundantes e interfaz equipo.

8.2.3. Sistema de monitoreo

Existe una estructura de Service Desk externalizada, que actúa como SPOC (Punto único de contacto) para problemas relacionados con la prestación de servicios.

Las consolas operativas del centro de datos están controladas por operadores de nivel superior H24x7. Para cada servidor individual bajo control, las consolas de monitorización reportan toda la información recopilada por los agentes que requieran la atención de los operadores. En caso de anomalías obvias en las consolas, los operadores de segundo nivel reciben alertas incluso fuera del horario de oficina. Se prevén operadores equipados que puedan realizar intervenciones remotas.

8.2.4. Descripción de los procesos de seguridad

Seguridad física y medioambiental

La ubicación del edificio no presenta riesgos ambientales debido a su proximidad a Instalaciones "peligrosas". Durante el diseño del edificio, se tomaron medidas apropiadas para aislar habitaciones potencialmente peligrosas, como las que contienen el grupo electrógeno y la calefacción de planta.

Estas salas están equipadas con los equipos y accesorios de control y seguridad necesarios por la normativa vigente.

El edificio ofrece numerosas soluciones para aumentar su seguridad. Dentro de la caseta de vigilancia hay un sistema de control en el cual los sistemas actuales son monitoreados y supervisados (sistema de alarma antirrobo, circuito cerrado de televisión, sistema de control de acceso).

El Centro de Datos principal, consta de dos edificios:

- El primer edificio contiene principalmente oficinas.
- El segundo el edificio alberga las áreas donde se realizan las actividades "sensibles".

Sistema anti-intrusos internos y externos

La defensa del perímetro externo del edificio está garantizada por:

- Una puerta que marca todo el perímetro.
- Control perimetral del edificio y acceso con sistema de circuito cerrado de televisión.
- Control de personal 24x7.
- Bitácora de recepción para la gestión de acceso.
- Torno de tres brazos frente a la sala de vigilancia.
- Las zonas internas son monitoreadas por:
    - Sensores piezodinámicos para detectar roturas de vidrio.
    - Detectores combinados de microondas e infrarrojos.
    - Unidad central anti – intrusión para la gestión y control de los elementos el campo y la notificación de cualquier mal funcionamiento.
    - Los sensores magnéticos pueden detectar el estado de la puerta.
    - Salidas de emergencia con sensores de estado de la puerta.

Seguridad del edificio

El acceso al edificio, durante las horas normales de trabajo, se controla mediante reconocimiento visual por el vigilante de seguridad. El acceso del personal no empleado siempre está sujeto a control documental.

El acceso de los empleados fuera del horario laboral está sujeto a control documental, sujeto a autorización por parte del responsable de la estructura a la que pertenecen.

8.2.5. Seguridad del área CED

El área CED es el área protegida dentro del edificio, accesible mediante el uso de la insignia autorizada.

La sala técnica está ubicada dentro del segundo edificio en la planta baja mencionado anteriormente. En este área se encuentra la sala de centro de datos real, que contiene los dispositivos HW y SW de los diferentes sistemas de Tinexta InfoCert.

Las salas que conforman la sala de CA que contienen los sistemas que requieren protección especial, incluidas las destinadas a las actividades más críticas (AC, PEC, etc.), se conectan a la sala de control, donde se monitorean y supervisan los sistemas (aire acondicionado, plomería, fuente de alimentación y continuidad) y la sala de monitoreo para el control de los sistemas de seguridad instalados.

Solo personas con una función operativa en la prestación del servicio y personas responsables de la gestión de la infraestructura tienen acceso. El acceso para mantenimiento externo (trabajo ordinario y extraordinario) solo se permite en presencia de personal autorizado para ingresar al área de CED.

8.2.6. Fuente de alimentación – Garantía de fuentes de alimentación ininterrumpibles

El sistema está diseñado para garantizar la continuidad eléctrica incluso en presencia de fallas individuales a lo largo de la cadena de distribución.

El sistema eléctrico primario consta de 4 transformadores de voltaje medio para un total de 4MW.
La alta fiabilidad está garantizada por:

- 4 transformadores de media a baja tensión para un total de 4MW.
- 4 grupos electrógenos de arranque automático de 32,000 cc con una capacidad total de 3.8 MW.
- 2 tanques diesel de 10,000 litros que garantizan autonomía por más de 72 horas por fuente de poder ininterrumpida.
- 2 grupos UPS de 500 KW cada uno para la gestión de interrupciones hasta un máximo de 2 horas.
- En los pasillos, la redundancia de la fuente de alimentación se logra mediante un doble radial de sistema de distribución de tipo A + B.
- La distribución de la sala se realiza mediante pares de barras de bus blindadas (equipado con puntos de toma de selección de fase cada 60 cm y con paso de 180 cm - intensivo configuración de rack) alimentado por paneles eléctricos dobles (A + B).

Para aumentar los niveles de servicio deseados, es posible instalar en bastidores ATS (Interruptor automático de transferencia) sistemas de transferencia de la fuente de alimentación. Estos dispositivos usan 2 fuentes de alimentación en la entrada (una fuente principal activa y una fuente secundaria de reserva) y permitir cambiar de automático a manual sin ninguna interrupción (tiempo de conmutación <6 ms).

El ATS también se puede usar para servidores con un número impar de fuentes de alimentación, ya que hacen que la tercera fuente de alimentación sea redundante (y, por lo tanto, en el caso de una falla única, siempre tendrá al menos dos fuentes de alimentación).

8.2.7. Control automático de temperatura y acondicionamiento

El sistema está diseñado para garantizar el mantenimiento constante de la temperatura dentro de las habitaciones.

La planta consta de dos (2) torres evaporativas de 750 KW cada una.

Los sistemas están equipados con bobinas de condensación con una recolección y drenaje sellado de condensado.

Es un sistema controlado por sondas anti-inundación.

Todo el sistema de aire acondicionado es atendido por generadores de emergencia en caso de que se produzca un corte de energía.

La capacidad de enfriamiento por gabinete está garantizada con una carga máxima esperada de 10kW y un máximo de 15 kW en dos gabinetes uno al lado del otro.

La distribución del agua enfriada se realiza mediante un anillo de circulación primario, con 3 bombas de distribución con redundancia N + 2, montantes redundantes y anillos secundarios dobles en el sistema de habitaciones.

El enfriamiento de las salas del sistema se realiza mediante acondicionadores de agua refrigerada tipo "debajo" (entrega de aire hacia abajo - debajo del piso flotante).

Los sistemas de aire acondicionado y enfriamiento están diseñados para eliminar todo el calor generado por los equipos informáticos, correspondiente a la energía eléctrica absorbida, asegurando una temperatura ambiente, medido en pasillos fríos (pasillos en los que se introduce el aire de enfriamiento), hasta 24 + 1 ° C y humedad relativa entre 30% y 70%.

8.2.8. Detección y supresión de incendios

En el centro de datos hay un sistema de detección de humo gestionado por un control analógico NOTIFIER, unidad con sensores ópticos colocados en la habitación y en el falso techo, así como sensores de muestreo de aire instalado debajo del piso y en los conductos de aire.

El sistema automático de detección de incendios está conectado a la automática ecológica ARGON IG-01 Sistemas de extinción de gases.

Se proporciona un sistema de extinción de incendios dedicado para cada compartimento de incendios. También existen medios de extinción portátiles de acuerdo con las leyes y regulaciones vigentes.
El centro de datos y las salas de CA están controlados por diferentes tipos de detectores:

- Detectores ópticos de humo en el techo y en el suelo.
- Detectores de alarma manuales
- Alarmas acústicas y ópticas para advertencia local.
- Instrumento de acondicionamiento de señal para la recopilación de datos, gestión y autodiagnóstico de sistema de extinción de incendios.

8.2.9. Sistemas anti-inundaciones

Las salas del sistema están equipadas con un sistema anti-inundación hecho por medio de sondas puntuales conectado a la unidad automática de detección de incendios y ubicado debajo del piso a lo largo del sistema hidráulico.

Además, los aires acondicionados están equipados con su propia sonda anti-inundación con alarma.

8.2.10.Protección de la autoridad de certificación, PEC y TSA

Los sistemas diseñados específicamente para la CA, PEC y TSA se ubican en las instalaciones utilizadas para el servicio de certificación, dentro del área CED (llamada Locales de CA).

Se ha tenido especial cuidado en hacer conexiones entre los dispositivos en esta área.

Todas las conexiones (cables, puentes, enrutadores) se asignan de una manera que no es directamente accesible. Para acceder al sitio se debe tener una insignia autorizada y un PIN de acceso personal. La entrada a la sala de aire acondicionado está protegida por una brújula que permite la entrada de una sola persona autorizada a la vez. Todas las puertas están equipadas con alarmas de contacto magnético.

La sala de CA se beneficia del sistema de detección de incendios provisto para todo el edificio, el subsistema de extinción y los detectores anti - inundación provistos para el área CED.

En el subsuelo se encuentran instalados los detectores anti-inundación. Todas las habitaciones y las puertas de acceso a la sala de aire acondicionado están controladas por un sistema de circuito cerrado de televisión y microondas combinado con detectores infrarrojos.

El nivel de protección descrito anteriormente es utilizado para ciertas estaciones:

- Sala de seguridad: Dentro de esta sala, se registra el acceso a la sala de CA. El control de acceso es llevado fuera por medio de insignias.
- Sala de telecomunicaciones: El área se encuentra en habitaciones a las que no se puede acceder directamente.
- Sala de control y monitoreo: Para acceder al área debe tener una insignia.

8.3.Seguridad lógica

8.3.1. Sistemas y gestión de incidentes

El Centro de datos de Tinexta InfoCert se administra de acuerdo con las mejores prácticas sugeridas por ITIL.

El proceso de gestión de incidentes utiliza una sólida infraestructura de gestión de eventos, donde los controles de recursos están integrados y correlacionados con la navegación web que prueba el servicio a lo largo de su cadena de infraestructura.

Los eventos detectados están relacionados con los mapas de servicio, registrados en la base de datos de gestión de configuración (CMDB). A través de estas fuentes de información, los operadores de Service Desk pueden operar con una solución de primer nivel.

Las consolas operativas del centro de datos están controladas por operadores de nivel superior 24x7. En las consolas operativas se informan, para cada servidor individual bajo control, toda la información recopilada por agentes y que requiere la atención de los operadores. Cualquier anomalía es comunicada a los operadores de segundo nivel durante las horas de supervisión de 07:00 a 19:00 y durante disponibilidad fuera de este horario.

El segundo nivel de soporte está compuesto por un equipo de técnicos con competencia cruzada en todos los componentes tecnológicos y de servicio. También se ha previsto un mayor nivel de apoyo con técnicos verticalmente especializados en los diversos componentes de infraestructura tecnológica.

8.3.2. Copia de seguridad de datos

Tinexta InfoCert está equipado con la infraestructura más moderna para realizar copias de seguridad. Utiliza productos como Veeam Backup y EMC NetWorker que controlan y gestionan la ejecución de copias de seguridad y archivo.

Las políticas de copia de seguridad incluyen guardar semanalmente el contenido de los discos del sistema del servidor y la base de datos.

El tiempo de retención de una copia de seguridad será de 30 días para copias de seguridad diarias, 14 meses para copias de seguridad mensuales y 3 años para copias anuales.

Estas políticas de retención se pueden adaptar en casos especiales o bajo pedido. El servicio incluye la posibilidad de restaurar sistemas de archivos en caso de problemas.

La biblioteca, que conserva la biblioteca de medios, actualmente está certificada en las instalaciones de la CA, por lo tanto, se garantiza un nivel adicional de seguridad a los datos respaldados.

Excepto por necesidades específicas, las cintas nunca salen de la biblioteca de medios administrada por la biblioteca, porque la biblioteca misma verifica su integridad y legibilidad al generar automáticamente copias de medios si detecta la necesidad.

8.3.3. Seguridad de los sistemas operativos

Todos los sistemas, tanto Linux Red Hat como Windows, están reforzados independientemente de su ubicación en la Arquitectura de red de Tinexta Infocert (DMZ, back end, área protegida, para sistemas dedicados a la Autoridad de certificación y gestión de sistemas de firma).

El acceso por parte de los administradores del sistema designados para este fin (de acuerdo con las disposiciones de la legislación actual), es a través de una aplicación root on demand que permite el uso de los privilegios del usuario raíz solo después de la autenticación individual.

Los accesos se rastrean, registran y almacenan durante 12 meses.

8.3.4. Seguridad de la red

El Centro de datos de Tinexta InfoCert utiliza una conexión Gigabit Ethernet dual de fibra óptica en redes troncales operado por Retelit y Vodafone. Ambas líneas aseguran una velocidad máxima de 10 Gb / s. Las conexiones están certificadas en POP separados, con rutas físicas y equipos de interfaz separados y los sistemas de firewall son completamente redundantes, interconectan las líneas con la intranet de Tinexta InfoCert.

La estructura permite garantizar la continuidad de los servicios en caso de falla de uno de los dos enlaces (o de una falla dentro de la red de uno de los dos Proveedores). En estos casos, a través de mecanismos de enrutamiento automático, el tráfico de datos del enlace fallido se desviará a otro enlace.

Tinexta InfoCert tiene dos sistemas de gestión de DNS ubicados en diferentes redes y, por lo tanto, pueden garantizar la máxima continuidad del servicio.

La seguridad de la red se basa en una arquitectura de red de 3 niveles:

- Sub redes DMZ
- Sub redes de intranet
- Área protegida que aloja los sistemas de la CA

Seguridad de red: Protección contra intrusiones:

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.

Todo el tráfico que fluye entre las diferentes áreas está sujeto a aceptación por el firewall, basado en un conjunto de reglas establecidas. Las reglas definidas en los firewalls están diseñadas de acuerdo con los principios de "denegación predeterminada" (lo que no está expresamente permitido está prohibido por defecto, es decir, las reglas solo permitirán lo que sea estrictamente necesario para el correcto funcionamiento de la aplicación) y "defensa en profundidad" (se organizan sucesivos niveles de defensa, primero en el nivel de red, a través de barreras de firewall sucesivas, y finalmente a nivel de sistema (endurecimiento)).

Los sistemas de firewall de Tinexta InfoCert están en alta confiabilidad (HA) y en modo de espera activo. Estos son, de hecho, grupos de cortafuegos hechos con pares de dispositivos independientes y conectados entre sí. Estos dispositivos se gestionan, a través de un SW especial, de modo que, en caso de fallo de una de las máquinas, el tráfico se desvía al segundo nodo activo del clúster de manera transparente para los servicios previstos.

8.3.5. Seguridad de acceso

El acceso a la información se controla mediante credenciales de autenticación emitidas individualmente.

Las credenciales son personales e intransferibles, se asignan en función de la necesidad de acceder a los datos o sistemas de la empresa y se gestionan al mismo tiempo que las autorizaciones.

Las contraseñas deben ser robustas, es decir, deben estar construidas de tal manera que no sean fáciles de 'adivinar' (adivinar la contraseña).

Para los sistemas más críticos de ser una autenticación fuerte usando tokens y certificados de autenticación.
Se aplican reglas similares a los llamados PIN de dispositivos con certificados digitales a bordo (tarjetas inteligentes, claves comerciales, etc.).

Los sistemas de autenticación aseguran que el uso de credenciales cumpla con las políticas de seguridad establecido por el sistema de gestión de seguridad, incluida la aplicación de reglas de formación de contraseña.

Solo el cliente puede acceder a los datos del cliente almacenados en los sistemas Tinexta InfoCert, a través de usuarios personales asignados a él cuando se activa el servicio.

La autorización es estrictamente relacionada con el servicio, por lo que los usuarios se relacionan con diferentes servicios, pero relacionados con el mismo cliente, a menos que el cliente solicite lo contrario, no comparta los mismos derechos de acceso.

8.3.6. Seguridad en la estación de trabajo

Todas las estaciones de trabajo están equipadas con un software antivirus que se actualiza al menos diariamente. La herramienta comprueba las configuraciones y detecta la presencia de software no autorizado.

8.3.7. Evaluación de vulnerabilidad

La seguridad es un proceso continuo, que incluye un ciclo continuo de diseño, implementación, verificación de la aplicación correcta y, finalmente, revisión de la efectividad con respecto al nivel deseado de seguridad.

Endurecimiento, aplicado al software básico y de middleware, es decir, la actividad que permite el logro y mantenimiento de un nivel adecuado de seguridad para la operación del sistema y el middleware es un componente indispensable de este proceso.

Para lograr y mantener un nivel adecuado de solidez a los ataques cibernéticos en los servidores de producción, Tinexta InfoCert selecciona un subconjunto de aplicaciones cada seis meses, que es verificado por un organismo externo a través de sesiones de prueba de penetración y evaluación de vulnerabilidad.

Registra y procesar los eventos de seguridad de un sistema es uno de los objetivos a tener en cuenta durante el endurecimiento. El sistema debe estar configurado para grabar y guardar la seguridad de la información, tal como la proporciona la tecnología.

8.3.8. Gestión de personal

El IMS y el Sistema de Gestión de Calidad (QMS) han definido procedimientos estrictos para la gestión de personal, desde su entrada hasta su salida. Estos procedimientos prevén la gestión de la asignación de recursos individuales, así como credenciales y autorizaciones en base de las necesidades reales determinadas por la ubicación prevista de la persona en la empresa.

Las personas también son nombradas formalmente para el procesamiento de acuerdo con la legislación sobre protección de datos personales y consciente de las obligaciones que este nombramiento implica. La revisión de las autorizaciones se realiza anualmente.

Para acceder a los locales y a los sistemas que respaldan las actividades reguladas por la ley, la auditoría se realizará al menos de manera anual.
Los cambios en las unidades organizativas y / o renuncias implican la revisión / eliminación inmediata de todas las credenciales.

Al final de la relación laboral se espera que devuelva todos los activos. Cualquier excepción puede ser solicitado al Departamento de Seguridad de la Información, que puede autorizarlos después de verificar que ningún dato de la empresa puede estar expuesto a riesgos.

8.4.Controles de procedimiento

Roles clave

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

8.5.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.

8.6.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.

8.7.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.

8.8.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 al documento “Continuidad del negocio”.

8.9.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.

8.10. Evaluación de riesgos

Anualmente, los proveedores de Camerfirma Perú llevan a cabo un análisis de riesgo de seguridad de la información, basado en el Plan de Tratamiento de Riesgo. 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.

9. Responsabilidades de Camerfirma Perú

Camerfirma Perú exige a sus proveedores cumplir controles de seguridad y privacidad necesarios para proteger la información soportada en los servicios del Sistema de Intermediación Digital, en conformidad con lo declarado en el presente documento y en la Guía de Acreditación de Servicios de Valor Añadido.

10. Organización que administra la política de seguridad

Camerfirma Perú administra los documentos de Política de Seguridad, y todos los documentos normativos del SVA.

Para cualquier consulta contactar:

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

11. Publicación de la política de seguridad y otros documentos

La Política de Seguridad de los Servicios de Valor Añadido de Camerfirma Perú, así como la Declaración de Prácticas de los Servicios de Valor Añadido, la Política y Plan de Privacidad 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.

El presente documento es firmado por el Responsable de Seguridad de la Información y Privacidad de Datos Personales.

12.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.

13.Conformidad

Este documento ha sido aprobado y su cumplimiento es supervisado anualmente por el Responsable del Prestador de Servicios de Valor Añadido de Camerfirma Perú, 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.

Camerfirma PERÚ

Tinexta Infocert

think next,
trust now