# Política de Seguridad Servicio de Intermediación de Evicertia Perú

Servicio de Valor Añadido de Intermediación

Evicertia

Febrero de 2024



Público

# Índice

# 1 Introducción

## 1.1 Objetivo

El presente documento tiene como objetivo contener la Política de Seguridad (PS) del Servicio de Valor Añadido (SVA) de Intermediación de Evicertia Perú S.A.C.

## 1.2 Alcance

El alcance del presente documento va a ser:

- Políticas y normas que cumple, indicando también si tiene alguna certificación.
- La descripción funcional del servicio, junto con alguna de sus características de funcionamiento.
- Explicar cómo se pueden solicitar sellos electrónicos y cómo van a ser las respuestas.

## 1.3 Control de versiones

| Ver. | Fecha | Observaciones |
|---|---|---|
| 1.0 | 14/02/2024 | Se aprueba la primera versión de este documento. |

## 1.4 Políticas y documentos aplicables

A continuación, se detallan las políticas y documentos relacionados con los que cumple el SVA de intermediación de Evicertia.

- Ley N.º 27269, Ley de Firmas y Certificados Digitales. Decreto Supremo N.º 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
- Ley N.º 29733, Ley de Protección de Datos Personales. Decreto Supremo N.º 003-2013-JUS, Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales.
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers.
- ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- Declaración de Prácticas de Servicios de Valor Añadido (DPSVA) de Evicertia.

## 1.5 Organización que administra los documentos del SVA

Evicertia Perú S.A.C., filial de Evicertia, S.L.U. (empresa del grupo Namirial), es una sociedad mercantil registrada en Perú, especializada en firma electrónica avanzada, notificación fehaciente e identificación digital, y en proporcionar otros servicios electrónicos de valor añadido como Servicio de

Intermediación (SI), mediante la explotación de la infraestructura tecnológica de Evicertia, S.L.U. En adelante identificada como “Evicertia”.

Evicertia está reconocida como Prestador de Servicios de Certificación (PSC) en el Registro Oficial de Prestadores de Servicio de Certificación (ROPS) bajo responsabilidad de INDECOPI (que en esta DPSVA se va a identificar como la Autoridad Administrativa Competente (AAC)).

Evicertia, S.L.U. (España), es un PSC, que actúa de acuerdo con lo dispuesto en el Reglamento (UE) 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, así como las normas técnicas del ETSI aplicables a los servicios de confianza, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios. Los servicios de confianza de Evicertia se auditan anualmente de acuerdo con la normativa europea aplicable, bajo lo indicado en las normas ETSI EN 319 401, y ETSI EN 319 521. En adelante identificada como “Evicertia España”.

## 1.6 Persona de contacto

Los datos adicionales de contacto de Evicertia, son los siguientes:

- Entidad: Evicertia Perú S.A.C.
- Web: https://www.evicertia.com.
- Email: info@evicertia.com.
- Teléfono: + 51 942 094 673.
- Domicilio postal: Calle Dos de Mayo 516, Oficina 406, Miraflores, Lima, Perú.

## 1.7 Publicación y difusión del documento

La presente PS es administrada por Evicertia, y está publicada, para su consulta por cualquier tercero interesado, en su web https://www.evicertia.com/, junto con el resto de documentación relativa a su SVA.

En el sitio web de Evicertia se podrán localizar todas las versiones de todos los documentos públicos relacionados con el SVA de los cuales Evicertia es considerada como PSVA.

El sitio de Evicertia se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de Evicertia, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo de acuerdo con los plazos y procedimientos establecidos con respecto de la continuidad del negocio.

# 2 Política de Seguridad

## 2.1 Evaluación de riesgos

Evicertia realiza una evaluación de riesgos de manera trimestral sobre todos los activos de la compañía, incluyendo los activos del SVA de intermediación. La evaluación de riesgos permite a Evicertia estimar los riesgos de los diferentes activos para intentar reducir o incluso eliminar la materialización de las amenazas sobre los activos, adoptando las medidas necesarias para ello.

La evaluación es realizada por el responsable de seguridad en colaboración con todas las áreas de Evicertia, y el resultado de la evaluación de riesgos trimestral es presentado al Comité de Seguridad, que es el órgano que vela por la seguridad de Evicertia, y es el órgano que debe tomar en cuenta las recomendaciones de la evaluación de riesgos, y velar por el cumplimiento de sus implementaciones.

Las fases de la evaluación de riesgos son:

- Identificación de activos, amenazas y los impactos que se producirían si las amenazas se materializan.
- Análisis de riesgos, basado en una simplificación de MAGERIT[1].
- Ejecución de un plan de tratamiento para aquellos riesgos no asumidos.
- Gestión de los riesgos donde se evalúa la disminución de los controles implantados, la asunción de aquellos riesgos que así se consideren o la transferencia de los riesgos mediante, principalmente, la contratación de pólizas de seguro.

## 2.2 Control de acceso

Evicertia ha implantado medidas de control de acceso en todas las capas de sus sistemas de información, basándose en el principio del mínimo privilegio. A continuación, se enumeran algunas de las medidas más importantes:

- Aprobación de políticas y procedimientos de control de acceso que establezcan, mediante la gestión de usuarios para determinar “quién”, “cómo” y “cuándo” puede tener acceso.
- Separación de tareas, mediante la definición de roles y documentar las responsabilidades de cada una de las funciones del personal de confianza.
- Privilegios mínimos, basadas en autorizaciones de acceso solo a lo que se necesite para la ejecución de las funciones del personal de confianza.
- Bloqueo de sesiones automática cuando el ordenador tenga un periodo de inactividad de cinco minutos.

[1] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Edita: © Ministerio de Hacienda y Administraciones Públicas, octubre 2012.- NIPO: 630-12-171-8.

- Supervisión y revisión de controles de acceso por lo menos una vez al año la revisión respecto de la asignación de permisos y se verificará que estos sean los adecuados para la realización de las funciones de los colaboradores.
- Teletrabajo, estableciendo diferencias de usuario para el acceso a los diversos sistemas de la organización, así como las consideraciones que se deben tener para el acceso remoto a redes internas de Evicertia.
- No existen sistemas de información externos donde se tenga que conectar el personal de confianza para la gestión del SVA de intermediación.

## 2.3 Seguridad del personal

Evicertia ha implantado medidas de selección de personal, además de establecer procedimientos internos de capacitación de este. A continuación, se enumeran algunas de las medidas más importantes:

- Implantación de un procedimiento de contratación de personal, en el que se evalúan los conocimientos del personal, el establecimiento de un proceso de capacitación, y las condiciones del puesto de trabajo.
- Asignación, cuando corresponda, a uno de los roles de personal de confianza, con requisitos laborales adicionales.
- Establecimiento de un procedimiento de cese de la relación laboral con el personal, para evitar fugas de información.
- Convenios de confidencialidad con el personal, donde todos los empleados y colaboradores de Evicertia firmarán acuerdos relativos a la confidencialidad de la información a la que accedan, y que contendrá:
    - Partes intervinientes.
    - El servicio o servicios al que va asociado el acuerdo de confidencialidad.
    - La información tendrá carácter confidencial.
    - Compromisos por ambas partes.
    - Posibles sanciones y legislación aplicable.
    - Sanciones al personal.
- Establecimiento de un procedimiento sancionador ante incumplimientos de lo firmado.

## 2.4 Seguridad física

Evicertia ha establecido una serie de medidas físicas para los sistemas y comunicaciones del SVA de intermediación. A continuación, se enumeran algunas de las medidas más importantes:

- Políticas de Seguridad Física, estableciendo medidas de protección que se implementan en los centros de datos, principal y redundante, así como en las oficinas administrativas de Evicertia para asegurar que los activos críticos se encuentran protegidos.

- Las autorizaciones de acceso físico a las áreas seguras de los centros de datos son gestionadas internamente, junto con el personal del CPD según procedimientos establecidos entre ambas compañías.
- Los accesos al área segura del CPD cuentan con cerraduras electrónicas las cuales son activadas mediante la tarjeta de proximidad asignada al personal autorizado.
- En cada uno de los CPD desde donde se prestan los servicios existen:
    - Certificaciones ISO27001, 9001 y otras adicionales.
    - Controles de seguridad perimetral.
    - Controles para dispositivos de almacenamiento externo
    - Monitoreo del acceso físico a las áreas seguras
    - Registro de ingreso de visitantes
    - Redundancia de la infraestructura eléctrica, y suministro de emergencia de energía eléctrica.
    - Protección contra incendios.
    - Controles de Temperatura y humedad.
    - Protección contra daños por agua.
    - Personal de vigilancia 24x7.
    - Servicio de operación 24x7.

## 2.5 Seguridad de comunicaciones y redes

Evicertia ha establecido una serie de medidas lógicas para su red de telecomunicaciones y redes propias. A continuación, se enumeran algunas de las medidas más importantes:

- Servicios de Telecomunicaciones, Evicertia cuenta con contratos con al menos dos proveedores de servicios de telecomunicaciones. Esto con la finalidad de garantizar la continuidad de sus servicios y hacer frente a las obligaciones contractuales que tienen con los suscriptores y partes interesadas.
- Segmentación de red, los equipos están en un segmento privado, y solo es posible acceder a ellos a través de los equipos de salto, y además es necesario que el identificador del usuario esté permitido para realizar la conexión.
- Acceso mediante VPN, el acceso a los segmentos de red privados se hace mediante VPN con doble factor de autenticación.
- Monitorización continua, Evicertia cuenta con sistemas de monitorización de red que le permiten conocer el comportamiento de las peticiones que se realizan. Se cuenta con tres diferentes herramientas que ayudan con la monitorización de las redes internas, las redes externas, así como de la disponibilidad de los DNS del servicio.
- Conexiones internas del sistema, para incrementar los niveles de seguridad del servicio y asegurar que el acceso a los módulos criptográficos se lleva a cabo únicamente por los recursos autorizados y que forman parte de la prestación del servicio las interacciones entre

recursos están restringidas a nivel de comunicaciones. Todo ello a través de las direcciones IP de cada uno de los equipos.

## 2.6 Mantenimiento de equipos y su desecho

Evicertia ha establecido una serie de procedimientos para el mantenimiento de los equipos y su eliminación. A continuación, se enumeran algunas de las medidas más importantes:

- Procedimientos para el mantenimiento de los sistemas, Evicertia cuenta con procedimientos internos para el mantenimiento de los componentes que integran la infraestructura del SVA de intermediación. Estos procedimientos incluyen la periodicidad en la que son ejecutados dichos procesos, así como la definición de aquellos escenarios que se consideran como mantenimientos preventivos y aquellos considerados como correctivos.
- Mantenimientos programados, los equipos de hardware que integran el SVA de intermediación, como parte de los programas de mantenimiento de Evicertia, están sujetos a mantenimientos programados que permiten garantizar que se encuentran en óptimas condiciones para prestar el servicio.
- Para el resto de los equipos, el mantenimiento será ejecutado por el personal de Evicertia que cuenta con los conocimientos y experiencia necesaria para desarrollar esta actividad.
- Eliminación de equipos, existen procedimientos para la eliminación de equipos específicos para los módulos criptográficos y también para el resto de infraestructura del SVA de intermediación. Si la eliminación es física se tendrá en cuenta lo indicado en la legislación vigente con respecto al desecho de material electrónico.

## 2.7 Control de cambios y configuración

Evicertia ha establecido un procedimiento de control de cambios para gestionar la autorización y documentación de cualquier cambio a realizar. A continuación, se enumeran algunas de las medidas más importantes:

- Procedimientos y políticas de configuración de los sistemas, Evicertia cuenta con procedimientos y personas autorizadas para el uso, adquisición, instalación y configuración de las herramientas de software que sean necesarias tanto en los equipos de los trabajadores como en los servidores de la SVA de intermediación. Todos estos procesos tienen que estar documentados en tickets.
- Configuración base de los sistemas de la SVA de intermediación, estos componentes sólo podrán ser administrados por personal de confianza.
- Control de cambios de las configuraciones, se llevará una bitácora respecto de los cambios realizados, así como de las fechas en que se llevaron a cabo.

## 2.8 Planificación de contingencias

Evicertia ha establecido, en base al resultado de las evaluaciones de riesgos, la ejecución de análisis de impacto de negocio y un plan de continuidad. A continuación, se enumeran algunas de las medidas más importantes:

- Plan de Continuidad de Negocio y Recuperación ante Desastres, cuya finalidad es el salvaguardar el SVA de intermediación, tras la materialización de una contingencia, cubriendo los procesos críticos que se desarrollan en las diferentes oficinas y centros de datos de Evicertia.
- El Plan de Continuidad de Negocio y Recuperación ante Desastres permite a Evicertia conseguir, entre otros, los siguientes objetivos:
    - Reaccionar de forma coordinada para minimizar de forma eficaz, las consecuencias de un incidente grave.
    - Mantener la confianza de los suscriptores, autoridades, empleados y partes interesadas.
- Capacitaciones para la aplicación del plan de continuidad, donde los trabajadores conozcan los procedimientos que se deben seguir, así como las responsabilidades asignadas en caso de la presencia de incidencias, complementado con el desarrollo de un plan de comunicación y capacitación interna a través del cual se concientiza respecto de las actividades que deben hacer, así como las que no. La capacitación respecto del Plan de Continuidad se acentúa en aquellos trabajadores o miembros de Evicertia que forman parte del Comité de crisis
- Pruebas de ejecución del plan de continuidad, ejecutando revisiones cuando se producen modificaciones significativas (de negocio, técnicas, organizativas) o de forma sistemática una vez al año.

## 2.9 Auditoría y detección de intrusiones

Evicertia ha establecido un calendario de auditorías de seguridad, tanto interno como externos para todos los activos de información. A continuación, se enumeran algunas de las medidas más importantes:

- Proceso de auditoría interna de Evicertia, se ha definido un proceso institucional de auditoría interna con el cual se busca garantizar que el SVA de intermediación se ejecuta, mantiene, opera y evoluciona de manera adecuada.
- Proceso de auditoría externa, dentro del proceso de auditoría contempla la contratación de servicios de auditoría externa con despachos de consultoría que cuenten con experiencia en manejos de infraestructura de PKI, algoritmos criptográficos y sistemas informáticos.
- Eventos de auditoría, Evicertia considera como un evento de auditoría toda presencia, dentro de los sistemas de información y controles de seguridad, de acciones que pueden poner en riesgo la correcta operación del servicio. Algunos ejemplos de este tipo de eventos son:

cambios en las contraseñas de los usuarios de administración y gestión del servicio, autenticaciones fallidas, accesos fallidos a los sistemas, entre otros.

- Sistemas de revisión de logs y detección de intrusiones, Evicertia cuenta con sistemas que permiten detectar y proteger la infraestructura tecnológica contra cualquier tipo de intrusión lógica.
- Contenido de los registros de auditoría, se deberá integrar un registro de auditoría el cual contendrá todos aquellos elementos que se determinen como de No Conformidad. Se considera como No Conformidad a todos aquellos eventos que no se desarrollan de acuerdo en cómo se establece en la documentación que ampara los procesos o procedimientos del cual forman parte.
- Respuesta a fallas en el proceso de auditoría, será necesario establecer un plan de acciones para corregir cualquier desviación o fallo detectado en la auditoría.
- Revisión, análisis y reporte de los procesos de auditoría, será revisada por el responsable de seguridad y los resultados de esta se elevarán al Comité de Seguridad. Si fuera necesario se indicarán las acciones correctivas o preventivas registrando las mismas en los gestores de incidencias. Así mismo, se acordará la planificación para resolver dichas no conformidades.

## 2.10 Medios de almacenamiento

Evicertia ha establecido procedimientos para la gestión del ciclo de vida de cualquier medio de almacenamiento que contenga información del servicio. A continuación, se enumeran algunas de las medidas más importantes:

- Módulos criptográficos, las claves criptográficas que serán utilizadas para el SVA de intermediación serán generadas y almacenadas en los módulos criptográficos propiedad de Evicertia. Para este servicio se estará utilizando modelos que cumplen con el estándar *Common Criterial EAL 4+ AVA_VAN.5*, que funcionalmente es superior al *FIPS 140-2 nivel 3* en sus elementos de seguridad e implantación de los algoritmos criptográficos.
- Controles para dispositivos de almacenamiento externo que tienen como finalidad asegurar que todo el personal tiene conocimiento sobre el almacenamiento, transporte, y borrado seguro de información en soportes extraíbles para evitar la revelación, modificación, eliminación o destrucción no autorizada de la información almacenada en dichos soportes. Ahora bien, el uso de los dispositivos de almacenamiento externo, en medida de los posible, se evitará dentro de todos aquellos componentes de la SVA de intermediación.
- Respaldo y recuperación, han sido comentadas en el apartado “Planificación de contingencias”.

# 3 Anexo I - Acrónimos

A continuación de muestra una lista de los acrónimos utilizados en el presente documento:

- AAC: Autoridad Administrativa Competente.

- AI: Autoridad de Intermediación.
- CC: *Common Criteria.*
- CSO: *Chief Security Officer.*
- CPD: Centro de Proceso de Datos.
- CRL: *Certificate Revocation List.*
- DPSVA: Declaración de Prácticas del Servicio de Valor Añadido.
- EAL: *Evaluation Assurance Leve*ls.
- ESI: *Electronic Signatures and Infrastructures*.
- ETSI: *European Telecommunications Standards Institute*.
- FIPS: *Federal Information Processing Standard*.
- HSM: *Hardware Secure Module*.
- HTTP: *Hypertext Transfer Protocol*.
- INDECOPI: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.
- NTP: *Network Time Protocol*.
- OCSP: Online Certificate Status Protocol.
- OTP: *One-Time Password*.
- PSC: Prestador de Servicios de Certificación.
- PSVA: Prestador del Servicio de Valor Añadido.
- ROPS: Registro Oficial de Prestadores de Servicio de Certificación.
- RSA: *Rivest–Shamir–Adleman* (criptosistema de clave pública).
- RFC: *Request For Comments*.
- RUC: Registro Único de Contribuyentes.
- SAC: Sociedad Anónima Cerrada.
- SGSI: Sistema de Gestión de la Seguridad de la Información.
- SLA: *Service Level Agreement* (Acuerdo de nivel de servicio).
- SI: Servicio de Intermediación.
- SVA: Servicio de Valor Añadido.
- TLS: *Transport Layer Security*.
- UE: Unión Europea.
- URL: *Uniform Resource Locator*.
- UTC: *Coordinated Universal Time*
- VPN: *Virtual Private Network*.