DECLARACIÓN DE PRÁCTICAS DE VALOR AÑADIDO (VAPS)

AUTORIDAD DE SELLADO DE TIEMPO
VERSIÓN 1.2

Idioma: **Español**

Fecha: Agosto 2022

Estado del documento: Activo

Historial de Versiones			
Versión	**Fecha**	**Autor**	**Resumen de Cambios**
1.0	Julio 2013	Wilfredo Dávila Fuentes	Documento inicial
1.1	Octubre 2021	Andrés Romero Chavez	**2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones y responsabilidad financiera –** Se agrega texto "tales como reembolsos, extensiones de garantías, indemnizaciones ni por fuerza mayor". Se agrega punto **4.5 Re emisión de la clave de TSA-TSU** **4.6 Fin del ciclo de vida de la clave de TSA-TSU –** Se agrego texto "La AC deberá 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. La destrucción o deshabilitación de las claves se detallará en un documento creado al efecto". **4 Gestion de Claves de la TSA –** Se agregan los siguientes puntos: **4.8 Revocacion de certificados** **4.8.1 Causas de Revocación** **4.8.2 Quien puede solicitar la revocación** **4.8.3 Procedimiento de solicitud de revacion** **5.2 Sincronizacion del reloj con UTC –** Se agregó texto "La precisión de la fecha y hora incorporada en los sellos de tiempo basadas en el sistema UTC con una desviación máxima de retardo de 100ms. Ante alguna falla se realizarán procedimientos de calibración, que lo realiza la entidad de certificación". Se agrego punto **5.3 Comunicaciones** **6.1 Gestion de la seguridad –** Se modifico texto "Sección 5 y 6" por "Sección 4 y 5". **6.1 Gestion de la seguridad –** Se agregan los siguientes puntos: **6.1.1 Auditorias y detección de instrusiones** **6.1.2 controles de auditoria de sistemas** **6.2 Compromiso de los servicios TSA –** Se agregó texto "Ante perdida de la precisión del reloj, compromiso del mismo o sospecha de compromiso en el tiempo de la TSA; SALMON dejará esta información a los suscriptores y terceros que confían indicando la descripción del evento. Esta comunicación será directa o a través de su sitio web". **6. Gestion y Operaciones de la TSA –** Se agregan los siguientes puntos: **6.8 Procedimiento de Gestion documental** **6.9 Planificacion del sistema** **6.10 Manejo de medios de seguridad** **6.11 Reporte de incidencias y respuesta** **6.12 Riesgo de intercambio de información** **6.13 Mantenimiento e implementación de sistemas de confianza** **6.14 Control de cambios** **6.15 Procedimiento de control de seguridad** **6.16 Registro de información concerniente a las operaciones del servicio de sello de tiempo** **6.17 Registros concernientes** **6.18 Auditoria**

1.2	Agosto 2022	Andrés Romero Chavez	**3.1.1 Declaración de Practicas de la TSA–** Se agrega el siguiente texto: La presente Declaración de Prácticas de Registro es administrada por SALMON CORP S.A.C., cada nueva versión será presentada al INDECOPI y luego de su aprobación, será debidamente publicada en la siguiente dirección: https://www.salmoncorp.com/wp-content/uploads/2022/08/VAPS-de-Sellado-de-tiempo-Salmon-v1.1-1.pdf

ÍNDICE DE CONTENIDO

1 INTRODUCCIÓN

1.1 Vista General

Salmón Corp SAC (en adelante Salmón Corp) es una organización con sede en Perú orientada a la cobertura de necesidades de protección documentaria y de marca al servicio de las organizaciones privadas y públicas, mediante la elaboración y comercialización de elementos con tecnología de punta que brindan altos niveles de seguridad contra su duplicación y su falsificación. Actúa también en el campo de la identificación, validación y trazabilidad de personas y documentos. En este sentido, Salmón Corp brinda el servicio de emisión de Sellos de Tiempo (Timestamp) conforme a la regulación peruana establecida por la Autoridad Administrativa Competente, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

El presente documento especifica la Declaración de Prácticas de Valor Añadido (VAPS) para Sello de tiempos de *Salmón Corp*, y es conforme a la norma del *ETSI TS 102 023 "Policy requirements for time-stamping authorities"* y a su especificación equivalente *RFC-3628 "Policy requirements for time-stamping authorities"*, en concordancia con el estándar *ISO/IEC 18014-1:2002 "Information technology -- Security techniques -- Time-Stamping Services -- Parte 1: Framework"*.

Salmón Corp brinda el servicio de sellado de tiempo provisto por AC Camerfirma SA (en adelante Camerfirma) (http://www.camerfirma.com), el cual cumple con lo estipulado en la ETSI TS 102 023 y su equivalente RFC-3628, siendo auditada anualmente por entidades acreditadas de reconocido prestigio respecto a los "Principles and Criteria for Certification Authorities" y a los "Principles and Criteria for Certification Authorities - Extended Validation" elaborados por AICPA/CICA. Asimismo la infraestructura de Camerfirma cuenta con las certificaciones ISO 27001 Sistema de Gestión de Seguridad de la Información e ISO 20000 Sistema de Gestión de Servicios de Tecnologías de la Información.

El servicio de sellado de tiempo se compone de dos componentes diferenciados:

- Suministro de Sellos de Tiempo.
- Gestión del servicio de sellado de tiempo.

La división de estos componentes solamente se toma por motivos de clarificación de los requerimientos especificados en estas políticas.

El certificado de Sello de tiempo es necesario para garantizar la existencia de un documento, o transacción electrónica, en un tiempo concreto, a través de:

- La firma digital de la autoridad de sellado de tiempo.
- Identificador electrónico único del documento (HASH o resumen)
- Fecha y hora recogida de una fuente fiable de tiempo.

En lo que se refiere al contenido de este documento, se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto.

Se ha utilizado el estándar *RFC 3647 "Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framewortk"* del Internet Engineering Task Force (IETF) como guía de asistencia en la redacción de este documento

1.2 Identificación

La forma de identificar distintos tipos de certificados digitales es a través de identificadores de objeto (OID's). Un OID concreto permite a las aplicaciones distinguir claramente el certificado que se presenta e identificar la política de certificación correspondiente.

En concreto el identificador correspondiente a este tipo de certificados es:

Nombre:	Declaración de prácticas de valor añadido (VAPS). Sello de tiempo
Código:	VAPS-SELLO-TSA
Versión:	1.1
Elaborado por:	Salmón Corp SAC
Idioma:	Español
Descripción:	Esta Política establece las reglas generales empleadas por la Autoridad de Sellado de Tiempo de Salmón Corp SAC, para la emisión de tokens que contienen sellos de tiempo firmados
Fecha de edición:	Octubre 2021
Estado del documento:	Activo
Localización:	http://www.salmoncorp.com/

1.3 Comunidad y Ámbito de Aplicación

Este documento puede ser utilizado por terceros receptores de los sellos de tiempo de Salmón Corp SAC y suscriptores del servicio de emisión de sellos de tiempo como base para confirmar la fiabilidad de los servicios descritos en el. La política de la autoridad de sellos de tiempo esta basada en criptografía de clave publica, fuentes seguras de tiempo y certificados digitales.

1.3.1 TSA-TSU

Una TSA (Autoridad de Sellado de tiempo) es un elemento de confianza en el que el usuario (suscriptores y terceras partes receptoras de sellos) confían para la emisión de sellos de tiempo. La TSA tiene la responsabilidad última sobre todos los servicios relacionados con la emisión de los sellos de tiempo.

Las TSU (Unidades de Sellado de Tiempo) pueden emitir sellos de tiempo en nombre de la TSA.

1.3.2 Suscriptor

Bajo esta Política, el Suscriptor es la persona natural o jurídica que requiere los servicios provistos por una Autoridad emisora de sellos de tiempo – TSA y que está de acuerdo con los acuerdos y obligaciones descritos en la Política de Sellado de Tiempo.

1.3.3 Tercero que confía o usuario

En esta Política se entiende por Tercero que confía o usuario, a la persona que voluntariamente confía en los sellos de tiempo emitidos bajo esta política y se sujeta a lo dispuesto en ella por lo que no se requerirá acuerdo posterior alguno.

1.3.4 Ámbito de Aplicación y Usos

Los sellos de tiempo emitidos por la Autoridad de Sellado de Tiempo pueden emplearse para garantizar la fecha y hora cierta de la existencia de un documento electrónico.

1.3.5 Usos Prohibidos y no Autorizados

No se permite el uso que sea contrario a la normativa Peruana ni la utilización distinta de lo establecido en esta Política de Sellado de Tiempo.

1.4 Conformidad y Contacto

Esta política de certificación está administrada y gestionada por Salmón Corp, pudiendo ser contactado por los siguientes medios:

E-mail:	info@salmoncorp.com
Teléfono:	+(51-1) 332 0797 / 333 2200
Fax:	+(51-1) 332 3576
Dirección:	Av. General Vidal #921, Breña, Lima - Perú

La directiva de Salmón Corp constituye la Autoridad de las Políticas (PA) y velará en todo momento por el cumplimiento de esta Política de Certificados y su alineamiento con los requisitos legales que le sean de aplicación, así como las buenas prácticas internacionales estableciendo las medidas y controles que considere necesarios a tal efecto.

2 OBLIGACIONES Y RESPONSABILIDAD

2.1 Obligaciones

Este apartado incluye todas las obligaciones, garantías y responsabilidades de la TSA frente a los usuarios y terceras partes que voluntariamente confían en los servicios de sellado de tiempo, así como las obligaciones asumidas por las partes.

2.1.1 Obligaciones de la TSA en relación a los suscriptores

Salmón Corp entregará los servicios con la confiabilidad y exactitud establecida en la presente Política de Sellado de Tiempo.

En particular, la TSA garantizará:

- Cumplir lo dispuesto en esta política.
- Proteger su información contra pérdidas, destrucciones y falsificaciones.
- El acceso permanente a los servicios de sellado de tiempo excluyéndose las tareas de mantenimiento programadas y situaciones de Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- La exactitud de la fecha y hora incorporada en los sellos de tiempo basadas en el sistema UTC.

2.1.2 Obligaciones del suscriptor

El suscriptor para hacer uso del Sistema de Certificación TSA, asume la obligación de conocer y comprender plenamente las características y limitaciones determinadas en esta Política de certificado y documentos referenciados.

En particular, es responsabilidad de los suscriptores:

- Realizar las peticiones e interpretación de las respuestas conforme al formato establecido en la RFC 3161
- Verificar el estado del certificado.

2.1.3 Obligaciones de las partes confiantes

Los terceros que confíen en los Sistemas de Certificación de esta TSA son responsables de verificar que los documentos sean firmados con un sello de tiempo, con un certificado digital reconocido por Salmón Corp y que estos sellos tengan como parte de su número de identificación el OID, la identificación de la respectiva política de sellado de tiempo.

Asimismo deben verificar que el certificado de sello de tiempo se encuentra firmado y que la clave privada no estuvo comprometida en el momento en el que se realizó el sellado de tiempo

En particular, las terceras partes asumen la obligación de:

- Verificar el estado de activación en que se encuentra el Certificado de la TSA al que se vincula el Sello Digital de Tiempo emitido, mediante consulta a la CRL u otro medio que se disponga para la verificación de estado del certificado.
- En el supuesto de que el certificado haya expirado o haya perdido su validez por revocación deberá comprobar que:
  - La fecha de revocación o de caducidad es posterior a la fecha en que se emitió el sello de tiempo.
  - La función criptográfica que se empleo para obtener el sello sigue siendo segura.
  - Que la longitud de la Clave criptográfica y el algoritmo de firma electrónica siguen siendo de práctica habitual.

- Tener en cuanta cualquier limitación en el uso del sello de tiempo indicado en la política y prácticas de certificación correspondientes.
- Tomar en consideración cualquier limite prescrito en otros acuerdos de servicio.

2.2 Responsabilidad

Salmón Corp es responsable de gestionar la implementación y velar por el cumplimiento de la presente Política de Sellado de Tiempo, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

La TSU será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de toda la información contenida en sello de tiempo o en los certificados de TSU emitidos.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- Cualquier responsabilidad que se establezca por la legislación vigente.

2.2.1 Exoneración de responsabilidad

La TSA no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor
- Por el uso de los certificados de TSA siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Certificación
- Por el uso indebido o fraudulento de los sellos de tiempo o CRL's emitidos por la TSA.
- Por el incumplimiento de las obligaciones establecidas para el Suscriptor o usuario en la normativa vigente, en la presente Política de Certificación, en las Prácticas Correspondientes o en los contratos establecidos por las partes.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación.
- Fraude en la información presentada por el solicitante

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones y responsabilidad financiera

La TSA no se responsabilizará de las pérdidas por transacciones. La TSA no asume ningún tipo de responsabilidad financiera tales como reembolsos, extensiones de garantías, indemnizaciones ni por fuerza mayor.

3 REQUISITOS DE LAS PRÁCTICAS DE TSA

3.1 Manifiesto de prácticas y divulgación

Salmón Corp cumple los requerimientos de la *RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs)*, conforme a lo exigido en la Guía de Acreditación de Entidades de Valor Añadido del INDECOPI, en su calidad de entidad de Entidad Emisora de Sellos de Tiempo.

3.1.1 Declaración de Practicas de la TSA

Salmón Corp demuestra que cuenta con la confiabilidad necesaria para proveer los servicios de sellado de tiempo a sus clientes, a través del sometimiento de sus servicios a la evaluación provista por el INDECOPI como Autoridad Administrativa Competente.

Los certificados e infraestructura de software y hardware utilizados en los servicios de emisión de sellos de tiempo son provistos por Camerfirma, quien es auditada periódicamente respecto del cumplimiento de todas las certificaciones y acreditaciones que posee respecto a la prestación del servicio por entidades de prestigio acreditadas para ello.

Las evidencias de estas auditorías serán presentadas al INDECOPI en cada sesión de auditoría periódica.

La presente Declaración de Prácticas de Registro es administrada por SALMON CORP S.A.C., cada nueva versión será presentada al INDECOPI y luego de su aprobación, será debidamente publicada en la siguiente dirección:

https://www.salmoncorp.com/wp-content/uploads/2022/08/VAPS-de-Sellado-de-tiempo-Salmon-v1.1-1.pdf

3.1.2 Declaración Informativa de la TSA-TSU.

La TSA informará a todos los suscriptores y potenciales usuarios, los términos y condiciones sobre el uso del servicio de sellado de tiempo. En particular, esta declaración al menos especificará:

- Contacto de la TSA
- Política de sello de tiempo aplicada
- Al menos un algoritmo resumen que se utilizara para representar a los datos a sellar en tiempo.
- Tiempo estimado de validez de la firma usada para firmar el token de tiempo. (Depende del algoritmo resumen usado el algoritmo de firma usado y la longitud de la clave).
- La exactitud de la fuente de tiempo empleada respecto a UTC.
- Cualquier limitación en el uso del servicio.
- Las obligaciones del suscriptor.
- Las obligaciones de las partes confiantes
- Información de cómo verificar los sellos de tiempo de forma que un usuario puede considerar razonable confiar en un sello de tiempo y cualquier posible limitación en la validez de este.

4 GESTIÓN DE CLAVES DE LA TSA

4.1 Generación de claves de la TSA

La generación de la clave privada del certificado digital con el cual se firman los sellos de tiempo es realizada bajo un estricto control en un ambiente físico seguro conforme a la sección 7.4.4 de la RFC 3628 y por personal confiable conforme a la sección 7.4.3 de la RFC 3628 bajo, al menos, autorización de dos personas, conforme a la sección 3.1.1 de la *Política de Certificación Camerfirma para Sello de Tiempo*.

La generación de la clave privada se realiza en un módulo hardware de seguridad – HSM con certificaciones FIPS 140-1 nivel 3 y su administración es protegida por al menos dos personas, conforme a la sección 3.1.2 de la *Política de Certificación Camerfirma para Sello de Tiempo*..

4.2 Protección de la clave privada de la TSA-TSU

La TSA se asegurará que la clave privada permanece confidencial y mantiene su integridad. Para ello, la clave privada del certificado de firma de cada sello de tiempo es resguardada durante su uso dentro de un módulo hardware criptográfico con certificación FIPS 140-1 nivel 3.

A pesar de que no se recomienda la copia de seguridad de las claves privadas para minimizar el riesgo de compromiso de clave. Si se realiza la copia de seguridad, se utilizara tanto para la copia como la restauración de la clave un entorno seguro así como al menos el concurso de dos personas cualificadas y confiables, encargadas expresamente para realizar estas operaciones conforme a la sección 3.1.2 de la *Política de Certificación Camerfirma para Sello de Tiempo*..

4.3 Distribución de la clave publica de la TSA-TSU

LA TSA se asegurará que en la distribución de las claves públicas se garantice su integridad y autenticidad. Para ello, la clave pública está contenida dentro de un certificado X.509 v3, firmada digitalmente por una Entidad de Certificación Digital de Camerfirma regulada por la *Declaración de Prácticas de Certificación Certificados Digitales AC Camerfirma SA*.

La clave pública de verificación se pondrá a disposición de las parte confiantes a través de la dirección web corporativa: https://www.camerfirma.com/certs/camerfirma_tsaii-2014.crt

4.4 Cambio de claves de TSU

El periodo de validez de las claves privadas del certificado de firma de cada sello de tiempo no será superior al periodo de tiempo que los algoritmos criptográficos elegidos sean adecuados para este uso.

La clave privada será remplazada antes de la expiración de su periodo de validez y en caso de obsolescencia o vulnerabilidad declarada del algoritmo, el tamaño de la clave u otra medida de seguridad relevante, conforme a la sección 3.1.4 de la *Política de Certificación Camerfirma para Sello de Tiempo.*

4.5 Re emisión de la clave de TSA-TSU.

No aplica.

4.6 Fin del ciclo de vida de la clave de TSA-TSU.

La TSA garantizará que la clave privada de la TSA-TSU no será usada después del final de su ciclo de vida. En este caso, terminado su ciclo de vida, será emitida una nueva clave y puesta en operación, realizando el cambio de un certificado digital por otro, incluyendo la generación segura y la publicación del nuevo certificado.

En particular, la TSA garantiza para el fin del ciclo de vida de la clave de TSA-TSU:

- Que se utilizaran procedimientos técnicos y operacionales seguros y de conformidad con la RFC 3628 para generar nuevas claves cuando la actual caduca.
- La clave privada de la TSA-TSU o cualquier parte de ella, es destruida completamente de tal forma que no pueda ser recuperada.
- El sistema no permitirá la emisión de un sello de tiempo firmado con una clave privada de TSU caducada, ni que se firme un certificado de TSU con una clave privada de TSA caducada.

La AC deberá 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.

La destrucción o deshabilitación de las claves se detallará en un documento creado

al efecto.

4.7 Gestión del ciclo de vida del dispositivo criptográfico usado para firmar los sellos de tiempo

Los módulos hardware criptográficos que se utilizan para almacenar y proteger las claves privadas con las cuales se firman los sellos de tiempo reconocidos por Salmón Corp, son protegidos contra manipulación no autorizada durante todo su ciclo de vida, incluyendo transporte, generación de la clave, uso y almacenamiento. Los controles son descritos en la sección 3.1.6 de la *Política de Certificación Camerfirma para Sello de Tiempo.*

La instalación, activación y duplicación de las claves de la TSU en el hardware criptográfico sólo puede ser realizada por el personal que tiene asignado un rol de confianza, usando al menos un control dual en un ambiente físico seguro (conforme a la sección 7.4.4 de la RFC 3628) con control de acceso físico de al menos dos personas.

Cuando sea necesario desechar el equipo, las claves privadas de la TSA serán borradas para evitar su uso no autorizado. Considerando el respaldo seguro de la clave si aún se encuentra vigente.

4.8 Revocacion de certificados

Se entenderá por revocación aquel cambio en el estado de un certificado motivado por la pérdida de validez de un certificado en función de alguna circunstancia distinta a la caducidad del mismo. Al hablar de revocación nos referiremos siempre a la pérdida de validez definitiva.

4.8.1 Causas de revocación

Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Suscriptor del sello de tiempo.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del Suscriptor del sello de tiempo (si es persona física) o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos.
- Terminación o extinción de la entidad.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el Solicitante para la obtención del certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Resolución de la TSA indicando que el certificado no se ha emitido siguiendo los términos y condiciones marcadas por las políticas de certificación correspondientes.
- Pérdida de los derechos de la TSA para emitir certificados bajo esta política.
- La TSA es consciente de que el Suscriptor del sello ha sido añadido a una lista de personas no autorizadas o insolventes, o está operando desde un lugar donde la política de la AC impida la emisión de certificados.
- Que se detecte que las claves privadas del Suscriptor del Sello de tiempo o de la TSA han sido comprometidas, bien porque concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualesquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al Suscriptor del Sello.
- Por incumplimiento por parte de la TSA, del Solicitante o el Suscriptor del Sello de tiempo de las obligaciones establecidas en esta política.
- Por la resolución del contrato con el Suscriptor del Sello de tiempo.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la presente política.

4.8.2 Quien puede solicitar la revocación

El representante de la Entidad

EL Suscriptor del Sello de tiempo

La TSA.

4.8.3 Procedimiento de solicitud de revocación

La revocación de un certificado podrá solicitarse únicamente por el representante de la Entidad, por el Suscriptor del Sello de tiempo mediante solicitud a la TSA. Todas las solicitudes deberán ser en todo caso autenticadas.

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son revocados basándose en peticiones de revocación autorizadas y validadas. La información relativa al retraso máximo entre la recepción de una petición de revocación y su publicación estará disponible como máximo en un periodo de 3 horas.

El Suscriptor del Sello de tiempo cuyo certificado haya sido revocado deberá ser informado del cambio de estado de su certificado. Así mismo, el Suscriptor del Sello de tiempo deberá ser informado del levantamiento de la suspensión. La TSA utilizará todos los medios a su alcance para conseguir este objetivo, pudiendo intentar la mencionada comunicación por e-mail, teléfono, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

Una vez que un certificado es revocado, este no podrá volver a su estado activo. Larevocación de un certificado es una acción, por tanto, definitiva.

La CRL, en su caso, será firmada por una AC emisora de certificados de TSU o por una autoridad de confianza de la TSA.

El servicio de gestión de las revocaciones estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la TSA, la TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

La información relativa al estado de la revocación estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la TSA, la TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información se encuentre disponible.

Se deberán realizar los esfuerzos que razonablemente estén a su alcance para confirmar la autenticidad y la confidencialidad de la información relativa al estado de los certificados.

La información relativa al estado de los certificados deberá estar disponible públicamente.

5 SELLADO DE TIEMPO

5.1 Tokens de sello de tiempo

Los sellos de tiempo de Salmón Corp cumplen lo siguiente, conforme a la sección 6.1 de la *Política de Certificación Camerfirma para Sello de Tiempo*:

- Los sellos de tiempo son conformes a la RFC 3161.
- El sello de tiempo incluye un identificador de la política de sello de tiempo, en concordancia con la TSA y la TSU de Camerfirma.
- El sello de tiempo será firmado por una clave generada para este propósito, correspondiente a la TSA de Camerfirma
- Cada sello de tiempo tiene asignado un único identificador
- El sello de tiempo incluye un resumen de los datos firmados (HASH)
- Se utiliza un servicio de sincronización a la fuente de tiempo confiable
- El tiempo incluido en el sello de tiempo será sincronizado con la UTC dentro de la exactitud de +/- 1 segundo.
- Si se detecta que el reloj del proveedor del sello de tiempo se encuentra fuera de la precisión indicada los sellos de tiempo no deben emitirse

5.2 Sincronización del reloj con UTC

El servicio de sincronización de tiempos estará compuesto por tres fuentes distintas conforme a la sección 6.1.6 de la *Política de Certificación Camerfirma para Sello de Tiempo* de modo que se adoptan medidas para asegurar que su reloj es sincronizado con la UTC dentro de la exactitud declarada:

- NTP del ROA (Real Observatorio de la Armada, que establece la hora oficial en España) vía RedIris.
- GPS sincronizado con 3 satélites. Precisión milisegundos.
- Sincronización de tiempos vía Radio DCF77 con la estación transmisora en Mainflingen (Frankfurt). La precisión 10 mseg.

El sistema calculará el tiempo en base a estas tres fuentes. El reloj del ordenador se controlará de acuerdo con los algoritmos de selección y sincronización de la RFC 1305 (NTP v3).

La calibración de los relojes será monitorizada y mantenida de modo que no se desvíen de la precisión de +/- 1 segundo. En caso de desviación, se informará a los terceros que confían afectados mediante una publicación en la página web de Salmón Corp o mediante correo electrónico a los clientes del servicio, a fin de que estos comuniquen a los terceros que confían.

Cuando un cambio en el tiempo sea notificado por una autoridad competente, los respectivos cambios serán realizados el último minuto del día cuando el cambio en el tiempo haya sido planificado. En este escenario se mantendrá un registro del tiempo exacto (dentro de la exactitud declarada) y será notificado a los terceros que confían del mismo modo que lo indicado para el caso de desviaciones.

La precisión de la fecha y hora incorporada en los sellos de tiempo basadas en el sistema UTC con una desviación máxima de retardo de 100ms.

Ante alguna falla se realizarán procedimientos de calibración, que lo realiza la entidad de certificación.

5.3 Comunicaciones

El método de comunicación entre las entidades y el servicio de sellado de tiempo de

Camerfirma se realizará:

Mediante protocolo HTTP/HTTPS con autentificación en cliente, con el fin de poder validar las peticiones realizadas.

Mediante usuario y contraseña.

Las comunicaciones con los suscriptores son mediante correo electrónico.

6 GESTIÓN Y OPERACIONES DE LA TSA

6.1 Gestión de la seguridad

Las medidas de seguridad adoptadas para proteger los activos críticos que sostienen los servicios de sellado de tiempo son señaladas en las secciones 4 y 5 de la *Política de Certificación Camerfirma para Sello de Tiempo* que se encuentra disponible para todo el personal, proveedores y clientes, y en particular a lo referente a:

- Dirección y gestión de la seguridad
- Gestión y clasificación de activos
- Controles de seguridad de personal
- Controles de seguridad física y ambiental
- Gestión de operaciones
- Gestión de accesos
- Implementación de sistemas fiables y mantenimiento

6.1.1 Auditorias y detección de intrusiones

El responsable de Seguridad Informática realizará revisiones periódicas de todas las áreas dela Organización a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

- Sistemas de información.
- Proveedores de sistemas.
- Propietarios de información.
- Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

6.1.2 Controles de auditoria de sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

a. Acordar con el Área que corresponda los requerimientos de auditoría.

b. Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.

c. Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:

- Eliminar archivos transitorios.

- Eliminar entidades ficticias y datos incorporados en archivos maestros.
- Revertir transacciones.
- Revocar privilegios otorgados

d. Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, la Unidad de Auditoría o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

e. Identificar y acordar los requerimientos de procesamiento especial o adicional.
f. Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:

- Fecha y hora.
- Puesto de trabajo.
- Usuario.
- Tipo de acceso.
- Identificación de los datos accedidos.

g. Estado previo y posterior. g. Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.
    -

6.2 Compromiso de los servicios TSA

La TSA ha establecido las medidas de seguridad adecuadas para evitar el compromiso de las claves privadas de la TSA. A pesar de ello, la TSA ha elaborado un Plan de continuidad de negocio donde se contempla como escenario de desastre el compromiso o la sospecha de compromiso de las claves privadas de la TSA. Es este supuesto, la TSA deberá realizar los esfuerzos que razonablemente están a su alcance para restablecer las claves tan pronto como sea posible.

En caso de compromiso, la TSA tomará como mínimo las siguientes medidas:

- Informar a todos los suscriptores, usuarios y otras TSAs con los cuales tenga acuerdos u otro tipo de relación del compromiso.
- Indicar que los certificados e información relativa al estado de la revocación firmados usando esta clave pueden no ser válidos.
- Ante perdida de la precisión del reloj, compromiso del mismo o sospecha de compromiso en el tiempo de la TSA; SALMON dejará esta información a los suscriptores y terceros que confían indicando la descripción del evento. Esta comunicación será directa o a través de su sitio web

La TSA debe restablecer los servicios de acuerdo con esta política dentro de las 48 horas posteriores a un desastre o emergencia imprevista. Tal plan incluirá una prueba completa y periódica de la preparación para tal restablecimiento.

6.3 Cese de la TSA

La TSA deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se minimizan los posibles perjuicios que se puedan crear a los suscriptores o terceros como consecuencia del cese de su actividad y en particular del mantenimiento de los registros necesarios a efectos probatorios en los procedimientos legales. En particular, antes del cese de su actividad deberá realizar, como mínimo, las siguientes actuaciones:

- Informar a todos los suscriptores, usuarios y otras TSA s con los cuales tenga acuerdos u otro tipo de relación del cese de su servicio de sellado de tiempo.
- La TSA revocará toda autorización a entidades subcontratadas para actuar en nombre de la TSA en el procedimiento de emisión de certificados.
- La TSA realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los logs incluyendo la obligación de mantener disponible su clave pública o certificado durante el periodo de tiempo indicado a los suscriptores y usuarios que confían.
- Las claves privadas de la TSA serán destruidas o deshabilitadas para su uso.
- La TSA tendrá contratado un seguro que cubra hasta el límite contratado los costes necesarios para satisfacer estos requisitos mínimos en caso de quiebra o por cualquier otro motivo por el que no pueda hacer frente a estos costes por sí mismo.

6.4 Cumplimiento legal

Salmón Corp, como Autoridad emisora de sellos de tiempo, cumple los requerimientos establecidos en la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, el Reglamento y la Ley de Firmas y Certificados Digitales -Ley27269 y exige a Camerfirma el cumplimiento de la RFC 3628.

Salmón Corp no recoge información personal de los usuarios (personas naturales) de los servicios de sellado de tiempo ya que estas transacciones no implican firma digital del usuario final.

La invalidez de una de las cláusulas contenidas en esta Política de Certificación no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

Cualquier notificación referente a la presente Política de Certificación se realizará por correo electrónico o mediante correo certificado dirigido a la dirección referida en el apartado Conformidad y Contacto.

6.4.1 Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento será notificada a la Autoridad de las Políticas (PA) mediante correo electrónico o mediante correo certificado dirigido a la dirección referida en el apartado Conformidad y Contacto para que puedan establecerse las acciones necesarias para la resolución del conflicto.

En caso de mantenerse el conflicto se resolverá definitivamente, mediante el arbitraje de la Autoridad Administrativa Competente (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI) atendiendo a lo dispuesto en el Reglamento de la Ley de Firmas y Certificados Digitales (D.S. 052-2008-PCM) en su artículo 57º apartado l) en la que se establece como una de sus funciones la de impulsar la solución de conflictos por medio de la conciliación y el arbitraje. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

6.5 Almacenamiento de los registros de operación de la TSA

Los registros concernientes a la operación del servicio de sellado de tiempo, incluyendo eventos relacionados a la sincronización del reloj con la fuente confiable de tiempo y la gestión de las claves de la TSA son salvaguardados de la misma manera que son protegidos los registros de la operación de la Entidad de Certificación de Camerfirma, los cuales son descritos en la sección 4.6 de la *Declaración de Prácticas de Certificación Certificados Digitales AC Camerfirma SA*

Los registros son almacenados y protegidos por un periodo de 5 años. En caso que la clave privada de la TSA se vea comprometida, entonces el periodo de almacenamiento de registros será mayor que los sellos de tiempo más afectados.

6.6 Aspectos organizativos

La TSA se asegurará de que su organización es confiable. En particular, para ello se asegurará que:

- La Autoridad de las Políticas vela porque las políticas y procedimientos bajo los cuales opera la TSA no sean discriminatorios.
- La TSA presta sus servicios de forma que sean accesibles para todos los usuarios dentro del ámbito de aplicación y se compromete a respetar sus obligaciones según lo especificado en la Política de Sellado de Tiempo.
- Salmón Corp se encuentra legalmente constituida de acuerdo con la legislación nacional.
- La TSA cuenta con un sistema de gestión de seguridad de la información acorde a la norma ISO 27001 apropiada para los servicios de sellado de tiempo que proporciona.
- La TSA cuenta con mecanismos adecuados para cubrir las responsabilidades derivadas de sus operaciones y / o actividades.
- Tiene la estabilidad y los recursos necesarios para operar de conformidad con esta política.
- Se emplea un número suficiente de personal con la educación, la formación, conocimientos técnicos y experiencia en relación con el tipo y volumen de trabajo necesario para proporcionar servicios de sellado de tiempo necesario.
- Se cuenta con procedimientos para la resolución de quejas y controversias recibidas de los clientes u otras partes acerca de la provisión de los servicios de sellado de tiempo u otros asuntos relacionados.
- Tiene un acuerdo contractual debidamente formalizado que permita cumplir con lo dispuesto en la presente política de sello de tiempo cuando se emplean terceros para la provisión de los servicios subcontratados.

6.7 Conformidad

Este documento ha sido aprobado por la Autoridad de la TSA de Salmón Corp, y tiene carácter normativo sobre todos los servicios de sellado de tiempo, por lo que cualquier incumplimiento por parte de las personas mencionadas en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

6.8 Procedimiento de gestión documental

Todo procedimiento operativo y de seguridad deben ser documentados.

6.9 Planificacion el sistema

La demanda deberá ser monitoreadas y se realizaran proyecciones futuras de las mismas.

6.10 Manejo de medios de seguridad

Los activos de la TSA de sALMON tienen nivel de protección. Para ello la TSA realiza anualmente un análisis de riesgos siguiendo una metodología de riesgos. En este análisis se ha levantado el inventario de los activos existentes en el proceso de sello de tiempo, junto con su clasificación de riesgo. Producto de lo anterior la TSA se generó plan de seguridad

6.11 Reporte de incidencias y respuesta

La TSA responderá de manera inmediata y coordinada para dar respuesta rápidamente a los incidentes y para reducir el impacto de los fallos de seguridad. Todos los incidentes serán reportados con posterioridad al incidente tan pronto como sea posible.

6.12 Riesgo de intercambio de información

SALMON evalúa los riesgos del intercambio de información que realiza, de acuerdo a la clasificación de la información que es intercambiada; y a partir de este análisis se determina el medio a utilizar para el intercambio.

6.13 Mantenimiento e implementación de sistemas de confianza

La TSA asegura que sus sistemas y productos están protegidos contra modificaciones no autorizadas.
Para ello, la TSA de SALMON y su PSC previo a cualquier cambio en sus sistemas o productos lleva a cabo:

Un análisis de requerimientos de seguridad es llevado a cabo durante el diseño y especificación de requerimientos. Es así como, cuando se pongan en marcha los proyectos para el desarrollo e implantación de nuevos sistemas, o ampliación/mejora de los ya existentes, además de las actividades tradicionales de cada una de las fases de éstos, se llevarán a cabo igualmente las actividades para determinar e implementar los requerimientos de seguridad necesarios.
Esto ocurrirá tanto cuando se vaya a adquirir un producto o cuando
este se desarrolle internamente; estableciendo igualmente los requerimientos de seguridad que debe cumplir y revisando dicho cumplimiento antes de su compra o desarrollo.

6.14 Control de cambios

Un procedimiento de control de cambio para nuevas versiones, modificaciones y/o correcciones de emergencia al software. El propósito de este Procedimiento es establecer las actividades necesarias para llevar a cabo los cambios y actualizaciones en los sistemas de una manera eficiente, incluido las nuevas versiones y los pasos a producción, minimizando el impacto y las incidencias que se puedan producir debido a ellos. SALMON documenta estos pasos a través de su Procedimiento de Gestión de Cambio.

6.15 Procedimiento de control de seguridad

El prestador de los servicios deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relevante concerniente a los servicios descritos en este documento es gestionada y protegida de forma segura durante el periodo de tiempo que pueda ser necesario a efectos probatorios en los procedimientos legales utilizando los medios ajustados al estado del arte en seguridad de la información.
Al ser procedimientos comunes a otros servicios de emisión, se desarrollará en la DPC correspondiente, los aspectos relativos a los procedimientos de Control de seguridad, cubriendo los siguientes aspectos:

- Archivo de registros
- Análisis de vulnerabilidades
- Gestion de contingencias
- Controles de Seguridad física
- Controles procedimentales
- Controles de seguridad de personal
- Controles de Seguridad Técnica de las claves.
- Controles de seguridad informática
- Controles de gestión de la seguridad
- Controles de seguridad de la red
- Controles de ingeniería de los módulos criptográficos

6.16 Registro de información concerniente a las operaciones del servicio de sello de tiempo

La TSA de SALMON mantiene registros de la información relevante, concerniente a su operación. La
información personal de los suscriptores, que ha recolectado la PSC de Camerfirma como parte de su
operación, está protegida de acuerdo con la Política de Privacidad de datos personales publicados por
SALMON en su sitio web.

6.17 Registros concernientes

Todos los registros concernientes a la operación del servicio de sello de tiempo se encuentran disponibles sólo al suscriptor o en caso que lo solicite una corte a través de un requerimiento legal. Lo anterior a fin de proteger la confidencialidad de dichos datos. La integridad de esta información es mantenida por la PSC de Camerfirma por un periodo de al menos 5 años posterior a la expiración de la validez de la llave usada para la firma por parte de la TSU. Estos registros incluyen:

Requerimiento de sello de tiempo

- Sello de tiempo creado
- Eventos relacionados con la administración de la TSA, incluyendo:
- Registros de eventos correspondientes al ciclo de vida de las llaves de la TSU
- Registros de eventos correspondientes a los certificados de la TSU
- Registros relacionados con la sincronización del reloj de usado por la TSU en sus TST
- Registros asociados a eventos de detección de pérdida de sincronización

Los registros antes mencionados, son almacenados por SALMON y no son de fácil eliminación o destrucción dentro del periodo de tiempo previamente declarado. A estos registros, sólo tiene acceso el personal autorizado por la PSC de Camerfirma.

6.18 Auditoria

El servicio de TSA es evaluado en el alcance de la certificación ISO27001 que anualmente realiza AC Camerfirma SA.

El auditor debe poseer conocimientos y experiencia en sistemas de PKI y en seguridad de sistemas informáticos.

La auditoría deberá ser realizada por un auditor independiente y neutral.

Lo anterior no impedirá la realización de auditorías internas periódicas.

La auditoría deberá verificar en todo caso:

- Que la TSA tiene un sistema que garantice la calidad del servicio prestado.
- Que la TSA cumple con los requerimientos de esta Política de Certificación.
- Que las Prácticas de Certificación de la TSA se ajustan a lo establecido en esta Política, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.

7 ANEXO I. ACRÓNIMOS Y DEFINICIONES

7.1 Acrónimos y abreviaturas

TSA	Autoridad de Sellado de Tiempo
TSU	Unidad de sellado de tiempo
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DSCF	Dispositivo seguro de creación de firma
FIPS	Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
ITU	International Telecommunications Union. Unión Internacional de Telecomunicaciones
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PKI	Public Key Infrastructure. Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA-1	Secure Hash Algorithm. Algoritmo seguro de Hash

7.2 Definiciones

Autoridad de Certificación:	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el usuario, vinculando una determinada clave pública con una persona.
Autoridad de políticas:	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y CPS.

Autoridad de Registro:	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
Certificación cruzada:	El establecimiento de una relación de confianza entre dos TSA 's, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes.
Certificado:	Archivo que asocia la clave pública con algunos datos identificativos del suscriptor y es firmada por la TSA.
Clave pública:	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada datos de verificación de firma.
Clave privada:	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada datos de creación de firma. La clave privada de la TSA será usada para firma de certificados y firma de CRL's
CPS:	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.
CRL:	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la TSA.
Datos de Activación:	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada
DSADCF:	Dispositivo seguro de almacén de los datos de creación de firma. Elemento software o hardware empleado para custodiar la clave privada del suscriptor de forma que solo él tenga el control sobre la misma.
DSCF:	Dispositivo Seguro de creación de firma. Elemento software o hardware empleado por el suscriptor para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el suscriptor.
Entidad:	Dentro del contexto de las políticas de certificación de Salmón Corp, aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el suscriptor.
Firma digital:	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a) que los datos no han sido modificados (integridad) b) que la persona que firma los datos es quien dice ser (identificación) c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)

OID: Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.

Par de claves: Conjunto formado por la clave pública y privada, ambas relacionadas entre si matemáticamente.

PKI: Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.

Política de certificación: Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes

Suscriptor: Persona natural o jurídica que requiere los servicios provistos por una Autoridad emisora de sellos de tiempo – TSA y que está de acuerdo con los acuerdos y obligaciones descritos en la Política de Sellado de Tiempo.

Tercero que confía o usuario: Dentro del contexto de las políticas de certificación de Salmón Corp, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado