Declaración de prácticas TSA y Políticas de Sellado de tiempo

TimeStamping

Av. 12 de octubre N24-739 y Av. Colon - Ed. Torre Boreal
170143 - Quito (Ecuador)
Teléfono: +593 02 3826877

Web: www.anf.ec

Nivel de Seguridad

Documento Público

Aviso Importante

Dirección: Av. 12 de Octubre N24-739 y Av. Colon - Ed. Torre Boreal 170143 - Quito (Ecuador)

Índice

1. Introducción

1.1. Visión general

El sello de tiempo electrónico es un conjunto de datos en formato electrónico que vincula otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante, por lo tanto, documenta el "cuándo" y "qué".

Una firma electrónica, a menudo referida como la firma personal, documenta el "quién" y "qué". En contraste con la firma electrónica, un sello de tiempo no está vinculado a las personas y sus acciones. Por lo tanto, puede integrarse de manera más sencilla y también de forma completamente automática en los procesos electrónicos.

Con el fin de verificar una firma electrónica, puede ser necesario demostrar que la firma del firmante se aplicó cuando el certificado del firmante era válido. Esto es necesario en dos circunstancias:

1. Durante el período de validez del certificado, el firmante puede revocarlo antes del fin de su vigencia, por ejemplo, porque la clave privada haya sido comprometida.
2. Después del final del período de validez del certificado, las entidades emisoras no están obligadas a procesar la información de estado de revocación más allá de dicho período.

Un sello de tiempo permite demostrar que un dato existía antes de un momento determinado. Esta técnica permite acreditar que la firma o el documento electrónico al que se asocia fue generado antes de la fecha consignada en el sello de tiempo.

ANF AC Autoridad de Certificación Ecuador C.A. es una entidad jurídica ecuatoriana, acreditada por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) para la prestación del servicio de sellado de tiempo electrónico, en su calidad de Entidad de Certificación Acreditada (ECA) conforme a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 67, 2002), su Reglamento General (Decreto Ejecutivo 3496, Registro Oficial 735, de 31 de diciembre de 2002), la Ley Orgánica de Telecomunicaciones (LOT) y la Resolución ARCOTEL-2024-0176 – Norma Técnica para la Prestación de los Servicios de Información y Servicios Relacionados de las Entidades de Certificación Acreditadas y Terceros Vinculados.

El presente documento especifica la política y los requisitos de seguridad relacionados con las operaciones y las prácticas de gestión de ANFAC Autoridad de Certificación Ecuador C.A. – Autoridad de Sellado de Tiempo (en adelante, ANF AC Ecuador TSA), para la emisión de sellos de tiempo electrónicos cualificados, así como las condiciones de uso, obligaciones y responsabilidades de las distintas entidades involucradas.

Este servicio se ajusta a:

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 67, 2002);

- Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos;
- Ley Orgánica de Telecomunicaciones (LOT);
- Resolución ARCOTEL-2024-0176;
- Ley Orgánica de Protección de Datos Personales (2021);
- Ley Orgánica para la Transformación Digital y Audiovisual (2022);
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles;
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;
- ETSI TS 119 312: Cryptographic Suites;
- IETF RFC 3161: Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP).

El servicio de sellado de tiempo electrónico de ANF AC Ecuador TSA se fundamenta en el cumplimiento de los principios de fiabilidad técnica, interoperabilidad e independencia, garantizando la sincronización de su fuente temporal con el Tiempo Universal Coordinado (UTC) conforme a los estándares internacionales definidos por la Unión Internacional de Telecomunicaciones (UIT-T) y los lineamientos emitidos por la ARCOTEL.

ANFAC Autoridad de Certificación Ecuador C.A.. en calidad de Entidad Certificadora Acreditada, hace uso de la estructura de la casa matriz, ANF Certification Authority, S.L, Prestador Cualificado de Servicios de Confianza ya certificado en conformidad con el reglamento eIDAS y las normas ETSI antes mencionadas para prestar sus servicios. Este Prestador Cualificado será referido en lo adelante como “Tercera Parte Certificada” o por simplicidad “Tercera Parte”.

El presente documento puede ser utilizado por organismos de evaluación y auditoría designados por la ARCOTEL como base para confirmar que ANF AC Ecuador TSA cumple con los requisitos técnicos y normativos aplicables para la emisión de sellos de tiempo electrónicos cualificados en la República del Ecuador.

El presente documento no especifica:

- Los protocolos utilizados para acceder al servicio de sellado de tiempo de ANF AC Ecuador TSA;
- La forma en que los requisitos especificados en este documento pueden ser evaluados por un organismo independiente;
- Los requisitos para poner a disposición la información a dichas entidades independientes;
- Los requisitos que deben cumplir dichos organismos;
- Ni los requisitos correspondientes a la custodia de evidencias o preservación cualificada a largo plazo de firmas y sellos electrónicos, salvo que se contrate expresamente el servicio cualificado correspondiente.

Los certificados raíz y los certificados técnicos necesarios para el funcionamiento de la infraestructura de clave pública (PKI) de ANF AC Ecuador se encuentran disponibles en el repositorio legal de la entidad: https://www.anf.ec/repositorio-legal/

En caso de conflicto entre la presente Declaración de Prácticas TSA y Política de Sellado de Tiempo (ANF AC Ecuador) y la Declaración de Prácticas de Certificación (DPC) ANF AC Ecuador, prevalecerá lo dispuesto en la Declaración de Prácticas TSA en lo relativo al servicio de sellado de tiempo electrónico.

En caso de existir versiones en diferentes idiomas, prevalecerá la versión en español como texto jurídico oficial en el territorio ecuatoriano.

1.2. Nombre del documento e identificación

Nombre del documento	Declaración de Prácticas TSA y Política de Sellado de tiempo *(Timestamping)*		
Versión	1.0		
OID	1.3.6.1.4.1.37442.15.1		
Fecha de aprobación	09/10/2025	Fecha de publicación	09/10/2025

1.2.1. Revisiones

Versión	Cambios	Aprobación	Publicación
1.0	Versión inicial del documento.	02/06/2023	02/06/2023

1.3. Definiciones y acrónimos

1.3.1. Definiciones

Para efectos del presente documento, se aplican tanto las definiciones dadas en la Declaración de Prácticas de Certificación (DPC) de ANFAC Autoridad de Certificación Ecuador C.A., como las siguientes:

Autoridad de Sellado de Tiempo (TSA): Es la entidad de certificación acreditada que presta servicios de sellado de tiempo electrónico utilizando una o varias Unidades de Sellado de Tiempo (TSU), conforme a los requisitos técnicos, organizativos y de seguridad establecidos en la Resolución ARCOTEL-2024-0176 y en las normas ETSI EN 319 421 y ETSI EN 319 422.

Declaración de divulgación de la TSA: Conjunto de declaraciones acerca de las políticas y prácticas de la TSA que requieren especial énfasis en su divulgación a los suscriptores y a las partes que confían, por ejemplo, para cumplir los requisitos normativos establecidos por la ARCOTEL.

Declaración de prácticas de la TSA: Documento que describe las prácticas aplicadas por la TSA en la emisión de sellos de tiempo electrónicos cualificados, así como los controles técnicos, de seguridad y organizativos empleados en su operación.

Función Hash: Es una operación matemática que se aplica sobre un conjunto de datos de cualquier tamaño, generando un valor de longitud fija (resumen o "hash") que identifica unívocamente el contenido original. Cualquier modificación de los datos genera un valor diferente, garantizando la integridad de la información.

Módulo criptográ8co hardware (HSM): Dispositivo de seguridad certificado conforme a lo establecido en la norma ETSI EN 319 421 y estándares internacionales FIPS 140-2/3, utilizado para generar, custodiar y proteger claves criptográficas en modo seguro, y para firmar electrónicamente los sellos de tiempo emitidos por las TSU.

NTP (Network Time Protocol): Protocolo de Internet utilizado para sincronizar los relojes de sistemas informáticos mediante el enrutamiento de paquetes en redes con latencia variable. El estándar de referencia es IETF RFC 1305 (NTP v3) y sus actualizaciones.

Política de sello de tiempo: Conjunto de reglas que define la aplicabilidad de un sello de tiempo a una comunidad o clase particular de servicios de confianza, y los requisitos de seguridad asociados. Se considera una política específica dentro de las políticas de servicios de confianza definidas en la norma ETSI EN 319 421.

Prestador de Servicios de Con8anza (TSP): Persona jurídica que proporciona uno o más servicios electrónicos de confianza, incluyendo la emisión de certificados digitales, sellos electrónicos, o servicios de sellado de tiempo, conforme a la legislación ecuatoriana. En el Ecuador, los TSP se denominan Entidades de Certi8cación Acreditadas (ECA) y están bajo la supervisión directa de la ARCOTEL, de acuerdo con el artículo 29 y siguientes de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Instituto Nacional de Metrología del Ecuador (INAMHI ỳ Laboratorio de Tiempo y Frecuencia): Organismo técnico nacional responsable del mantenimiento y difusión de la escala de tiempo oficial del Ecuador, en coordinación con el Servicio Nacional de Normalización y los laboratorios internacionales adscritos al Bureau International des Poids et Mesures (BIPM). Constituye la referencia nacional para la sincronización con el Tiempo Universal Coordinado (UTC) conforme a los lineamientos de la ARCOTEL.

Sello de tiempo (Time-Stamp): Datos en formato electrónico que vinculan otros datos electrónicos con un instante concreto, aportando la prueba de que dichos datos existían en ese instante y que no han sido modificados desde entonces.

Servicio de sellado de tiempo: Servicio electrónico de confianza que permite emitir sellos de tiempo electrónicos cualificados conforme al marco legal ecuatoriano y los estándares internacionales ETSI EN 319 421 / 422.

Sistema TSA: Conjunto de componentes técnicos, productos de tecnología de la información, infraestructuras y procedimientos operativos empleados para soportar la prestación del servicio de sellado de tiempo.

Suscriptor: Persona natural o jurídica a la que se emite un sello de tiempo y que está obligada a cumplir las condiciones y obligaciones derivadas del contrato de prestación de servicios suscrito con la TSA.

Tercero que confía: Persona natural o jurídica que recibe y confía en un sello de tiempo emitido por la TSA, presumiendo su validez técnica y jurídica conforme a la presente política.

Tiempo Universal Coordinado (UTC): Escala internacional de tiempo basada en el segundo, definida por la International Telecommunication Union ỳ Recommendation ITU-R TF.460-6, que constituye el patrón mundial de referencia para la hora legal. En Ecuador, la hora oficial se determina en relación con el UTC(INAMHI) o el laboratorio nacional designado por el Servicio Ecuatoriano de Normalización (INEN) y validado por la ARCOTEL.

Unidad de Sellado de Tiempo (TSU): Conjunto de hardware y software que se gestiona como una sola unidad, y que posee una única clave activa de firma de sello de tiempo en cada momento, utilizada para firmar los Tokens de Sellado de Tiempo (TST).

UTC(k): Escala de tiempo generada por un laboratorio "k" que mantiene una relación próxima y controlada con el Tiempo Universal Coordinado (UTC), con el objetivo de alcanzar una precisión de ±100 nanosegundos.

1.3.2. Acrónimos

A los efectos del presente documento, las abreviaturas dadas son las siguientes:

Acrónimo	Significado
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones
BIPM	Bureau International des Poids et Mesures
CA	Certification Authority (Autoridad de Certificación)
ECA	Entidad de Certificación Acreditada
ETS	European Telecommunications Standards
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
INAMHI	Instituto Nacional de Meteorología e Hidrología (Laboratorio Nacional de Tiempo y Frecuencia)
INEN	Instituto Ecuatoriano de Normalización
IT	Information Technology (Tecnologías de la Información)
LOT	Ley Orgánica de Telecomunicaciones
MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información
NTP	Network Time Protocol
OID	Object Identifier
PKI	Public Key Infrastructure (Infraestructura de Clave Pública)
RFC	Request For Comments
TAI	International Atomic Time
TSA	Time-Stamping Authority (Autoridad de Sellado de Tiempo)

Acrónimo	Significado
TSP	Trust Service Provider (Prestador de Servicios de Confianza)
TST	Time Stamp Token (Token de Sellado de Tiempo)
TSU	Time-Stamping Unit (Unidad de Sellado de Tiempo)
UIT-T	Unión Internacional de Telecomunicaciones – Sector de Normalización de las Telecomunicaciones
UTC	Tiempo Universal Coordinado
UTC(k)	Escala de tiempo generada por un laboratorio "k" sincronizado con UTC

1.4 Información de contacto

Departamento	Departamento Compliance
Correo electrónico 1	soporte@anf.ec
Correo electrónico 2	asanchez@anf.ec
Dirección	Av. 12 de Octubre N24-739 y Av. Colón - Ed. Torre Boreal,
Localidad	Quito (Ecuador)
Código Postal	170517
Número de teléfono	+593 02 3826877

2. Conceptos generales

El presente documento hace referencia a la Declaración de Prácticas de Certi8cación (DPC) de ANFAC Autoridad de Certi8cación Ecuador C.A., para los requisitos de política genéricos comunes a todos los servicios de certificación y confianza que presta la entidad.
Esta política está dirigida a satisfacer los requisitos del servicio de sellado de tiempo electrónico para validez a largo plazo, aplicable a cualquier uso que requiera una calidad equivalente en términos de precisión temporal, integridad de los datos y fiabilidad del servicio.

La presente política se emite en el marco normativo ecuatoriano definido por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 67, 2002), su Reglamento General (Decreto Ejecutivo 3496, Registro Oficial 735, de 31 de diciembre de 2002), la Ley Orgánica de Telecomunicaciones (LOT) y la Resolución ARCOTEL-2024-0176, que regula la prestación de servicios de certificación, emisión de certificados, registro de datos y sellado de tiempo.

Sin perjuicio de lo anterior, ANFAC Autoridad de Certificación Ecuador C.A. podrá referenciar, cuando resulte aplicable, estándares y recomendaciones internacionales como ISO/IEC, FIPS o RFC, en materia de interoperabilidad y seguridad criptográfica, con el fin de garantizar la compatibilidad técnica y la calidad del servicio.

2.1. Servicios de sellado de tiempo

La prestación del servicio de sellado de tiempo por parte de ANFAC Autoridad de Certi8cación Ecuador C.A. se estructura en los siguientes componentes principales:

- Provisión de sellado de tiempo: Es el componente operativo encargado de la generación de los Tokens de Sellado de Tiempo (TST) mediante las Unidades de Sellado de Tiempo (TSU), utilizando mecanismos criptográficos seguros y sincronización con el Tiempo Universal Coordinado (UTC) a través de fuentes reconocidas.
- Gestión del sellado de tiempo: Es el componente de control encargado de la administración, supervisión, monitoreo y auditoría del funcionamiento del servicio, garantizando que las operaciones se ejecuten conforme a la presente Declaración de Prácticas TSA, la Declaración de Prácticas de Certi8cación (DPC) y los lineamientos técnicos y regulatorios emitidos por la ARCOTEL.

ANFAC Autoridad de Certi8cación Ecuador C.A. TSA asegura la confiabilidad, continuidad y precisión del servicio de sellado de tiempo mediante la aplicación de medidas de seguridad organizativas, técnicas y criptográficas que cumplen con la legislación ecuatoriana vigente y las mejores prácticas internacionales de referencia.

2.2. Participantes del servicio de sellado de tiempo

2.2.1. Entidad de Certificación Acreditada (ECA)

ANFAC Autoridad de Certificación Ecuador C.A. es una Entidad de Certificación Acreditada (ECA) reconocida por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) para la prestación de servicios electrónicos de confianza, conforme a lo dispuesto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 67, 2002), su Reglamento General, la Ley Orgánica de Telecomunicaciones (LOT) y la Resolución ARCOTEL-2024-0176.

En el marco de sus servicios acreditados, ANFAC Autoridad de Certificación Ecuador C.A. provee servicios de sellado de tiempo electrónico, actuando en esta función como Autoridad de Sellado de Tiempo (TSA).

La entidad mantiene la responsabilidad total sobre la gestión, operación y control del servicio, garantizando el cumplimiento de las disposiciones legales, técnicas y de seguridad establecidas por la ARCOTEL y por la presente Declaración de Prácticas TSA.

ANFAC Autoridad de Certificación Ecuador C.A. podrá emplear, bajo su control y supervisión, terceras partes certificadas o infraestructuras técnicas de apoyo para la provisión del servicio, manteniendo en todo momento la responsabilidad sobre su conformidad con los requisitos definidos en este documento.

2.2.2. Autoridad de Sellado de Tiempo (TSA)

La Autoridad de Sellado de Tiempo (TSA) es la unidad operativa de ANFAC Autoridad de Certificación Ecuador C.A. encargada de la generación de los Tokens de Sellado de Tiempo (TST), mediante el uso de una o varias Unidades de Sellado de Tiempo (TSU), que operan en entornos criptográficos seguros y controlados.

Cada TSU se identifica de forma única y cuenta con su propio certificado de clave pública, utilizado exclusivamente para firmar electrónicamente los sellos de tiempo emitidos.

El servicio de sellado de tiempo electrónico está sujeto a los procesos de auditoría y control establecidos por la Resolución ARCOTEL-2024-0176, que dispone:

La realización de auditorías externas de seguridad informática de carácter anual, efectuadas por entidades independientes.

La remisión de los informes de auditoría a la ARCOTEL dentro de los plazos y formatos establecidos.

La notificación inmediata a la autoridad supervisora de cualquier evento que comprometa la seguridad, disponibilidad o integridad del servicio.

ANFAC Autoridad de Certificación Ecuador C.A. TSA podrá operar una o más unidades de sellado de tiempo (TSU) identificables, y se encuentra debidamente identificada en los certificados utilizados por dichas unidades para firmar los sellos de tiempo (TST).

2.2.3. Suscriptor/Cliente

El suscriptor es la persona jurídica o natural a la que se emite un sello de tiempo electrónico, y que está obligada a cumplir las obligaciones derivadas del uso de dicho servicio, conforme a las condiciones establecidas en el presente documento y en el contrato de prestación del servicio de sellado de tiempo suscrito con ANFAC Autoridad de Certificación Ecuador C.A.

Cuando el suscriptor es una organización, compuesta por varios usuarios finales o por un usuario individual, algunas de las obligaciones que se aplican a la organización deberán ser también observadas por dichos usuarios finales.
En cualquier caso, la organización será responsable del cumplimiento de las obligaciones de sus usuarios y, por tanto, asume la responsabilidad de informar y capacitar adecuadamente a los mismos respecto del correcto uso del servicio.

Cuando el suscriptor es un usuario final individual, este será responsable directo del cumplimiento de las obligaciones establecidas para el uso del servicio de sellado de tiempo electrónico.

2.2.4. Terceros que confían

Un tercero que confía es una persona natural o jurídica que actúa confiando en un Token de Sellado de Tiempo (TST) emitido bajo la presente Declaración de Prácticas TSA y Política de Sellado de Tiempo Electrónico de ANFAC Autoridad de Certificación Ecuador C.A.

Una parte que confía puede, o no, ser también un suscriptor, y acepta la validez del sello de tiempo como prueba de la existencia y la integridad de los datos electrónicos en el instante indicado en dicho sello

3. Política de Sellado de Tiempo

3.1. General

ANFAC Autoridad de Certificación Ecuador C.A. TSA, en su calidad de Entidad de Certificación Acreditada (ECA) ante la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), emite Tokens de Sellado de Tiempo (TST) en conformidad con las disposiciones establecidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 67, 2002), su Reglamento General, y la Resolución ARCOTEL-2024-0176, que regula la prestación de los servicios de certificación, incluyendo el sellado de tiempo electrónico.

Las Unidades de Sellado de Tiempo (TSU) operadas por ANFAC Autoridad de Certificación Ecuador C.A. TSA generan exclusivamente sellos de tiempo electrónicos cualificados, no emitiendo sellos de tiempo electrónicos no cualificados.

Cada TSU está identificada de manera unívoca, al encontrarse asociada a un certificado de clave pública emitido por la propia infraestructura de certificación de ANF AC Ecuador. Dicho certificado utiliza un nombre de sujeto distinto, incorporando un número secuencial para diferenciar cada unidad de operación.

Los Tokens de Sellado de Tiempo (TST) emitidos por la TSA se generan con una precisión superior a un (1) segundo respecto al Tiempo Universal Coordinado (UTC), conforme a la sincronización establecida por el Instituto Nacional de Meteorología e Hidrología (INAMHI) o el laboratorio nacional designado por el Instituto Ecuatoriano de Normalización (INEN), bajo control y supervisión de la ARCOTEL.

3.2. Identificador

El identificador de la Política de Sellado de Tiempo Electrónico Cuali8cado, especificado en el presente documento, es el siguiente:

OID 2.16.218.1.1.3.5.1

Para indicar que el sello de tiempo emitido por la TSA es cuali8cado conforme a la legislación ecuatoriana, se incorpora en el campo ‘ Policy“ del TSTInfo uno de los siguientes identificadores:

- 2.16.218.1.1.3.5.1 – Correspondiente a la presente Declaración de Prácticas TSA y Política de Sellado de Tiempo Electrónico de ANFAC Autoridad de Certificación Ecuador C.A.
- 0.4.0.2023.1.1 – Correspondiente a la política de mejores prácticas internacionales (*best-practices-ts-policy*), utilizada como referencia técnica voluntaria.

4. Políticas y Prácticas

4.1. Evaluación de Riesgos

ANFAC Autoridad de Certi8cación Ecuador C.A. TSA lleva a cabo evaluaciones de riesgo de forma regular, con el propósito de garantizar la calidad y fiabilidad de los servicios de sellado de tiempo.

A fin de asegurar su eficacia, se dispone de medidas de salvaguarda y controles de seguridad definidos dentro de un marco de gestión adecuado a la prestación del servicio de sellado de tiempo electrónico.

Con una periodicidad mínima anual, y siempre que se produzca un cambio relevante en la infraestructura o en los procedimientos, se realiza una revisión de las políticas de seguridad y se efectúan auditorías externas de seguridad informática, conforme a los requisitos establecidos por la Resolución ARCOTEL-2024-0176 y las buenas prácticas internacionales publicadas por ISO y FIPS.

4.2 Declaración de Practicas del Servicio de Confianza

Asegurar la calidad del servicio es uno de los valores fundamentales de ANFAC Autoridad de Certi8cación Ecuador C.A. TSA.

La entidad aplica una variedad de controles de seguridad organizativos y técnicos para garantizar la calidad, el rendimiento y el correcto funcionamiento del servicio de sellado de tiempo.

Los controles de seguridad se encuentran documentados y son revisados periódicamente por organismos independientes, empleando personal de con8anza debidamente cualificado para verificar el cumplimiento de los requisitos establecidos en el presente documento.

4.2.1. Formato del sello de tiempo

El token de sello de tiempo electrónico emitido por ANFAC Autoridad de Certificación Ecuador C.A. TSA es compatible con el protocolo RFC 3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol).

Mediante algoritmo RSA con una longitud de clave mínima de 2048 bits, se emiten sellos de tiempo que admiten los siguientes algoritmos de resumen (*hash*):

- SHA256
- SHA384
- SHA512

4.2.2. Exactitud del tiempo

El servicio de sellado de tiempo se presta en Ecuador, donde la fuente de sincronización oficial corresponde al Instituto Nacional de Meteorología e Hidrología (INAMHI), laboratorio reconocido por el Servicio Ecuatoriano de Normalización (INEN) y vinculado al Bureau International des Poids et Mesures (BIPM), responsable del mantenimiento y difusión de la escala del Tiempo Universal Coordinado (UTC) en el territorio ecuatoriano.

El servicio de sellado de tiempo utiliza esta señal de tiempo UTC (INAMHI) y un conjunto de servidores NTP internacionales de referencia (por ejemplo: METAS, GUM, LT, NPL, INRIM, PTB, LNE-SYRTE e ILNAS).

Con dicha configuración, el servicio de sellado de tiempo alcanza una precisión de ±100 milisegundos o superior respecto al UTC.

4.2.3. Limitaciones del servicio

ANFAC Autoridad de Certificación Ecuador C.A. TSA se responsabiliza de la exactitud de la referencia temporal (UTC) incluida en el sello de tiempo electrónico emitido en el momento de la solicitud, pero no de la veracidad ni del contenido de los datos electrónicos remitidos por los suscriptores del servicio, que constituyen el objeto del sello de tiempo.

La entidad no responderá ante los suscriptores o terceros que confíen en el sello de tiempo cuando el uso del servicio haya sido negligente, entendiéndose como tal la falta de observancia de las condiciones establecidas en la presente Declaración de Prácticas TSA, en el contrato de servicio o en los Términos y Condiciones aplicables.

ANFAC Autoridad de Certificación Ecuador C.A. TSA no garantiza los algoritmos criptográficos empleados ni responderá de los daños ocasionados por ataques externos exitosos contra dichos algoritmos, siempre que haya aplicado la diligencia debida y las mejores prácticas tecnológicas vigentes.

La entidad tampoco responderá por software, sistemas o integraciones no proporcionadas directamente, ni por causas de fuerza mayor, caso fortuito, catástrofes naturales, fallos de red, atentados, huelgas o cualquier otra circunstancia que afecte su infraestructura de forma imprevisible.

La cuantía máxima que, en concepto de daños y perjuicios, pudiera corresponder por disposición judicial a un tercero perjudicado o miembro de la comunidad de confianza, en ausencia de regulación contractual específica, se limita a un máximo de cinco mil dólares estadounidenses (USD 5.000,00)

4.2.4. Verificación del sello de tiempo

El suscriptor y el tercero que confía, antes de depositar su con8anza en el sello de tiempo electrónico, deberán veri8car su validez conforme a lo establecido en la cláusula 6.7.5 ‘Validación de Sello de Tiempo“ del presente documento.

4.2.5. Ley aplicable

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 67, 2002)
- Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Decreto Ejecutivo 3496, R.O. 735, 31-dic-2002)
- Ley Orgánica de Telecomunicaciones (LOT)
- Resolución ARCOTEL-2024-0176 – Norma Técnica para la Prestación de los Servicios de Información y Servicios Relacionados de las Entidades de Certificación Acreditadas y Terceros Vinculados.

4.2.6. Disponibilidad del servicio

ANFAC Autoridad de Certi8cación Ecuador C.A. TSA ha implementado las siguientes medidas para garantizar la disponibilidad y continuidad operativa del servicio:

- Configuración redundante de los sistemas informáticos, a fin de evitar puntos únicos de fallo.
- Conexiones de alta velocidad y rutas de comunicación redundantes para prevenir interrupciones.
- Uso de sistemas de alimentación ininterrumpida (UPS) y respaldo eléctrico permanente.

A pesar de dichas medidas, no se puede garantizar una disponibilidad del 100 %, si bien ANFAC Autoridad de Certi8cación Ecuador C.A. TSA tiene como objetivo una disponibilidad anual del 99 %, de acuerdo con los Acuerdos de Nivel de Servicio (SLA) publicados en su sitio web oficial: https://www.anf.ec

4.3. Términos y condiciones

El documento ‘Términos y Condiciones para los Servicios Electrónicos de Con8anza“ (OID 2.16.218.1.1.3.9.1) publicado en el repositorio legal de ANFAC Autoridad de Certificación Ecuador C.A.:

https://www.anf.ec/repositorio-legal-terminos-y-condiciones/

contiene información aplicable, entre otros aspectos, sobre las limitaciones del servicio, las obligaciones de los suscriptores, y las limitaciones de responsabilidad de la entidad en la prestación de los servicios electrónicos de confianza.

Además, se aplican las disposiciones contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento General, y la Resolución ARCOTEL-

2024-0176, en lo relativo a los derechos y obligaciones de las Entidades de Certificación Acreditadas, los usuarios y los terceros que confían.

4.3.1. Aplicación de la política de servicio de confianza

Este documento informa sobre la política de servicio de confianza aplicada. Véase el capítulo 5 para más información relativa al alcance de las obligaciones y responsabilidades de las partes.

4.3.2 Periodo de tiempo de retención de los logs

Los registros de logs se retienen durante al menos tres meses. Los protocolos del sello de tiempo, lo que significa cada sello de tiempo emitido, se mantienen durante al menos 15 años.

4.4. Información de la política de seguridad

ANFAC Autoridad de Certificación Ecuador C.A. TSA mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) documentado, diseñado para garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de todos los procesos relacionados con la prestación del servicio de sellado de tiempo electrónico.

El sistema de gestión de seguridad cubre las áreas técnicas, organizativas y procedimentales, incluyendo la protección de las claves criptográficas, la gestión de accesos, el control de incidentes, la monitorización de la infraestructura y la continuidad de las operaciones.

El marco de seguridad implementado cumple con los principios establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la Ley Orgánica de Telecomunicaciones, la Ley Orgánica de Protección de Datos Personales (2021) y las obligaciones establecidas por la Resolución ARCOTEL-2024-0176.

Los registros de logs se conservan durante un período mínimo de tres (3) meses, de conformidad con las exigencias establecidas por ARCOTEL.
Los protocolos del servicio de sellado de tiempo, es decir, los registros que documentan cada sello de tiempo emitido, se conservan por un período no inferior a quince (15) años, garantizando su disponibilidad para efectos de auditoría, control o requerimientos judiciales.

El acceso a estos registros se encuentra restringido al personal autorizado, y cualquier manipulación, revisión o consulta se realiza bajo registro y control documental.

5. Obligaciones y Responsabilidades

5.1. Obligaciones de la TSA (ANFAC Autoridad de Certificación Ecuador C.A.)

5.1.1. Obligaciones

Al hacer uso de la Tercera Parte, ANFAC Autoridad de Certificación Ecuador C.A., actuando como Autoridad de Sellado de Tiempo (TSA), se compromete a:

- Respetar lo dispuesto en la presente Declaración de Prácticas TSA y Política de Sellado de Tiempo Electrónico.
- Supervisar, directa o indirectamente a través de la Tercera Parte, la protección segura de las claves privadas empleadas para la firma de los sellos de tiempo.
- Garantizar que el reloj empleado por la infraestructura de la TSA, o por la Tercera Parte, esté sincronizado con el Tiempo Universal Coordinado (UTC) dentro de la exactitud declarada, utilizando el protocolo NTP (Network Time Protocol).
- Supervisar la sincronización del reloj empleado y asegurar que cualquier desviación respecto al UTC sea detectada y corregida oportunamente.
- No emitir sellos de tiempo en caso de que el reloj empleado se desvíe de la precisión declarada, hasta que se restablezca la sincronización correcta.
- Proporcionar el servicio de sellado de tiempo desde el territorio de la República del Ecuador, utilizando como referencia temporal la señal oficial del Instituto Nacional de Meteorología e Hidrología (INAMHI), reconocida por el Servicio Ecuatoriano de Normalización (INEN) y vinculada al Bureau International des Poids et Mesures (BIPM).
- Supervisar, directamente o por medio de la Tercera Parte, que se mantenga una precisión de ±100 milisegundos o superior con respecto al UTC, mediante el uso de servidores certificados de la red de laboratorios UTC(k), reconocidos por el BIPM.
- Retener los registros de logs durante un período mínimo de tres (3) meses, y conservar los protocolos del servicio de sellado de tiempo —es decir, el registro de cada sello de tiempo emitido— durante un período no inferior a quince (15) años, conforme a lo dispuesto por la Resolución ARCOTEL-2024-0176.
- Informar a todos los Suscriptores antes de que ANFAC Autoridad de Certificación Ecuador C.A. deje de prestar los servicios de sellado de tiempo, y mantener la documentación relacionada con los servicios finalizados, junto con la información necesaria, de acuerdo con los procesos establecidos en la Declaración de Prácticas de Certificación (DPC) de ANFAC Autoridad de Certificación Ecuador C.A. TSA.

5.1.2. Responsabilidad

- ANFAC Autoridad de Certi8cación Ecuador C.A., para afrontar el riesgo derivado de la responsabilidad por los posibles daños y perjuicios que pudieran ocasionarse

en la prestación del servicio de sellado de tiempo, mantiene contratado un seguro de responsabilidad civil profesional, cuyo importe cumple con lo dispuesto por la normativa ecuatoriana vigente y las exigencias de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), estableciendo una cobertura mínima equivalente a cinco millones de dólares estadounidenses (USD 5.000.000,00).

- La responsabilidad de ANFAC Autoridad de Certi8cación Ecuador C.A. TSA frente a los suscriptores se encuentra regulada contractualmente en los acuerdos de prestación de servicios de sellado de tiempo suscritos con cada suscriptor.
- Son aplicables las disposiciones sobre responsabilidad definidas en la Declaración de Prácticas de Certi8cación (DPC) de ANFAC Autoridad de Certi8cación Ecuador C.A., en particular las establecidas en las secciones 9.6, 9.7 y 9.8, o aquellas que las sustituyan en versiones futuras del documento.
- Igualmente, resultan aplicables las limitaciones de servicio y las cláusulas de exoneración de responsabilidad establecidas en el presente documento, así como las previstas en la Resolución ARCOTEL-2024-0176 y en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

5.1.3. Exoneración de responsabilidad

ANFAC Autoridad de Certi8cación Ecuador C.A. no será responsable cuando concurra cualquiera de las siguientes circunstancias:

- Los errores en la veri8cación de la validez de los sellos de tiempo o las conclusiones erróneas derivadas de omisiones o de las consecuencias de tales conclusiones.
- El incumplimiento de sus obligaciones si dicho incumplimiento se debe a fallos o problemas de seguridad del organismo de supervisión (Agencia de Regulación y Control de las Telecomunicaciones ỳ ARCOTEL), de la autoridad nacional de protección de datos personales, o de cualquier otra entidad pública competente.
- El incumplimiento si dicho incumplimiento fue ocasionado por fuerza mayor o caso fortuito.
- Por la interrupción del servicio en caso de detectarse una desviación o pérdida de sincronización con el Tiempo Universal Coordinado (UTC), conforme a lo establecido en los procedimientos internos y en la Resolución ARCOTEL-2024-0176, que obliga a suspender la emisión de sellos hasta el restablecimiento de la sincronización.
  Cuando la parada del servicio se realice en cumplimiento de dicha obligación, el suscriptor no tendrá derecho a reclamación alguna.
- El Suscriptor, con la aceptación del sello de tiempo, exime de toda responsabilidad a ANFAC Autoridad de Certi8cación Ecuador C.A., y se compromete a mantener indemne a la entidad frente a cualquier daño derivado de acciones u omisiones que resulten en responsabilidad, pérdida o gasto de cualquier tipo —incluyendo los judiciales y de representación letrada— por la publicación y uso del sello de tiempo, cuando concurra alguna de las siguientes causas:

i. Negligencia en la conservación de sus datos de acceso al servicio de sellado de tiempo, o en la protección de su confidencialidad frente a accesos no autorizados.
ii. Extralimitación en el uso del sello de tiempo, contraviniendo lo dispuesto en la normativa ecuatoriana vigente o en la presente Declaración de Prácticas TSA.
iii. Falsedad o manifestación errónea realizada por el usuario del sello de tiempo.
iv. Error del usuario del sello de tiempo al facilitar los datos de la solicitud, cuando haya mediado dolo o negligencia respecto de ANFAC Autoridad de Certi8cación Ecuador C.A. o cualquier Tercero que Confía en el sello de tiempo.
v. Incumplimiento en el pago de las tasas o tarifas correspondientes al servicio contratado.

- El Tercero que Confía en el sello de tiempo se compromete igualmente a mantener indemne a ANFAC Autoridad de Certi8cación Ecuador C.A. de todo daño, pérdida o gasto derivado de acciones u omisiones que generen responsabilidad, incluyendo los judiciales o de representación letrada, cuando concurra alguna de las siguientes causas:
  i. Incumplimiento de las obligaciones del tercero que confía en el sello de tiempo.
  ii. Confianza temeraria o negligente en un sello de tiempo, atendiendo a las circunstancias.
  iii. Falta de comprobación de la suspensión, revocación o pérdida de vigencia del certificado electrónico de la TSA, disponible en el servicio de consulta de validez de certificados.
  iv. No utilización del servicio de retimbrado o actualización de sellos de tiempo, cuando algún componente criptográfico entre en situación de riesgo, conforme a las publicaciones que ANFAC Autoridad de Certi8cación Ecuador C.A. realiza en su sitio web oficial.

5.2. Obligaciones de los suscriptores / clientes

Las obligaciones generales especificadas en este documento y en la cláusula 9.5.3 de la Declaración de Prácticas de Certi8cación (DPC) de ANFAC Autoridad de Certi8cación Ecuador C.A. son aplicables en su totalidad.

- El suscriptor está obligado a no utilizar el servicio de sellado de tiempo electrónico de ANFAC Autoridad de Certi8cación Ecuador C.A. hasta haber formalizado el correspondiente contrato de uso del servicio.
  La mera disposición de un programa cliente para el consumo de sellos de tiempo de ANFAC Autoridad de Certi8cación Ecuador C.A., o incluso el disponer de credenciales de acceso al servicio, no otorga derecho de uso si no se ha suscrito el contrato correspondiente.

- El suscriptor deberá respetar lo establecido en la Declaración de Prácticas de Certi8cación (DPC) y en la presente Declaración de Prácticas TSA, así como lo dispuesto en los documentos contractuales y, en especial, en los Términos y Condiciones publicados por ANFAC Autoridad de Certi8cación Ecuador C.A..
- El suscriptor está obligado a:
    - Verificar la 8rma electrónica del Token de Sellado de Tiempo (TST).
    - Comprobar que la firma ha sido generada con un certi8cado de Unidad de Sellado de Tiempo (TSU) emitido por ANFAC Autoridad de Certi8cación Ecuador C.A..
    - Confirmar que el certi8cado empleado para 8rmar el TST estaba vigente en el momento de su emisión.

  Para realizar estas comprobaciones, se deberá utilizar un servicio de validación electrónica con8able o una aplicación compatible con el protocolo RFC 3161.

- El suscriptor deberá tomar las medidas necesarias para garantizar la validez y veri8cabilidad del TST más allá del tiempo de vida de los certificados empleados por ANFAC Autoridad de Certi8cación Ecuador C.A. TSA, mediante mecanismos de preservación o re-sellado.
- Si el suscriptor no utiliza un cliente de sellos de tiempo autorizado o proporcionado por la Tercera Parte de ANFAC Autoridad de Certi8cación Ecuador C.A., deberá veri8car que el hash contenido en el sello de tiempo coincide con el hash que fue enviado en su solicitud de TST.
- En el mismo supuesto, si el suscriptor no utiliza un cliente autorizado por la TSA, estará obligado a emplear funciones criptográ8cas seguras y conformes con los estándares internacionales vigentes para la generación de sus solicitudes de sellado de tiempo.
- El suscriptor deberá comprobar la veracidad e integridad de los datos electrónicos remitidos al servicio de sellado de tiempo de ANFAC Autoridad de Certi8cación Ecuador C.A., asumiendo plena responsabilidad por el contenido de dichos datos.
- En caso de no haber contratado el servicio de custodia de evidencias y preservación a largo plazo de sellos electrónicos, el almacenamiento y conservación de los sellos de tiempo entregados por la TSA será responsabilidad exclusiva del suscriptor.
- El suscriptor está obligado a informar a sus usuarios 8nales (por ejemplo, los terceros que confían) sobre el uso correcto de los sellos de tiempo electrónicos, así como sobre las condiciones de uso establecidas por ANFAC Autoridad de Certi8cación Ecuador C.A. y ANFAC Autoridad de Certi8cación Ecuador C.A. TSA.
- El suscriptor no podrá utilizar ni presentar los sellos de tiempo electrónicos emitidos por la TSA como referencia temporal fuera de los límites establecidos para dichos sellos en la presente política y en su correspondiente documento de especificación técnica.

5.3. Obligaciones de los terceros que confían

Las obligaciones generales establecidas en la Declaración de Prácticas de Certi8cación (DPC) de ANFAC Autoridad de Certi8cación Ecuador C.A., y en particular las disposiciones recogidas en su cláusula 9.5.4, son igualmente aplicables a los terceros que confían en los sellos de tiempo emitidos por la Autoridad de Sellado de Tiempo (TSA).

Los terceros que confían deberán actuar de forma diligente y conforme a las instrucciones contenidas en la presente Declaración de Prácticas TSA y Política de Sellado de Tiempo Electrónico, así como en los Términos y Condiciones de ANFAC Autoridad de Certi8cación Ecuador C.A.

En particular, los terceros que confían están obligados a:

- Veri8car la validez y autenticidad del Token de Sellado de Tiempo (TST) antes de depositar su confianza en él, asegurando que:
    - El sello fue emitido por ANFAC Autoridad de Certi8cación Ecuador C.A. TSA,
    - El certi8cado TSU utilizado para la firma se encuentra vigente y no ha sido revocado,
    - Y que el TST no presenta indicios de alteración o manipulación.
- Comprobar el estado de revocación o suspensión del certificado TSU utilizado por la TSA, empleando para ello los mecanismos de verificación puestos a disposición por ANFAC Autoridad de Certi8cación Ecuador C.A., tales como el servicio OCSP o las Listas de Certi8cados Revocados (CRL) publicadas en su repositorio legal.
- Abstenerse de con8ar en un sello de tiempo si existen dudas razonables sobre su validez, autenticidad, integridad o sincronización temporal.
- No modi8car, truncar ni reproducir parcialmente los sellos de tiempo electrónicos emitidos por la TSA, ni utilizarlos fuera del contexto o finalidad para la que fueron emitidos.
- Emplear herramientas de validación reconocidas y actualizadas para la comprobación de sellos de tiempo, preferiblemente aquellas que sean compatibles con los estándares internacionales RFC 3161 y RFC 5816, garantizando su correcta interpretación técnica.
- Respetar las limitaciones de uso establecidas en el presente documento, en la DPC y en los Términos y Condiciones de ANFAC Autoridad de Certi8cación Ecuador C.A., especialmente en lo relativo a la validez, precisión y alcance temporal de los sellos electrónicos.
- Mantener indemne a ANFAC Autoridad de Certi8cación Ecuador C.A. de toda reclamación, perjuicio o daño que pudiera derivarse de un uso incorrecto, temerario o negligente del sello de tiempo o de su información asociada.

6. Gestión y Operación de la TSA

6.1. Introducción

ANFAC Autoridad de Certificación Ecuador C.A. TSA mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) documentado, alineado con los requisitos establecidos por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y la legislación ecuatoriana vigente.

La provisión de un Token de Sellado de Tiempo (TST) en respuesta a una solicitud es una decisión discrecional de ANFAC Autoridad de Certificación Ecuador C.A. TSA, dependiendo de las condiciones contractuales acordadas con el suscriptor y de la disponibilidad operativa del servicio.

6.2. Organización interna

Todas las prácticas de ANFAC Autoridad de Certi8cación Ecuador C.A. TSA están descritas en el apartado 9 de la Declaración de Prácticas de Certi8cación (DPC) de ANFAC Autoridad de Certi8cación Ecuador C.A.

La estructura organizativa, las políticas, procedimientos y controles aplicables al servicio de sellado de tiempo forman parte del sistema general de gestión de la entidad, y son consistentes con las disposiciones descritas en el apartado 1.1 del presente documento.

a) Entidad legal: La Autoridad de Sellado de Tiempo (TSA) es gestionada por ANFAC Autoridad de Certi8cación Ecuador C.A., pudiendo hacer uso de un Tercera Parte autorizado y supervisado conforme a la Resolución ARCOTEL-2024-0176.

ANFAC Autoridad de Certi8cación Ecuador C.A. es una entidad de tecnología especializada en la prestación de servicios electrónicos de confianza, certificación digital y soluciones de infraestructura de clave pública (PKI).

ANFAC Autoridad de Certi8cación Ecuador C.A.

Av. 12 de Octubre N24-739 y Av. Colón - Ed. Torre Boreal, Quito (Ecuador)

Teléfono: +593 02 3826877

Web: www.anf.ec

b) Gestión de la información de seguridad y calidad del servicio: La gestión de la seguridad y la calidad del servicio se realiza dentro del marco del SGSI implementado por la entidad, de acuerdo con los principios de integridad, disponibilidad, confidencialidad y trazabilidad definidos por la legislación ecuatoriana y la ARCOTEL.

6.3. Personal de confianza

Se aplican las prácticas definidas en las cláusulas 5.2 y 5.3 de la DPC de ANFAC Autoridad de Certi8cación Ecuador C.A.

ANFAC Autoridad de Certi8cación Ecuador C.A. TSA reconoce que el personal cualificado y motivado constituye un factor esencial para el correcto funcionamiento del servicio. Por ello, los procesos de contratación y designación de personal de con8anza son rigurosos y verifican la idoneidad técnica y ética de los candidatos.

El concepto de ‘rol“ garantiza la segregación de funciones, asegurando que solo el personal autorizado realice tareas operativas críticas.

Antes del nombramiento en puestos de confianza, ANFAC Autoridad de Certi8cación Ecuador C.A., o en su caso el Tercera Parte, verifica que el personal disponga de los conocimientos y experiencia necesarios, proporcionando formación interna cuando sea pertinente.
El personal debe superar las pruebas de adquisición de conocimientos antes de asumir responsabilidades operativas.

El personal de confianza se encuentra libre de con9ictos de interés que puedan comprometer la imparcialidad de las operaciones de ANFAC Autoridad de Certi8cación Ecuador C.A. TSA.

6.4. Gestión de activos

Se aplican las prácticas definidas en las cláusulas 5, 6.4 y 6.5 de la DPC de ANFAC Autoridad de Certificación Ecuador C.A.

Todos los sistemas informáticos utilizados en el servicio están identificados, clasificados y registrados en una base de datos de gestión de activos.
Los recursos se administran de forma controlada, asegurando su disponibilidad y protección frente a accesos no autorizados.

La información contenida en los equipos se elimina de forma segura al final de su ciclo de vida, mediante procedimientos de borrado seguro o destrucción física certificada, conforme a las normas internacionales de seguridad de la información.

6.5. Control de accesos

Las prácticas identificadas en las cláusulas 6.4 y 6.5 de la DPC de ANFAC Autoridad de Certificación Ecuador C.A. son aplicables.

Las diferentes barreras de seguridad con respecto al acceso físico y acceso lógico garantizan un funcionamiento seguro del servicio de sellado de tiempo. Por ejemplo:

- Entorno físico seguro
- Segregación de los segmentos de red
- Segregación de responsabilidades
- Firewalls
- Monitorización del Servicio de Red

- Fortalecimiento de los Sistemas IT

En caso de que una persona lleve a cabo operaciones en la Tercera Parte empleada por ANF Certification Authority, S.L. TSA, y esta cambie de rol o deje de prestar sus servicios a la entidad, le serán retirados todos sus tokens de seguridad.

6.6. Certificado de TSA (TSU)

ANFAC Autoridad de Certi8cación Ecuador C.A. TSA, directamente o mediante una Tercera Parte, aplica procedimientos que garantizan la seguridad criptográ8ca del servicio.
Estas prácticas están documentadas en el manual técnico interno ' Controles de Seguridad Criptográ8ca CAỳTSA".

Los certificados de TSA no se renuevan automáticamente; al finalizar su vigencia, se emite un nuevo certificado con las condiciones técnicas y de seguridad actualizadas.

6.6.1. Generación de claves TSA

Las claves privadas de la TSA se generan y custodian en un dispositivo criptográ8co seguro (HSM) certificado conforme a los estándares FIPS 140-2 nivel 3 o superior o ISO/IEC 15408 EAL 4+, que no permite su exportación a otros módulos.

La generación de las claves de 8rma de la TSA (TSU) se realiza en un entorno físico protegido (véase cláusula 5.8 del presente documento), por personal de con8anza (véase cláusula 5.3), y bajo el control de al menos dos personas de con8anza.

Estas claves se utilizan exclusivamente para la 8rma de Tokens de Sellado de Tiempo (TST).

El algoritmo de firma empleado es RSA, con una longitud mínima de 2048 bits, y la duración de los certificados se ajusta a la seguridad criptográfica recomendada en ISO/IEC 18033 y FIPS 186-4.

Cada Unidad de Sellado de Tiempo (TSU) mantiene una única clave privada activa en cada momento.

6.6.2. Protección de la clave del TSU

Se aplican las prácticas de protección de claves de TSU, almacenamiento, backups y recuperaciones descritas en las cláusulas 6.2 y 6.3 de la DPC de ANFAC Autoridad de Certificación Ecuador C.A.

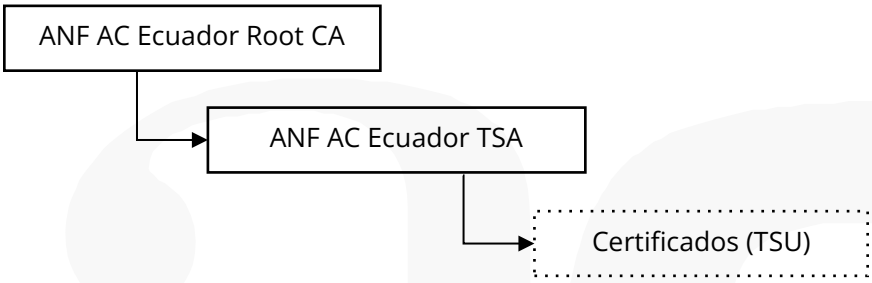
La clave privada del TSU se encuentra protegida en un módulo criptográfico HSM certificado en ISO 15408, Common Criteria EAL 4+ y que cumple los requerimientos que se detallan en FIPS 140-2 nivel 3 o superior.

6.6.3. Publicación de los Certificados de la TSA

Los sellos de tiempo electrónicos emitidos bajo esta política son firmados mediante certificados específicos, emitidos por la Cadena de Certi8cación de ANFAC Autoridad de Certi8cación Ecuador C.A., bajo su autoridad raíz CN = ANF AC Ecuador Root CA.

En ningún caso ANFAC Autoridad de Certi8cación Ecuador C.A. TSA emitirá TST antes de que el certificado del servicio TSA (clave pública) haya sido cargado y activado en la Unidad de Sellado de Tiempo (TSU) correspondiente.

El certi8cado del servicio TSA se adjunta en la respuesta de cada sello de tiempo emitido y está disponible públicamente en el repositorio legal de la entidad: https://www.anf.ec/repositorio-legal/



Certificado Autoridad de Certificación Raíz (Root CA), ANF AC Ecuador Root CA;

<table>
<tr><th colspan="4">ANF AC Ecuador Root CA</th></tr>
<tr><td rowspan="4">Sujeto</td><td>CN = ANF AC Ecuador Root CA</td><td rowspan="2">Serial number</td><td rowspan="2">03390B08202D32EF49150F2F</td></tr>
<tr><td>SERIALNUMBER = VATEC-1792601215001</td></tr>
<tr><td>O = ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.</td><td>Clave Pública</td><td>RSA (4096 Bits)</td></tr>
<tr><td>C = EC</td><td>Algoritmo de 8rma</td><td>Sha256RSA</td></tr>
<tr><td>Periodo de vigencia</td><td colspan="3">Válido desde el 2024-10-09 hasta el 2044-10-04</td></tr>
<tr><td>Fingerprint SHA-256</td><td colspan="3">2C:FF:D0:68:2D:C8:35:4C:86:1B:3B:E8:2C:4A:53:A2:74:68:48:19:2D:2D:7F:C5:6D:33:E3:BE:7A:29:10:05</td></tr>
</table>

Certificado Autoridad de Certificación Intermedia, ANF AC Ecuador TSA:

ANF AC Ecuador TSA			
Sujeto	CN = ANF AC Ecuador TSA	Serial number	0338C3B3863044BD10206A11
	SERIALNUMBER = B87341228	Clave Pública	RSA (4096 Bits)
	OU = Servicio de Sellado de tiempo		
	O = ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A.	Algoritmo de firma	Sha256RSA
	C = ES		
Periodo de vigencia	Válido desde el 2026-01-27 hasta el 2044-10-03		
Fingerprint SHA-256	A3:0E:DA:CC:B6:BD:EA:1A:2F:F5:F5:9E:BA:1B:FC:FF:6A:14:85:FB:F6:F4:4F:03:85:58:5A:8B:38:5D:A8:1C		

El servicio cualificado de Sellado de Tiempo empleará los siguientes certificados electrónicos de TSU para prestar el servicio:

ANF AC Ecuador Time-Stamping Unit 1399			
Subject	C = EC O = ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A. OU = TSU 2.5.4.97 = VATEC- 1792601215001 CN = ANF AC Ecuador Time-Stamping Unit 1399	Serial number	338CE72AF09B6556435EA41
		Public key	RSA (2048 Bits)
		Signature algorithm	Sha256RSA
Validity period	Válido desde el 2026-01-27 hasta el 2031-01-21		
Private Key Usage Period	5 años		
Fingerprint SHA-256	7E:63:FD:8C:06:C7:17:86:72:BC:94:5D:70:F8:3B:FB:DC:EF:B1:E2:8B:1F:A3:F1:26:B1:E6:7B:33:88:32:2F		

ANF AC Ecuador Time-Stamping Unit 1400			
Subject	C = EC O = ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A. OU = TSU 2.5.4.97 = VATES- 1792601215001 CN = ANF AC Ecuador Time-Stamping Unit 1400	Serial number	33972080A9D48CBDCF87BB1
		Public key	RSA (2048 Bits)
		Signature algorithm	Sha256RSA
Validity period	Válido desde el 2026-01-27 hasta el 2031-01-21		

Private Key Usage Period	5 años
Fingerprint SHA-256	75:3F:D4:C5:2F:6C:B1:51:F1:2F:8C:26:A1:48:91:60:EF:35:17:62:85:99:8D:31:0C:28:1E:89:08:88:1D:53

ANF AC Ecuador Time-Stamping Unit 1401			
Subject	C = EC O = ANFAC AUTORIDAD DE CERTIFICACION ECUADOR C.A. OU = TSU 2.5.4.97 = VATEC-1792601215001 CN = ANF AC Ecuador Time-Stamping Unit 1401	Serial number	338E7A5ACE10491AFA747D7
		Public key	RSA (2048 Bits)
		Signature algorithm	Sha256RSA
Validity period	Válido desde el 2026-01-27 hasta el 2031-01-21		
Private Key Usage Period	5 años		
Fingerprint SHA-256	8713C819F7AA9B503A13E38F9750A700F601A24A7903C2F5AD83E64E2791146E		

6.6.4. Cambio del Certificado de TSA

Se establecen los controles necesarios para garantizar el cese de uso de la clave privada antes de su caducidad.

El certificado de la TSA podrá ser sustituido en cualquier momento por otro certificado TSA, previa aprobación de la Dirección Técnica y de Cumplimiento de ANFAC Autoridad de Certi8cación Ecuador C.A., conforme a los procedimientos internos y la supervisión de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).

Este cambio no será notificado individualmente a los usuarios del servicio, quienes deberán confiar en todos los sellos de tiempo emitidos por ANFAC Autoridad de Certi8cación Ecuador C.A. TSA, firmados con certificados TSA válidos dentro de la jerarquía de certificación de la entidad.

En caso de sustitución del certificado, las claves asociadas serán destruidas de forma irreversible, conforme a las instrucciones del fabricante del HSM utilizado para su generación y custodia.

El certificado de la TSA tendrá una vida útil máxima de cinco (5) años. La duración del certificado de la Unidad de Sellado de Tiempo (TSU) estará limitada por:

- El tiempo de validez del certificado de la Autoridad de Certificación emisora.
- El tiempo de vigencia establecido en el propio certificado.
- Si el algoritmo o la longitud de clave entra en situación de riesgo, la TSA cesará su uso y emitirá nuevos certificados con algoritmos y longitudes de clave seguras.

- Cese de actividad, en cuyo caso se aplicará lo dispuesto en el apartado ' Finalización de TSA y Plan de Cese" de este documento.

6.6.5. Gestión del ciclo de vida del hardware criptográfico

Las prácticas de gestión del ciclo de vida del hardware criptográfico se describen en la cláusula 6.2 de la Declaración de Prácticas de Certi8cación (DPC) de ANFAC Autoridad de Certi8cación Ecuador C.A.

El hardware criptográ8co (HSM) utilizado es inspeccionado por personal de con8anza (al menos dos personas) de ANFAC Autoridad de Certi8cación Ecuador C.A. o de una Tercera Parte, durante las fases de transporte, recepción y almacenamiento.

Durante la inspección se verifican los siguientes aspectos:

- Integridad de los sellos de seguridad.
- Ausencia de daños físicos en el equipamiento (golpes, arañazos, roturas).
- Estado del embalaje y precintos originales.

La inspección se documenta mediante un acta protocolizada.

a) Asimismo, la instalación y activación de las claves de firma de las TSU en el hardware criptográfico se realiza únicamente por personal de con8anza, bajo el principio de control dual, en un entorno físicamente protegido.
b) Las claves privadas de firma almacenadas en los módulos criptográficos se eliminan de forma segura al retirarse el dispositivo, imposibilitando cualquier recuperación posterior.

6.6.6. Fin del ciclo de vida de la clave del TSU

ANFAC Autoridad de Certificación Ecuador C.A. TSA, siguiendo las recomendaciones técnicas internacionales, define el tiempo de vigencia de las claves de la TSU de manera que nunca exceda el tiempo de validez del certificado de clave pública asociado.

Con el objetivo de garantizar la posibilidad de verificación de los sellos de tiempo emitidos durante un período suficiente, la vigencia de la clave de firma de la TSU es inferior al tiempo de validez del certificado público vinculado.

Una vez expiradas las claves privadas, estas son destruidas de forma irreversible, conforme al procedimiento de borrado seguro definido por el fabricante del módulo criptográfico (HSM) utilizado para su almacenamiento.

6.7. Sellado de tiempo

ANFAC Autoridad de Certificación Ecuador C.A. TSA, directamente o mediante una Tercera Parte, emite exclusivamente sellos electrónicos de tiempo cualificados, y no emite sellos de tiempo no cualificados.

Las Unidades de Sellado de Tiempo (TSU) no emiten ningún sello antes de verificar su certificado público y cadena de confianza.

Una vez cargado el certificado en la TSU, la TSA verifica que este ha sido firmado correctamente por una autoridad de certificación confiable dentro de la jerarquía de ANFAC Autoridad de Certificación Ecuador C.A.

6.7.1. Emisor de sello de tiempo

ANFAC Autoridad de Certificación Ecuador C.A. TSA presta el servicio de sellado de tiempo conforme al protocolo RFC 3161 "Time-Stamp Protocol (TSP)".

La URL del servicio se especifica en los contratos de suscripción.

Cada Token de Sellado de Tiempo (TST) contiene:

- El identificador de la política de sellado de tiempo,
- Un número de serie único,
- Y el certificado de la TSU que contiene su información de identificación.

El servicio admite los algoritmos de hash SHA-256, SHA-384 y SHA-512; la función de hash mínima para firmar el TST es SHA-256.

Las claves de las TSU son RSA con una longitud mínima de 2048 bits, y se utilizan exclusivamente para la firma de los TST.

ANFAC Autoridad de Certificación Ecuador C.A. TSA mantiene un registro de todos los TST emitidos, los cuales son conservados durante el tiempo legalmente establecido (mínimo quince años).

El sistema genera un encadenamiento de hash relativo a todos los TST emitidos por cada TSU, garantizando la integridad cronológica y sin incluir información que permita identificar al solicitante.

Este mecanismo permite demostrar la existencia y secuencia temporal de cada TST.

6.7.2. Sincronización de la hora con UTC

ANFAC Autoridad de Certificación Ecuador C.A. TSA supervisa que el reloj de cada TSU o de la Tercera Parte esté sincronizado con el Tiempo Universal Coordinado (UTC) dentro de una precisión de un (1) segundo o mejor.

La sincronización se realiza a través del Instituto Nacional de Meteorología e Hidrología (INAMHI) y servidores NTP internacionales de referencia vinculados al Bureau International des Poids et Mesures (BIPM).

En caso de pérdida de sincronización o desviación del tiempo superior a los márgenes permitidos, la TSA interrumpe la emisión de sellos de tiempo hasta que se restablezca la sincronización correcta.

Se auditan periódicamente los siguientes aspectos:

- Calibración y control de precisión de los relojes TSU.
- Verificación del comportamiento frente a segundos intercalados.
- Análisis de protección ante ataques a la señal de tiempo.
- Revisión del comportamiento ante desviaciones superiores a 1 segundo del UTC.

6.7.3. Solicitud de Sellos de Tiempo

ANFAC Autoridad de Certificación Ecuador C.A. TSA presta el servicio de sellado de tiempo electrónico en dos modalidades:

- Utilizando un cliente TST autorizado por la TSA o por una Tercera Parte.
- Mediante consulta directa al servidor TSU, para lo cual las solicitudes deben cumplir la sintaxis de la especificación RFC 3161 y superar los controles de autenticación y acceso establecidos.

ANFAC Autoridad de Certificación Ecuador C.A. TSA, directamente o mediante su Tercera Parte, proporciona soporte técnico a los suscriptores en cualquiera de las modalidades anteriores.

6.7.4. Formato de las respuestas de Sellos de Tiempo

Las respuestas emitidas por la TSA no incluyen extensiones adicionales. El certificado TSU se incluye en la respuesta, y el Token de Sellado de Tiempo (TSP) se envía con el siguiente formato:

Content-Type: application/timestamp-reply

Method: POST

Content-Length: required

<<Contiene la respuesta del sello de tiempo en ASN.1, codificada en DER (incluyendo el código de error si procede)>>

Campo	Tratamiento
Policy	1.3.6.1.4.1.37442.15.1
Ordering	Falso
Nonce	Si la petición lo contiene se devuelve el mismo valor Sino se crea uno nuevo
Certificados adjuntos	<Certificado de TSA> <Certificado de CA Subordinada>
Accuracy	La correspondiente, no permitido TST superior a 1

Si la solicitud se ha podido procesar, se devuelve en la respuesta un TimeStampToken. Esta es una estructura firmada del tipo CMSSignedData en la que se incluye el sellado de tiempo y el sello electrónico del mismo. Incluye el certificado de TSU que lo firma:

```
TSTInfo ::= SEQUENCE  {
   version                      INTEGER  { v1(1) },
   policy                       TSAPolicyId,
   messageImprint               MessageImprint,
     -- MUST have the same value as the similar field in
     -- TimeStampReq
   serialNumber                 INTEGER,
    -- Time-Stamping users MUST be ready to accommodate integers
    -- up to 160 bits.
   genTime                      GeneralizedTime,
   accuracy                     Accuracy                 OPTIONAL,
   ordering                     BOOLEAN              DEFAULT FALSE,
   nonce                        INTEGER                  OPTIONAL,
     -- MUST be present if the similar field was present
     -- in TimeStampReq.  In that case it MUST have the same value.
   tsa                          [0] GeneralName          OPTIONAL,
   extensions                   [1] IMPLICIT Extensions   OPTIONAL  }
```

- policy corresponde al OID de la TSAPolicyId. Los OIDs aceptados son:
- 2.16.218.1.1.3.5.1, correspondiente a la Declaración de Prácticas TSA y Política de Sellado de Tiempo Electrónico de ANFAC Autoridad de Certi8cación Ecuador C.A. TSA, registrada ante la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).
- 0.4.0.2023.1.1, correspondiente a la política de *best-practices-ts-policy*, utilizada como referencia técnica internacional según lo descrito en la norma ETSI EN 319 421, sin carácter obligatorio en el marco ecuatoriano.
- MessageImprint corresponde al resumen criptográ8co (hash) del dato electrónico remitido por el suscriptor en la solicitud de sello de tiempo.
- SerialNumber es un identi8cador único del token de sello de tiempo (TST) generado, que permite su trazabilidad dentro del registro operativo de la TSA.
- GenTime indica la fecha y hora exactas de generación del sello de tiempo, mientras que accuracy representa el nivel de precisión temporal del servidor, el cual se encuentra sincronizado con el Tiempo Universal Coordinado (UTC) a través de fuentes oficiales nacionales, principalmente el Instituto Nacional de Meteorología e Hidrología (INAMHI), y servidores NTP de referencia internacional.
- El nonce es una cadena aleatoria enviada por el suscriptor en la solicitud y devuelta por la TSA en la respuesta, con el fin de garantizar la correspondencia exacta entre ambas y evitar reutilización o manipulación de solicitudes.
- El campo tsa es opcional y contiene los datos del sujeto del certi8cado de sellado de tiempo (TSU) utilizado por la TSA para firmar electrónicamente el TST.
- El campo extensions puede incluir extensiones opcionales que la TSA incorpore en la respuesta, de conformidad con el protocolo técnico RFC 3161.

Si la solicitud no puede ser procesada. Los códigos de error posibles son los siguientes:

1. badRequest: cuando la política indicada en la solicitud no coincide con la política de la TSA.
2. badAlg: cuando el algoritmo del *messageImprint* no está soportado o no es válido.
3. badTime: cuando la exactitud temporal es igual o superior a un segundo (1000 milisegundos) respecto al UTC.
4. timeNotAvailable: cuando la fecha actual no es válida por no ser superior a la última fecha registrada en la base de datos operativa de la TSA.
5. systemFailure: cuando el encadenamiento criptográfico previo es incorrecto, o no puede generarse un nuevo encadenamiento. También se aplica cuando se produce un error interno o una excepción que impide continuar con el procesamiento de la solicitud.

6.7.5. Validación del sello de tiempo electrónico

Para validar un sello de tiempo electrónico cuali8cado, las partes que confían deberán verificar el Token de Sellado de Tiempo (TST) utilizando un sistema de validación con8able o una aplicación de validación de 8rmas y sellos electrónicos que disponga de capacidad de verificación de TST, conforme a los estándares RFC 3161 y RFC 6960.

ANFAC Autoridad de Certi8cación Ecuador C.A., directamente o mediante una Tercera Parte, pone a disposición del público un servicio gratuito de veri8cación de TST, accesible a través de su sitio web oficial: https://www.anf.ec

El servicio de verificación de TST utiliza el campo ‘ messageImprint“ descrito en el apartado anterior, así como el estado de validez del certi8cado TSU mediante el servicio de validación del estado de certi8cados (OCSP) operado por la propia TSA o por la Tercera Parte.

El punto de acceso al servicio OCSP se encuentra incluido en el certificado de la TSU correspondiente.

Operación I – Verificación del emisor del sello de tiempo

El emisor del sello de tiempo es ANFAC Autoridad de Certi8cación Ecuador C.A. TSA, una Entidad de Certi8cación Acreditada (ECA) reconocida y supervisada por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), conforme a lo dispuesto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y la Resolución ARCOTEL-2024-0176.

ANFAC Autoridad de Certi8cación Ecuador C.A. TSA utiliza los certificados electrónicos adecuados para la emisión de sellos de tiempo electrónicos cualificados. Las claves públicas de los certificados utilizados están incluidas en los certificados de TSU y de la Autoridad de Certi8cación raíz, y se publican para permitir la verificación de que el sello de tiempo ha sido firmado correctamente por la TSA.

Los certificados se encuentran disponibles en el repositorio legal de la entidad: https://www.anf.ec/repositorio-legal/

Operación II – Verificación del estado de revocación del certificado TSU

El servicio OCSP de ANFAC Autoridad de Certi8cación Ecuador C.A. o, en su caso, de su Tercera Parte , cumple con las especificaciones del IETF RFC 6960 y permite comprobar el estado de revocación o vigencia de los certificados utilizados por las TSU para firmar los sellos de tiempo.

La dirección de acceso al servicio OCSP está incorporada en el propio certificado del TSU, dentro del campo Authority Information Access (AIA).

Operación III – Verificación de la integridad del sello de tiempo

La integridad criptográfica del sello de tiempo —es decir, la estructura ASN.1 y la correspondencia de los datos fechados— se verifica mediante los dispositivos o servicios de validación de sellos electrónicos proporcionados por ANFAC Autoridad de Certi8cación Ecuador C.A. TSA o por una Tercera Parte , disponibles públicamente en su sitio web.

El servicio de validación permite determinar la asociación del TST con los datos electrónicos sellados, comprobando que el hash de los datos originales coincide con el hash incluido en el sello de tiempo emitido por la TSA.

Además, se puede verificar la existencia y la imposibilidad de manipulación del sello de tiempo electrónico comprobando:

- La presencia del hash del TSP dentro de las actas de encadenamiento generadas por la TSA, y
- Su correspondencia temporal y cronológica respecto al conjunto de TST emitidos por la misma Unidad de Sellado de Tiempo (TSU).

Las actas de encadenamiento hash se protocolizan mediante intervención notarial o fedatario público ecuatoriano, garantizando su autenticidad y valor probatorio.

6.8. Seguridad física y ambiental

Se aplican las prácticas identificadas en las cláusulas 5.1 y 6.5 de la Declaración de Prácticas de Certificación (DPC) de ANFAC Autoridad de Certificación Ecuador C.A.

Un entorno físico de alta seguridad es requisito fundamental para la operación del servicio de sellado de tiempo.
Las instalaciones donde se encuentra alojada la TSA de ANFAC Autoridad de Certificación Ecuador C.A., o aquellas provistas por una Tercera Parte, se encuentran diseñadas para proteger física y lógicamente los sistemas críticos frente a accesos no autorizados o manipulaciones indebidas.

Cada acceso a las áreas de seguridad está sujeto a supervisión independiente y controlado por el personal de confianza de la TSA.

El ingreso de personas al entorno seguro requiere acompañamiento, registro de identidad, motivo de la visita, hora de entrada y de salida.

Las zonas de acceso restringido están delimitadas mediante perímetros físicos de seguridad (barreras, cerraduras electrónicas, sistemas biométricos o similares).

Los controles físicos y ambientales de seguridad tienen por objeto proteger las instalaciones que albergan los recursos del sistema, incluyendo servidores, módulos criptográficos, soportes de almacenamiento y redes de comunicación.

La política de seguridad física y ambiental de la TSA está orientada a prevenir y mitigar riesgos derivados de:

- Acceso físico no autorizado.
- Desastres naturales (terremotos, inundaciones, tormentas eléctricas).
- Incendios o fallas estructurales.
- Fallos en los suministros eléctricos o de telecomunicaciones.
- Daños por fugas de agua o humedad.
- Robo, vandalismo o intrusión.
- Fallos en el sistema de climatización o en los equipos críticos.
- Pérdida de disponibilidad por eventos de fuerza mayor.

Los controles físicos y organizativos implementados por ANFAC Autoridad de Certificación Ecuador C.A. TSA garantizan la protección integral contra accesos no autorizados desde el exterior a los servidores, la información, los medios de comunicación y el software relacionados con el servicio de sellado de tiempo.

El cumplimiento de estas medidas es verificado y auditado periódicamente, en conformidad con los requisitos establecidos por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y las políticas de seguridad de la propia entidad.

6.9. Seguridad de las operaciones

Se aplican las prácticas identificadas en las cláusulas 6.3, 6.4 y 6.5 de la DPC de ANFAC Autoridad de Certificación Ecuador C.A.

ANFAC Autoridad de Certificación Ecuador C.A. TSA hace uso del sistema avanzado de seguridad de la Tercera Parte , para garantizar la calidad y disponibilidad del servicio. En particular, estos controles de la Tercera Parte son:

a) Se lleva a cabo un análisis de los requisitos de seguridad en las especificaciones de diseño, y los requisitos para cualquier etapa del proyecto de desarrollo de sistemas emprendida por el TSP o en nombre de la TSP, para asegurar que la seguridad se integra adecuadamente en los sistemas de tecnología de la información.
b) Como procedimiento de control de cambios, se aplica un control de versionado para modificaciones y correcciones del software.
c) La integridad de los sistemas y la información TSP está protegido contra virus, software malicioso y software no autorizado.
d) Los medios empleados en los sistemas TSP son seguros y protegen contra daños, robo, acceso no autorizado y la obsolescencia.

e) Dentro del período de tiempo que se requiere que deben conservarse los registros, los procedimientos de gestión de medios hacen que la información se proteja contra la obsolescencia y el deterioro de los medios de comunicación.
f) La aplicación de procedimientos adecuados para todas las funciones de confianza y administrativos que tienen un impacto en el suministro de servicios.
g) El TSP ha especificado y aplicado procedimientos para asegurar que los parches de seguridad se aplican dentro de un tiempo razonable después de que estén disponibles. La aplicación de un parche de seguridad no será obligatoria si introduce vulnerabilidades o inestabilidades adicionales que superan a los beneficios de aplicar dicho parche. Se debe documenta la razón por la cual no se aplica un parche de seguridad
h) Se monitoriza la correcta calibración del reloj de su TSU. En caso de detectar una desviación superior a 1 segundo, el servicio de TSA se detendrá automáticamente.
i) Se realiza un monitoreo continuo del número de solicitudes diarias, con el objetivo de determinar la capacidad de respuesta del sistema y proyectar en consecuencia los requisitos futuros para asegurar que se dispone de capacidad de procesamiento y almacenamiento adecuados.

6.10. Seguridad de la red

Se aplican las prácticas identificadas en la cláusula 6.5 de la Declaración de Prácticas de Certificación (DPC) de ANFAC Autoridad de Certificación Ecuador C.A.

La Tercera Parte empleado por ANFAC Autoridad de Certificación Ecuador C.A., protege la red y los sistemas frente a ataques o accesos no autorizados.
En particular:

a) La red de la TSA se encuentra segmentada en redes o zonas según una evaluación de riesgos, teniendo en cuenta las relaciones funcionales, lógicas y físicas (incluida la ubicación) entre los sistemas y los servicios de confianza.
b) El Prestador de Servicios de Confianza (Entidad de Certificación acreditada) restringe el acceso y comunicación entre zonas exclusivamente a lo necesario para el funcionamiento del servicio de sellado de tiempo.
   Las conexiones innecesarias o los servicios no requeridos se encuentran desactivados o explícitamente prohibidos.
   El conjunto de reglas y políticas de red se revisa de forma periódica conforme a los requisitos establecidos por la Resolución ARCOTEL-2024-0176.
c) Todos los elementos críticos de los sistemas del TSP (por ejemplo, los sistemas de la Autoridad de Certificación Raíz y las Unidades de Sellado de Tiempo —TSU—) se mantienen dentro de una zona de seguridad reforzada, con acceso controlado y monitorizado.
d) Se dispone de una red dedicada para la administración de los sistemas de TI, físicamente separada de la red operativa.
   Los sistemas utilizados para la administración no pueden ser empleados para fines distintos de la gestión técnica y de seguridad.

e) La plataforma de pruebas y la plataforma de producción se encuentran totalmente separadas.
La plataforma de pruebas opera en un entorno independiente, no involucrado en operaciones activas o en la emisión real de sellos de tiempo.
f) La comunicación entre los distintos sistemas de confianza solo puede realizarse a través de canales de comunicación seguros, lógicamente separados de cualquier otro canal y que garanticen la identificación mutua segura de los extremos y la protección de los datos frente a modificación o divulgación no autorizada.
g) La conexión a la red externa de Internet es redundante, garantizando la disponibilidad continua del servicio en caso de fallo de una de las líneas o proveedores.
h) El TSP realiza de forma regular un análisis de vulnerabilidades sobre las direcciones IP públicas y privadas previamente identificadas, evaluando los riesgos detectados. Cada análisis de vulnerabilidades es realizado por personal o entidades especializadas, con competencias técnicas, independencia, herramientas adecuadas y código ético profesional, asegurando la emisión de informes fiables y verificables.
i) Tras la aplicación de actualizaciones o modificaciones significativas en la infraestructura, el TSP lleva a cabo pruebas de penetración en los sistemas críticos de red.

Estas pruebas se realizan por personas o entidades con las habilidades, herramientas, conocimientos y ética profesional necesarias para garantizar un informe independiente y fiable.

Los resultados y evidencias de cada prueba de penetración son documentados y conservados conforme a los procedimientos internos de auditoría y los requerimientos establecidos por la ARCOTEL.

6.11. Gestión de incidentes

Se aplican las prácticas identificadas en las cláusulas 5.7 y 6.6 de la Declaración de Prácticas de Certificación (DPC) de ANFAC Autoridad de Certificación Ecuador C.A.

ANFAC Autoridad de Certificación Ecuador C.A. TSA, directamente o mediante una Tercera Parte , aplica un conjunto de procedimientos documentados para la gestión de incidentes de seguridad con el fin de garantizar la continuidad, integridad y disponibilidad del servicio de sellado de tiempo.

En particular:

a) Se dispone de un procedimiento formal de notificación, análisis, tratamiento y resolución de incidentes de seguridad, que establece responsabilidades, plazos y niveles de escalamiento.
b) Todo incidente de seguridad detectado en los sistemas de la TSA es registrado, categorizado y evaluado en función de su impacto sobre la confidencialidad, integridad y disponibilidad de los servicios.

c) Los incidentes que puedan afectar a la validez o fiabilidad de los sellos de tiempo electrónicos emitidos se tratan con carácter prioritario, siguiendo los protocolos internos definidos por la Dirección Técnica y de Cumplimiento de la TSA.
d) En caso de incidentes que impliquen compromisos de claves, corrupción de datos o interrupción del servicio, ANFAC Autoridad de Certificación Ecuador C.A. TSA informará inmediatamente a la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), conforme a los plazos establecidos en la Resolución ARCOTEL-2024-0176 (máximo de 48 horas desde su detección).
e) Cuando el incidente tenga impacto sobre la protección de datos personales, se notificará adicionalmente a la Autoridad de Protección de Datos Personales del Ecuador, en cumplimiento de la Ley Orgánica de Protección de Datos Personales (2021).
f) Los incidentes son objeto de registro detallado que incluye fecha, hora, descripción, causas identificadas, medidas adoptadas, impacto y acciones de mejora.
   Dichos registros se conservan por un período mínimo de tres (3) años y están disponibles para revisión por los auditores o por ARCOTEL.
g) Se realiza un análisis posterior al incidente para identificar sus causas raíz, documentar las lecciones aprendidas y actualizar los procedimientos de seguridad, con el objetivo de prevenir su repetición.
h) ANFAC Autoridad de Certificación Ecuador C.A. TSA dispone de un Plan de Respuesta a Incidentes (PRI) integrado en su Sistema de Gestión de Seguridad de la Información (SGSI), que se somete a pruebas periódicas para verificar su eficacia y tiempo de respuesta.
i) Cuando la gestión del incidente requiera la participación de una Tercera Parte, éste actuará bajo la supervisión directa de la TSA y conforme a los procedimientos internos aprobados, garantizando la trazabilidad y control de todas las acciones realizadas.

6.12. Gestión de evidencias

Se aplican las prácticas identificadas en la cláusula 4.12 de la Declaración de Prácticas de Certificación (DPC) de ANFAC Autoridad de Certificación Ecuador C.A.

En el momento en que se detecta un incidente de seguridad, puede no ser evidente si dicho incidente requerirá posteriores investigaciones.
Por ello, es esencial que cualquier evidencia, estado del sistema o información relevante sea preservada de forma segura antes de que pueda resultar inutilizable o ser destruida.

Los registros y evidencias electrónicas de ANFAC Autoridad de Certificación Ecuador C.A., gestionados directamente o mediante una Tercera Parte, se mantienen accesibles durante un período adecuado de tiempo, incluso después de la finalización de las actividades de la TSA.
Toda la información pertinente relativa a los datos emitidos y recibidos por el Prestador de Servicios de Confianza (TSP) se conserva y custodia con el fin de proporcionar pruebas en procedimientos legales y garantizar la continuidad del servicio.

En particular:

a) Se garantiza la confidencialidad e integridad de los registros activos y archivados relativos a la operación del servicio.
b) La información relativa a la gestión de servicios se considera confidencial y se archiva conforme a las prácticas comerciales y políticas de seguridad descritas en la DPC.
c) La información relativa a la gestión de servicios podrá ponerse a disposición de las autoridades competentes o órganos judiciales, cuando sea necesario, a fin de aportar pruebas del correcto funcionamiento del servicio.
d) El TSP registra de forma precisa los acontecimientos significativos relacionados con el entorno operativo, la gestión de claves y la sincronización de relojes. El tiempo utilizado para el registro de estos eventos, tal como requiere el sistema de auditoría, está sincronizado continuamente con el Tiempo Universal Coordinado (UTC), a través de las fuentes oficiales del Instituto Nacional de Meteorología e Hidrología (INAMHI), reconocido por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL).
e) La información relativa a los servicios se preserva durante un período de tiempo posterior a la expiración de las claves de firma o de cualquier token de confianza emitido, a fin de garantizar la validez jurídica y probatoria de los sellos de tiempo electrónicos, de acuerdo con lo establecido en el presente documento y en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
f) Los eventos se registran en una forma que impide su eliminación o destrucción, salvo que sean transferidos de forma fiable a medios de almacenamiento de largo plazo, garantizando su autenticidad e integridad durante todo el periodo de retención establecido.

6.13. Gestión de la Continuidad del Negocio

Se aplican las prácticas identificadas en la sección 4.15 de la Declaración de Prácticas de Certificación (DPC) de ANFAC Autoridad de Certificación Ecuador C.A.

La Tercera Parte empleado por ANFAC Autoridad de Certificación Ecuador C.A. garantiza que las copias de seguridad de la base de datos de todos los TST emitidos por ANFAC Autoridad de Certificación Ecuador C.A. TSA se mantengan en almacenamiento seguro fuera del sitio (off-site), conforme a los requisitos de seguridad establecidos en la Resolución ARCOTEL-2024-0176.

Si la clave privada del TSU se ve comprometida o se sospecha su compromiso, ANFAC Autoridad de Certificación Ecuador C.A. TSA, directamente o mediante su Tercera Parte, informará de inmediato a los suscriptores y terceros que confían, y cesará el uso de la clave comprometida.

En caso de revocación del certificado de TSU, las acciones se ejecutarán conforme a las decisiones adoptadas por el Comité de Crisis y Plan de Continuidad del Negocio y Recuperación ante Desastres de ANFAC Autoridad de Certificación Ecuador C.A.

Si se produce una pérdida de sincronización del reloj, ANFAC Autoridad de Certificación Ecuador C.A. TSA suspenderá inmediatamente sus operaciones para evitar cualquier afectación a la integridad del servicio.
El Plan de Recuperación se activará para restaurar la sincronización y reanudar las operaciones una vez comprobada la precisión temporal.

El servicio de sellado de tiempo se encuentra alojado en un entorno físico asegurado, diseñado para minimizar los riesgos de desastres naturales (como incendios, sismos o inundaciones).
Las claves privadas de las TSU se almacenan en módulos de seguridad criptográfica (HSM) certificados conforme a FIPS 140-2 nivel 3 o superior, aislados de la red pública.

En caso de que las claves privadas pudieran verse comprometidas, el archivo de sellos de tiempo emitidos permite diferenciar entre sellos válidos y falsos, conservando así la trazabilidad completa mediante la pista de auditoría.

El HSM opera de manera completamente aislada de la red pública, y en caso de detectarse una situación que pueda afectar su seguridad, ANFAC Autoridad de Certificación Ecuador C.A., directamente o a través de la Tercera Parte, aplicará las siguientes medidas correctoras:

- Notificar de forma inmediata al Responsable de Seguridad, quien coordinará todas las acciones a ejecutar.
- Iniciar una auditoría de seguridad sobre las claves privadas restantes, incluyendo comprobaciones de integridad y análisis de los registros de auditoría.
- Notificar la incidencia a los terceros que confían.
- Iniciar el procedimiento de sustitución de componentes y restaurar la redundancia N + 1 en la infraestructura operativa.

En caso de desastres naturales (como incendios, terremotos o tormentas), si se produce una pérdida total o parcial de las instalaciones, el servicio de sellado de tiempo podrá suspenderse temporalmente hasta que se complete la reconstrucción y una entidad independiente haya realizado la evaluación de seguridad de las nuevas instalaciones.

La pérdida de calibración o sincronización del reloj de un TSU se encuentra cubierta en la cláusula 5.7.1 del presente documento.

6.14. Finalización de TSA y Plan de Cese

Se aplican las prácticas identificadas en las secciones 4.16 y 4.17 de la Declaración de Prácticas de Certificación (DPC) de ANFAC Autoridad de Certificación Ecuador C.A.

Adicionalmente, la Tercera Parte empleado por ANFAC Autoridad de Certificación Ecuador C.A. aplica las siguientes medidas:

- En el caso de que la TSA finalice sus operaciones por cualquier motivo, se notificará previamente a la autoridad nacional de control, la Agencia de Regulación y

Control de las Telecomunicaciones (ARCOTEL), antes de la terminación efectiva del servicio.

- Se proporcionará un aviso oportuno a todos los suscriptores y terceros que confían, con el fin de minimizar cualquier perjuicio que pueda derivarse de la interrupción o cese de los servicios de sellado de tiempo.
- En coordinación con la ARCOTEL, la Entidad de Certificación Acreditada (ECA) tomará las medidas necesarias para asegurar la conservación de todos los registros y evidencias archivadas pertinentes antes de la terminación del servicio.

Asimismo, se aplican las siguientes disposiciones:

a) El TSP mantiene un Plan de Terminación actualizado, que define las acciones y responsabilidades a ejecutar en caso de cese total o parcial de las operaciones.
b) Antes de que el TSP dé por finalizados sus servicios, se aplicarán, al menos, los siguientes procedimientos:
    i. El TSP informará formalmente de la terminación del servicio a todas las partes interesadas: suscriptores, terceros que confían, y otras entidades con las que existan acuerdos contractuales o relaciones operativas.
    Además, esta información será publicada en el sitio web oficial y en el repositorio legal de la entidad, asegurando su disponibilidad pública.
    ii. El TSP revocará la autorización de todos los subcontratistas o Terceros Vinculados para actuar en su nombre o realizar funciones relacionadas con la emisión de sellos de tiempo.
    iii. El TSP transferirá a una entidad fiable —acreditada o autorizada por ARCOTEL—, por un período razonable, las obligaciones de conservación de la información y registros necesarios para proporcionar evidencias de sus operaciones, salvo en los casos en que el TSP no sea titular legítimo de dicha información.
    iv. Las claves privadas del TSP, incluidas las copias de seguridad, serán destruidas o retiradas de uso de forma que resulte imposible su recuperación, siguiendo los procedimientos de borrado seguro establecidos por el fabricante del HSM y la normativa técnica aplicable.
    v. Se tomarán las medidas necesarias para revocar los certificados TSU que permanezcan vigentes en el momento del cese.
    vi. Siempre que sea posible, el TSP facilitará la transferencia de los servicios de los clientes a otro prestador acreditado de servicios de confianza, a fin de garantizar la continuidad y disponibilidad de los servicios.
c) El TSP mantendrá un acuerdo financiero o contractual que garantice la cobertura de los costos asociados al proceso de cese, incluyendo las obligaciones de custodia y comunicación, en caso de insolvencia o imposibilidad económica para afrontarlos, conforme a la legislación ecuatoriana aplicable.
d) El TSP mantendrá o transferirá a una entidad fiable la obligación de poner a disposición del público, durante un período razonable, su clave pública y los tokens de servicio de confianza necesarios para verificar los sellos de tiempo emitidos antes de la terminación de la TSA.

6.15 Conformidad

ANFAC Autoridad de Certificación Ecuador C.A. TSA, haciendo uso de la Tercera Parte , asegura el cumplimiento de la legislación aplicable en todo momento.

En concreto, esta Política se encuentra en conformidad con las normativas y disposiciones legales indicadas en la sección 1.1 del presente documento, incluyendo:

- La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- La Ley Orgánica de Telecomunicaciones (LOT).
- La Ley Orgánica de Protección de Datos Personales (2021).
- La Ley Orgánica para la Transformación Digital y Audiovisual (2022).

Y las Resoluciones y Normas Técnicas emitidas por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), especialmente la Resolución ARCOTEL-2024-0176 sobre requisitos de acreditación, auditoría y control de Entidades de Certificación Acreditadas (ECA).

La validación del cumplimiento de estas normas se realiza mediante las evaluaciones de conformidad y auditorías de seguridad informática requeridas por la ARCOTEL, así como las revisiones internas y auditorías externas independientes efectuadas conforme a lo descrito en el apartado 8 de la Declaración de Prácticas de Certificación (DPC) de ANFAC Autoridad de Certificación Ecuador C.A.