



Sistema de Gestión de la Seguridad de la Información

Términos y Condiciones TSA Avansi

ÍNDICE

1. OBJETO Y ÁMBITO DE APLICACIÓN DEL DOCUMENTO	5
1.1. Datos de contacto del prestador	5
2. TÉRMINOS Y CONDICIONES.....	6
2.1. Generales	6
2.2. Tipos y usos de los sellos de tiempo electrónico	6
2.2.1.Formato de la Request	7
2.2.2.Formato de la Response	8
2.3. Límites de uso del servicio de sellado de tiempo	9
2.4. Obligaciones de los suscriptores	10
2.5. Obligación de verificar el estado de los certificados de la TSU	10
2.6. Limitaciones de responsabilidad.....	11
2.7. Acuerdos aplicables y Declaración de Política y Prácticas	12
2.8. Política de privacidad	12
2.9. Política de reintegro	13
2.10. Normativa aplicable, reclamaciones y disputas.....	13
2.11. Acreditaciones y auditorías.....	13
2.12. Otros datos relevantes	13

CONTROL DE DOCUMENTO

Título:	Sistema de Gestión de la Seguridad de la Información		
Asunto:	Términos y Condiciones TSA Avansi		
Versión:	1	Fecha:	12-11-2019
Código:	TERMS-TSA-AVANSI	Revisión anterior:	
Idioma:	Castellano	Núm. Páginas:	13

CONTROL DE CAMBIOS Y VERSIONES		
Fecha	Versión	Motivo del Cambio
12-11-2019	1.0	Primera versión del documento

ACERCA DEL DOCUMENTO

Este documento, con nivel de seguridad público, es propiedad de Avansi , S.R.L. Para más información contacte con:

Avansi , S.R.L. (Viafirma)

RNC: 130222509

Avenida Lope de Vega, #19, Edificio PIISA A, Suite 102

Ensache Naco, Santo Domingo, República Dominicana

Telf. : +1 809 682 3928

info@avansi.com.do

1. OBJETO Y ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento contiene los términos y condiciones aplicables al servicio cualificado de sellado de tiempo electrónico de Avansi. Sirve de complemento al contrato de prestación de servicios firmado entre Avansi y el suscriptor.

1.1. Datos de contacto del prestador

Avansi , S.R.L. (Viafirma)

RNC: 130222509

Avenida Lope de Vega, #19, Edificio PIISA A, Suite 102

Ensache Naco, Santo Domingo, República Dominicana

Telf. : +1 809 682 3928

info@avansi.com.do

2. TÉRMINOS Y CONDICIONES

2.1. Generales

Avansi declara que:

- Ofrece un servicio de sello de tiempo electrónico conforme a la Ley 126-02 sobre Comercio Electrónico, Documentos y Firma Digital de la República Dominicana.
- Los términos y condiciones son vinculantes para las partes contempladas en las políticas y prácticas y la norma, tanto suscriptor como terceras partes que confían en los sellos de tiempo emitidos.
- Los términos y condiciones complementan al contrato establecido entre las partes (Avansi y suscriptor). En el eventual caso de conflicto entre lo estipulado en los términos y condiciones y el contrato, prevalece lo recogido en el contrato.
- Los términos y condiciones complementan a las CPS de Avansi.
- Se reserva el derecho de modificación de los Términos y Condiciones en caso de necesidad.

2.2. Tipos y usos de los sellos de tiempo electrónico

El servicio cualificado de Sellado de Tiempo es ofrecido por Avansi como Entidad de Certificación en base a la autorización emitida por el órgano regulador en la materia en el país, el Instituto Dominicano de las Telecomunicaciones (Indotel), en su Resolución No. 166-06 de fecha 28 de septiembre de 2006, sin perjuicio de su adaptación a la Reglamento eIDAS y a las especificaciones recogidas en los siguientes estándares y normas:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers.
- 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.
- RFC-3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs).

- El sello de tiempo tendrá presente el OID de política de firma 0.4.0.2023.1.1.

El servicio de sellado de tiempo es un servicio comercial que requiere la suscripción de un acuerdo con Avansi. Los suscriptores deberán:

- Cumplir lo especificado en la declaración de prácticas y políticas del servicio y los términos y condiciones contractuales.
- Verificar el sello de tiempo.
- Validar el certificado de la TSA.
- Verificar que no se ha alterado el hash enviado al servicio de sello de tiempo.

Para validar los certificados de sello de tiempo se dispone de CRLs, disponibles en:

- <http://crl.avansi.com.do/avansisub.crl>
- <http://crl2.avansi.com.do/avansisub.crl>

2.2.1. Formato de la Request

Los sellos de tiempo emitidos por Avansi TSA siguen el estándar RFC 3161 y están conformes con la especificación ETSI EN 319 422, y tendrán el siguiente formato en la llamada (request):

```
TimeStampReq ::= SEQUENCE {  
    version INTEGER {v1(1)},  
    messageImprint MessageImprint,  
    reqPolicy TSAPolicyId OPTIONAL,  
    nonce INTEGER OPTIONAL,  
    certReq BOOLEAN DEFAULT FALSE,  
    extensions [0] IMPLICIT Extensions OPTIONAL}
```

Donde messageImprint sigue la siguiente estructura:

```
MessageImprint ::= SEQUENCE {  
    hashAlgorithm AlgorithmIdentifier,
```

hashedMessage OCTET STRING}

Y reqPolicy se define de la siguiente forma:

TSAPolicyId ::= OBJECT IDENTIFIER

De acuerdo al apartado 5 de ETSI EN 319 422, los campos opcionales reqPolicy, nonce y certReq deben ser soportados. Se aceptan algoritmos SHA1, SHA256, SHA384 y SHA512 de acuerdo a las recomendaciones de la Guía de Seguridad de las TIC CCN-STIC 807.

2.2.2. Formato de la Response

El formato de la response generada por Avansi TSA cumple el estándar RFC3161:

*TimeStampResp ::= SEQUENCE {
 status PKIStatusInfo,
 timeStampToken TimeStampToken OPTIONAL}*

Destacando el desglose de TimeStampToken:

*TSTInfo ::= SEQUENCE {
 version INTEGER {v1(1)},
 policy TSAPolicyId,
 messageImprint MessageImprint,
 TimeStampReq serialNumber INTEGER,
 genTime GeneralizedTime,
 accuracy Accuracy OPTIONAL,
 ordering BOOLEAN DEFAULT FALSE,
 nonce INTEGER OPTIONAL,
 tsa [0] GeneralName OPTIONAL,
 extensions [1] IMPLICIT Extensions OPTIONAL}*

GeneralizedTime sigue la estructura YYYYMMDDhhmmss[.s...].Z. Mientras tanto, Accuracy refleja la desviación respecto a UTC de la fecha/hora recogida en genTime:

*Accuracy ::= SEQUENCE {
 seconds INTEGER OPTIONAL,
 millis [0] INTEGER (1..999) OPTIONAL,*

micros [1] INTEGER (1..999) OPTIONAL}

La respuesta sigue las restricciones específicas recogidas en el apartado 5 de ETSI EN 319 422, que indica que:

- *El campo policy debe estar presente.*
- *El campo genTime debe tener la precisión exigida.*
- *El campo accuracy debe estar presente, con un valor inferior a 1 segundo, en concreto 0.8 segundos.*
- *El campo ordering no debe estar presente o estar a false.*
- *Ningún campo extension debe estar marcado como crítico.*

2.3. Límites de uso del servicio de sellado de tiempo

- Los suscriptores deben haber formalizado el correspondiente acuerdo de uso del servicio de Sellado de Tiempo, que establecerá tarifas y limitaciones en el uso permitido.
- Para confiar en un sello de tiempo emitido por Avansi TSA, se deberá realizar un proceso de comprobación de la validez del certificado utilizado para generar el sello de tiempo, utilizando los protocolos publicados a tal efecto.
- Avansi TSA únicamente proporciona evidencia de la existencia de los datos electrónicos sellados en el momento de generación del sello de tiempo. Avansi no se responsabiliza del proceso de creación, contenido o uso posterior del documento electrónico sellado, y en general, de cualquier parte del proceso que no está bajo su control.
- La TSA se sincroniza con UTC(ROA) por protocolo NTP, más otros proveedores confiables de sello stratum 1, garantizando un desfase menor de 1 segundo. Se dispone de automatización para detener el servicio de emisión de sellos de tiempo en el caso de que el desfase de la precisión supere el máximo legal exigible (1 segundo).

2.4. Obligaciones de los suscriptores

Los suscriptores:

- Deben respetar y cumplir lo plasmado en el presente documento y en los documentos que regulan la relación comercial con Avansi, incluyendo al menos el contrato de servicio y los términos y condiciones.
- Deben comprobar el estado de revocación del certificado utilizado para emitir el sello de tiempo.
- Deben disponer de sistemas de generación de sellos de tiempo adecuados a los estándares técnicos.
- Deben utilizar los sellos para los usos permitidos por la política.

2.5. Obligación de verificar el estado de los certificados de la TSU

Los terceros que confían en los TSTs deben verificar que el certificado con el que se firman los sellos de tiempo no está revocado y considerar las limitaciones de uso descritas en las Prácticas de Avansi. Para ello:

- Deben verificar la validez del certificado de sellado de tiempo mediante los métodos disponibles a tal efecto.
- Deben asegurar que el hash enviado no ha sido alterado en el proceso de sellado y coincide con el devuelto en la respuesta.
- Deben comprobar que el sello de tiempo electrónico está correctamente sellado con los datos de creación de sello de la TSU y determinar que el sello de tiempo electrónico ofrece garantías suficientes para el uso previsto.

2.6. Limitaciones de responsabilidad

Avansi no se responsabilizará de:

- Daños y perjuicios en los usos que puedan realizarse, ya sean estos por culpa de los interesados o por defectos de origen de los elementos, producidos por los TSTs emitidos por Avansi.
- Hechos acontecidos por usos no acordes con la Declaración de Prácticas de Certificación, en casos de desastres naturales, atentado terrorista, huelga, fuerza mayor (incidencias en servicios eléctricos o redes telemáticas o de comunicaciones), así como en los supuestos que se trate de acciones constitutivas de delito o falta que afecten a sus infraestructuras prestadoras, salvo que hubiera mediado culpa grave de la entidad.
- Usos indebidos, fraudulentos, en ausencia de convenio o contrato suscrito con Avansi, en caso de extralimitación del uso o de omisiones del suscriptor.
- Los algoritmos criptográficos ni de los daños causados por ataques exitosos externos a los algoritmos criptográficos usados, si se ha procedido con la diligencia debida de acuerdo al estado actual de la técnica, y conforme a los documentos publicados y la normativa vigente.
- Problemáticas asociadas al incumplimiento por parte de los suscriptores de las condiciones de contratación (por ejemplo, impagos).
- En todo caso y con la condición de cláusula penal, las cuantías que en concepto de daños y perjuicios debiera satisfacer por imperativo judicial Avansi a los suscriptores en defecto de regulación específica en los contratos o convenios, se verán cubiertas por el Seguro de Responsabilidad suscrito por Avansi y registrado en el Indotel, cumpliendo con la normativa del propio regulador en la materia.

Los contratos de suscripción del servicio de sellado de tiempo pueden incluir a mayores información adicional sobre limitaciones de responsabilidad.

2.7. Acuerdos aplicables y Declaración de Política y Prácticas

Aplican los siguientes acuerdos y documentos:

- Declaración de Prácticas de Certificación (OID 1.3.6.1.4.1.27395.7.1), disponibles ambos documentos en el sitio <https://qtsp.viafirma.com/>.
- El presente documento de términos de uso.
- Las condiciones recogidas en el contrato de servicios suscrito, así como en el texto divulgativo publicado en el sitio www.avansi.com.do.

2.8. Política de privacidad

Avansi dispone de procedimientos y medidas para el cumplimiento de la legislación vigente en materia de protección de datos personales, en este sentido, cumplirá con todos los requisitos impuestos por la legislación aplicable en materia de protección de datos, en concreto, los referidos en Resolución 055-06 del Indotel, que aprueba la Norma sobre Protección de Datos de Carácter Personal por los Sujetos Regulados, sin perjuicio de cumplir también con las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Avansi obtiene y trata los datos facilitados por el cliente con la finalidad exclusiva de llevar a cabo la gestión de la prestación solicitada por el mismo. De dichos datos será responsable Avansi como encargado del tratamiento, siendo tratados meramente por el tiempo necesario para la prestación del servicio mientras el cliente mantenga la cuenta activa; en caso de ser necesario, estos datos serán cedidos a empresas terceras exclusivamente a los meros efectos técnicos necesarios para la prestación del servicio. Avansi suscribe por tanto un contrato de encargado de tratamiento de datos con el cliente

2.9. Política de reintegro

Avansi no contempla una política de reintegro del servicio.

2.10. Normativa aplicable, reclamaciones y disputas

Las relaciones entre los suscriptores y Avansi se rigen por la normativa dominicana vigente, así como la legislación específica civil, mercantil y de protección de datos que sea aplicable.

En el caso de conflictos surgidos en relación con los servicios de Entidad de Certificación, las partes tratarán una resolución amistosa. En el caso de no ser posible, las partes se someten a la jurisdicción exclusiva de los tribunales de República Dominicana, en la ciudad de Santo Domingo.

2.11. Acreditaciones y auditorías

Avansi, como Entidad de Certificación, cumple con la realización de auditorías periódicas llevadas a cabo por una institución acreditada en República Dominicana para ello, como es el propio regulador, Indotel.

2.12. Otros datos relevantes

Avansi garantiza el almacenamiento de los logs de operaciones en un sistema de almacenamiento de acceso inmediato por un mínimo de seis meses, procediendo a almacenar los logs anteriores en un repositorio accesible bajo petición. Dicho repositorio cuenta con un período de retención de 15 años.

El horario del servicio es ininterrumpido 24x7, con una disponibilidad objetivo mínima del 99%.