CPS-ERDS - Viafirma Delivery

Prácticas de Certificación del Servicio de Entrega Electrónica Certificada Viafirma Delivery en República Dominicana

ÍNDICE

1. INTRODUCCIÓN 3
1.1. Alcance 3
1.2 Audiencia 3
1.3 Referencia normativa 3
1.4 Frecuencia de publicación 4
1.5 Identificación y Obligación de terceros 5
2. QUÉ CONSTITUYE UNA ENTREGA 7
2.1. Definición de entrega 7
2.2 Entrega fallida, caducidad y cancelación 7
2.3 Evidencias generadas 8
3. CÓMO SE PROTEGE LA COMUNICACIÓN 10
3.1. AccessKey y TTL 10
3.2. Comportamiento al expirar el TTL 10
3.3. Sin pérdida de datos 10
3.4 Modificaciones del contenido 10
3.5 Comprobación periódica de la configuración 11
3.6 Seguridad de la transmisión 12
4. IDENTIFICACIÓN Y AUTENTICACIÓN DEL EMISOR Y DEL DESTINATARIO 13
4.1. Emisor (remitente) 13
4.2 Destinatario (receptor) 14
4.3 Obligaciones 14
4.3.1 Obligaciones del emisor 14
4.3.2 Obligaciones de receptor 15
4.3.3 Obligaciones de otras terceras partes 15
4.4 Limitaciones de uso 16
4.4.1 Limitaciones funcionales 16
4.4.2 Limitaciones de alcance 17
5. CÓMO OBTENER EVIDENCIAS 18
5.1 Para el emisor 18
5.2 Contenido de las evidencias 18
5.3 Para autoridades y auditores 19
6. PERÍODO DE RETENCIÓN 20
6.1 Plazo mínimo de retención 20
6.2 Configuración del período de retención 20

6.3 Garantías de inalterabilidad 20
6.4 Conservación de los registros de seguridad 21
7. DISPOSICIONES DE TERMINACIÓN DEL SERVICIO 22
7.1 Terminación por el cliente 22
7.2 Terminación del servicio por Viafirma 22

CONTROL DE DOCUMENTO

Título	Prácticas de Certificación del Servicio de Entrega Electrónica Certificada Viafirma Delivery		
Código	CPS-ERDS-DO		
Versión	1.1	**Fecha Versión Actual**	27/10/2026
Fecha Creación	05/06/2026	**Fecha Aprobación**	09/11/2026
Revisado por	Cristina Parreño	**Aprobado por**	Benito Galán
Tipología información	Pública		

Control de Cambios y Versiones		
Fecha	**Versión**	**Motivo del Cambio**
05/06/2026	1.0	Primera versión.
20/10/2026	1.1	Rev. Cap. 1 referencia a ISO/IEC 27001 y otras certificaciones acreditadas. Nuevo Cap. 1.5 Identificación y Obligación de terceros. Rev. Cap. 2.1, 2.2 y 2.3 en definiciones de entrega. Nuevo Cap. 3.4 Modificaciones del contenido. Nuevo Cap. 3.5 Comprobación periódica de la configuración. Rev. Cap. 4.3 y 4.4 Obligaciones y Limitaciones de uso. Rev. Cap. 7.2 Terminación del servicio por Viafirma: comunicación al INDOTEL y a las partes afectadas, transferencia de la custodia, remisión al Plan de Cese

		y cese imprevisto. / Rev. Cap. 6.3: obsolescencia de algoritmos criptográficos de las evidencias (ETSI EN 319 521, REQ-ERDSP-7.11-10; NCMIN-7). / Rev. Cap. 4.1: verificación del emisor por certificado electrónico y supervisión del responsable de verificación de identidad (ETSI EN 319 521, REQ-QERDSP-7.2.2; NCMIN-6). / Rev. Cap. 5.2: referencia de tiempo del servicio y registro de eventos sin sello de tiempo (ETSI EN 319 521, REQ-ERDS-5.3.1-01; NCMIN-8). / Rev. Caps. 3.1 y 4.2: autenticación del destinatario con certificado electrónico (ETSI EN 319 521, cap. 5.2). / Rev. Caps. 1.4, 1.5 y 4.4.1 y nuevo cap. 3.6 Seguridad de la transmisión (ETSI EN 319 521, cap. 4) / Rev. Cap. 6.3: comunicación del compromiso de la clave de firma de las evidencias (ETSI EN 319 521, REQ-ERDSP-7.11-09) / Nuevo cap. 6.4 Conservación de los registros de seguridad (ETSI EN 319 521, REQ-ERDSP-7.10-04).

1. INTRODUCCIÓN

Este documento constituye el ERDS Practice Statement (Declaración de Prácticas del Servicio de Entrega Electrónica Registrada) de Viafirma Delivery, el servicio de Comunicaciones Electrónicas Certificadas de Viafirma para la República Dominicana.

Su propósito es describir, de forma pública y auditable, las prácticas y procedimientos que rigen el servicio, en cumplimiento del requisito REQ-ERDS-4.1.1-03 del marco normativo basado en los estándares ETSI EN 319 521 y ETSI EN 319 531.

El servicio es ofrecido como parte de los servicios de confianza de Viafirma, incorporado por tanto en su sistema de gestión SGSI, para el que se cuenta con certificación ISO/IEC 27001, ETSI EN 319 401, Esquema Nacional de Seguridad (ENS) y otros esquemas de cumplimiento disponibles todos ellos en la siguiente dirección:

https://www.viafirma.com/es/certificados-y-reconocimientos/

1.1. Alcance

Este documento aplica a todas las operaciones del servicio Viafirma Delivery que gestionan comunicaciones electrónicas con valor probatorio: envío, entrega, acceso, decisión del destinatario y generación de evidencias.

1.2 Audiencia

- Remitentes (emisores) que utilizan el servicio.
- Destinatarios que reciben comunicaciones certificadas.
- Organismos reguladores (Indotel, autoridades judiciales, auditores).
- Equipos técnicos y operativos de Viafirma.

1.3 Referencia normativa

- ETSI EN 319 521: Policy and security requirements for Electronic Registered Delivery Service Providers.

- ETSI EN 319 531: Policy and security requirements for Registered Electronic Mail (REM) Service Providers.
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers.
- Ley 126-02 (RD): Ley de Comercio Electrónico, Documentos y Firmas Digitales.
- Resolución 067-25 del INDOTEL: Artículo 32 Requisitos de servicios de entrega electrónica certificada en República Dominicana.
- Este documento es público y está disponible para consulta por parte de clientes, destinatarios y organismos reguladores.

1.4 Frecuencia de publicación

Cualquier versión que actualice la presente CPS será publicada en el sitio web https://cps.viafirma.do manteniendo el histórico de versiones anteriores. El intervalo máximo establecido para la revisión es de seis meses a contar desde la fecha de su última publicación.

Este documento se revisa:

- para verificar su vigencia y alineación con la normativa aplicable.
- ante cambios normativos de Indotel o de los estándares ETSI de referencia.
- ante cambios técnicos significativos en el servicio que afecten a las prácticas descritas.

El responsable de la revisión es el equipo de producto de Viafirma Delivery, con validación del equipo legal/cumplimiento de Viafirma.

Antes de aplicar una nueva versión que afecte a las obligaciones de los clientes o de las partes que confían en las evidencias, Viafirma la publica en https://cps.viafirma.do y la comunica a los clientes con antelación razonable, conforme a los términos y condiciones del servicio.

1.5 Identificación y Obligación de terceros

Proveedor	Tipo de Servicio	Términos aplicables
VIAFIRMA	Gestión de infraestructura, operación y servicios de TSA, Emisión de Certificados y Firma electrónica.	Política de Seguridad de la Información y de las Redes https://cps.viafirma.do https://qtsp.viafirma.com
SVQ Datacenter, S.L. (COMVIVE)	Housing Almacenamiento Base de Datos Dispositivo Criptográfico HSM	Política de Seguridad de la Información y de las Redes
Green Way Telecomunicaciones, S.L. (GWC)	Housing Almacenamiento Base de Datos Dispositivo Criptográfico HSM	Política de Seguridad de la Información y de las Redes
Amazon Web Services EMEA SARL, SUCURSAL EN ESPAÑA	Cloud Hosting EC2, EKS Almacenamiento EFS, S3 Base de Datos RDS	Política de Seguridad de la Información y de las Redes
Veridas	Verificación de identidad (KYC)	Política de Seguridad de la Información y de las Redes https://cps.viafirma.do
Metamap	Verificación de identidad (KYC)	Política de Seguridad de la Información y de las Redes https://cps.viafirma.do
JCE - Junta Central Electoral	Validación de cédulas electorales en la República Dominicana	Política de Seguridad de la Información y de las Redes

Prestadores cualificados que intervienen en el servicio:

- Viafirma, S.L., prestador cualificado de servicios de confianza conforme al Reglamento (UE) 910/2014, que emite los sellos de tiempo cualificados de los eventos y de las evidencias.
- La autoridad de certificación de Viafirma Dominicana (Avansi SRL), reconocida por el INDOTEL, que emite el certificado con el que se firman las evidencias.

2. QUÉ CONSTITUYE UNA ENTREGA

2.1. Definición de entrega

Una comunicación se considera entregada cuando se produce cualquiera de los siguientes eventos, registrado mediante evidencia técnica certificada:

- Puesta a disposición (consignación): la comunicación queda disponible para el destinatario en la plataforma, y el aviso se entrega al servidor de correo del destinatario o al operador SMS.
- Acceso: el destinatario abre el enlace y, tras autenticarse, accede al contenido.
- Decisión: cuando la comunicación lo requiere, el destinatario acepta o rechaza la recepción.

A efectos de este servicio, la comunicación se considera entregada cuando se pone a disposición del destinatario. Esta definición coincide con la de los términos y condiciones del servicio.

2.2 Entrega fallida, caducidad y cancelación

- Si el aviso no puede entregarse, se registra el resultado devuelto por el servidor de correo o el operador (rebote, descarte, error).
- Si vence el plazo de disponibilidad sin acceso del destinatario, se registra la caducidad. Si además no consta la entrega, se registra la no entrega.
- Si el remitente cancela la comunicación, se registra la cancelación con su motivo.

Estas evidencias quedan a disposición del remitente como prueba del intento de entrega y de su resultado.

2.3 Evidencias generadas

El servicio genera una evidencia por cada uno de los siguientes eventos del proceso de entrega:

Fase	Evento	Hecho que acredita	Actor
Envío	Comunicación creada	El remitente ha enviado la comunicación y el servicio la ha aceptado	Remitente
Envío	Envío rechazado	El servicio no ha podido procesar la comunicación tras aceptarla	Sistema
Aviso	Aviso por email enviado	Se ha enviado el aviso por email	Sistema
Aviso	Resultado del envío del email	Lo que comunica el servidor de correo: recibido, entregado al servidor del destinatario, rebotado, descartado, aplazado, en lista de bloqueo, sin servidor de destino, error o desconocido	Sistema
Aviso	Aviso por SMS enviado y confirmación del operador	Se ha enviado el SMS y el operador ha confirmado su recepción	Sistema
Acceso	Acceso a la comunicación	El destinatario ha abierto el enlace	Destinatario
Acceso	Acceso denegado por caducidad	Se ha intentado abrir una comunicación caducada	Destinatario
Acceso	Lectura del contenido	El destinatario, ya autenticado, ha accedido al contenido	Destinatario
Acceso	Descarga de adjunto	El destinatario o el remitente han descargado un adjunto	Destinatario / remitente

Decisión	Aceptación / rechazo	El destinatario ha aceptado o rechazado la recepción, con el motivo en caso de rechazo	Destinatario
Cierre	Cancelación	El remitente ha cancelado la comunicación, con su motivo	Remitente
Cierre	Caducidad / no entrega	Ha vencido el plazo de disponibilidad sin acceso del destinatario	Sistema
Conservación	Fin del periodo de retención	Se ha aplicado la política de retención	Sistema

Cada evidencia incluye el tipo de evento, la fecha y hora, el actor y los datos técnicos descritos en el capítulo. 5.2. Las evidencias se firman y se sellan conforme al capítulo 5.2. La correspondencia con los tipos de evento de ETSI EN 319 522-2 figura en el anexo.

3. CÓMO SE PROTEGE LA COMUNICACIÓN

3.1. AccessKey y TTL

El destinatario recibe un aviso con un enlace a la comunicación, que incluye un token de acceso firmado (AccessKey) con un tiempo de vida (TTL) configurable. El enlace lleva a la autenticación del destinatario: el contenido solo se entrega cuando se autentica con su certificado electrónico (cap. 4.2).

3.2. Comportamiento al expirar el TTL

Una vez expirado el TTL del token:

- El acceso público al contenido queda bloqueado: cualquier intento de acceso devuelve un error de acceso denegado.
- La comunicación permanece íntegra y accesible en el sistema para el emisor y los auditores autorizados.
- El evento de expiración queda registrado como evidencia en el timeline de la comunicación.
- El emisor puede, según política configurada, emitir un nuevo token de acceso para el destinatario.

3.3. Sin pérdida de datos

La expiración del token de acceso nunca implica la eliminación de la comunicación ni de sus evidencias. Los datos permanecen bajo el período de retención legal vigente.

3.4 Modificaciones del contenido

El servicio no modifica el asunto, el cuerpo ni los adjuntos que aporta el remitente. Se conservan y se ponen a disposición del destinatario tal como se recibieron. El servicio calcula y registra en las evidencias la huella digital (hash) de los adjuntos para acreditar su integridad.

No existe ningún medio para modificar el contenido una vez creada la comunicación. El remitente sólo puede cancelarla (cap. 2.2). La cancelación queda registrada como evidencia y se comunica al destinatario.

Antes de aceptar la comunicación, el servicio aplica estos controles:

- **Nombre de los adjuntos:** se normaliza para eliminar caracteres no válidos. El contenido del fichero no cambia.
- **Tipo de fichero:** se comprueba el tipo real de cada adjunto frente a la lista de tipos admitidos (cap. 4.4).
- **Software malicioso:** se analizan los adjunto .

Si un adjunto no supera estos controles, se rechaza y no se envía. El servicio no lo corrige ni lo transforma. El rechazo se comunica al remitente en la respuesta del servicio en el momento del envío, con el motivo. Si la comunicación no puede procesarse después de aceptarla, se registra además una evidencia de envío rechazado.

El aviso que recibe el destinatario lo genera el servicio y no reproduce el contenido de la comunicación. El destinatario accede al contenido completo en la plataforma, tras autenticarse.

3.5 Comprobación periódica de la configuración

La configuración de los sistemas que prestan el servicio se comprueba periódicamente para detectar cambios que incumplan la Política de Seguridad de la Información y de las Redes de Viafirma. Cada comprobación verifica, al menos, que:

- la configuración en uso coincide con la configuración de referencia aprobada, incluida la configuración de seguridad;
- las cuentas y credenciales de los sistemas cumplen la política de contraseñas y no hay cuentas sin uso o no autorizadas;
- los cambios realizados desde la comprobación anterior se han tramitado conforme al procedimiento de gestión de cambios.

El **intervalo máximo entre dos comprobaciones es de seis meses**. Además, se hace una comprobación extraordinaria tras un incidente de seguridad significativo o un cambio significativo en la infraestructura del servicio.

Las desviaciones detectadas se corrigen o, si están justificadas, se aprueban como cambio. El resultado de cada comprobación queda registrado.

3.6 Seguridad de la transmisión

Las comunicaciones entre el servicio y los emisores y destinatarios se cifran con HTTPS (TLS). La integridad del contenido se protege con los resúmenes de los adjuntos registrados en las evidencias, que se firman y se sellan (cap. 5.2). El contenido y las evidencias se almacenan en infraestructura replicada, con acceso restringido al personal autorizado.

4. IDENTIFICACIÓN Y AUTENTICACIÓN DEL EMISOR Y DEL DESTINATARIO

4.1. Emisor (remitente)

La identidad del emisor se verifica y protege mediante los siguientes mecanismos:

Autenticación de acceso al servicio:

- OAuth2 con opaque token: todos los endpoints de emisión (POST /api/v1/communication) requieren un token OAuth2 válido emitido por el servidor de autorización de Viafirma.
- Introspección activa: el token es validado en cada petición contra el servidor de autorización, descartando tokens revocados o expirados.
- Scopes de autorización: el emisor debe poseer el scope delivery:write para crear comunicaciones y delivery:read para consultarlas.

Verificación previa al servicio:

Antes de otorgar acceso al servicio, el emisor se autentica con su certificado electrónico. El alta solo se completa si el número de documento de identidad del certificado coincide con el del usuario que la organización emisora ha autorizado.

El responsable de verificación de identidad de Viafirma comprueba periódicamente que las verificaciones de identidad de emisores y destinatarios se ajustan al proceso descrito en este capítulo.

Confidencialidad de la identidad:

La identidad del emisor se protege durante todo el proceso. No se expone a terceros salvo requerimiento judicial o regulatorio.

4.2 Destinatario (receptor)

Acceso al contenido:

- El destinatario recibe el aviso por correo electrónico o SMS, con un enlace que incluye un token de acceso firmado.
- Este token identifica de forma unívoca al destinatario y a la comunicación concreta.
- Para acceder al contenido, el destinatario se autentica con su certificado electrónico. El servicio valida el certificado y comprueba que el número de identificación coincide con el que indicó el remitente. Si la autenticación no se completa, el contenido no se entrega.
- La apertura del enlace se registra como evidencia de acceso, y la lectura del contenido tras la autenticación como evidencia de lectura, con dirección IP, user-agent y fecha y hora.

Registro de decisión:

- Para registrar una decisión (aceptar/rechazar), el destinatario usa el endpoint PUT /api/v1/public/delivery/{token}/status, autenticado con el mismo token de acceso.
- El scope delivery:recipient delimita las operaciones permitidas al destinatario.

Confidencialidad de la identidad del destinatario:

La dirección de contacto del destinatario y su identidad no se exponen en ningún dato público ni en los informes de auditoría descargables por terceros no autorizados.

4.3 Obligaciones

4.3.1 Obligaciones del emisor

El emisor (remitente) se obliga a:

a. Facilitar datos de contacto del destinatario exactos y actualizados, y estar legitimado para usarlos con la finalidad de la comunicación.

b. Ser responsable del contenido que envía: su licitud y su veracidad, y que no contenga software malicioso.
c. Custodiar sus credenciales de acceso al servicio y comunicar a Viafirma, sin demora, cualquier uso no autorizado o sospecha de que se han comprometido.
d. Usar el servicio conforme a esta Declaración de Prácticas, a los términos y condiciones del contrato y a las limitaciones del cap. 4.4.
e. Revisar la respuesta del servicio en el momento del envío: si la comunicación o alguno de sus adjuntos se rechaza, no se envía (cap. 3.4).
f. Cuando proceda, informar al destinatario del tratamiento de sus datos personales y de la finalidad de la comunicación.

4.3.2 Obligaciones de receptor

El receptor (destinatario) se obliga a:

a. Custodiar los medios por los que recibe los avisos y los códigos de autenticación y no facilitarlos a terceros.
b. No reenviar ni ceder a terceros el enlace de acceso a la comunicación.
c. Comunicar a Viafirma, sin demora, cualquier acceso no autorizado del que tenga conocimiento.
d. Tener en cuenta que aceptar o rechazar la comunicación acredita su decisión sobre la recepción, no su conformidad con el contenido.

4.3.3 Obligaciones de otras terceras partes

Quien utilice una evidencia del servicio para acreditar un hecho del proceso de entrega (por ejemplo, un órgano judicial o administrativo, la otra parte de una relación contractual o un auditor) debe:

a. Verificar la firma electrónica y el sello de tiempo de la evidencia o del informe de auditoría, y la validez de los certificados utilizados en la fecha del evento.
b. Interpretar cada evidencia conforme al cap. 2.3 y a la versión de esta Declaración de Prácticas vigente en la fecha del evento: cada evidencia acredita un hecho concreto del proceso de entrega.
c. Tener en cuenta las limitaciones del cap. 4.4.

4.4 Limitaciones de uso

4.4.1 Limitaciones funcionales

Limitación	Valor
Destinatarios por comunicación	1
Plazo máximo de disponibilidad de la comunicación para el destinatario	Fecha límite configurada por el emisor en cada comunicación, con un máximo de 30 días
Número máximo de adjuntos por comunicación	10
Tamaño máximo de cada adjunto y de la comunicación	El tamaño individual o en conjunto de los adjuntos se sumará al tamaño de los metadatos y otros datos necesario para construir la comunicación (request), y ésta no podrá exceder de 10MB.
Tipos de adjunto admitidos	Documentos, imágenes y formatos ofimáticos de uso habitual: PDF, PNG, JPG, etc.
Canales de aviso al destinatario	Correo electrónico y SMS
Métodos de autenticación del destinatario	Certificado digital
Frecuencia de envío	No contemplado
Longitud del motivo de rechazo o cancelación	240 caracteres
Idiomas de la plataforma y de los avisos	Español e inglés

4.4.2 Limitaciones de alcance

a. El servicio acredita los hechos del proceso de entrega indicados en el cap. 2.3. No acredita que el destinatario haya leído o comprendido el contenido, ni su conformidad con él.
b. El servicio no verifica el contenido de la comunicación. Tampoco verifica la identidad que el emisor atribuye al destinatario, más allá del método de autenticación utilizado (cap. 4.2).
c. Las comunicaciones se envían y se reciben dentro de Viafirma Delivery. El servicio no ofrece interoperabilidad con otros prestadores de servicios de entrega electrónica certificada.
d. El servicio se presta en la República Dominicana conforme a la Ley 126-02 y a la Resolución 067-25 del INDOTEL, si hay usos excluidos, por ejemplo notificaciones que la ley obliga a practicar por un canal específico.
e. Las evidencias se conservan durante el período indicado en el cap. 6. Una vez transcurrido, Viafirma no puede aportarlas.

5. CÓMO OBTENER EVIDENCIAS

5.1 Para el emisor

El emisor puede obtener las evidencias generadas a través de los siguientes endpoints autenticados:

- Timeline de eventos → GET /api/v1/communication/{id}/evidence: Lista cronológica de todos los eventos con sus metadatos forenses.
- Informe de auditoría PDF → GET /api/v1/communication/{id}/report: Informe consolidado descargable con todos los eventos firmados, sellados y presentados de forma legalmente comprensible.

5.2 Contenido de las evidencias

Cada evidencia incluye, como mínimo:

- Tipo de evento (SENT, DELIVERED, ACCESSED, FAILED, etc.).
- Fecha y hora del evento, tomadas de los servidores del servicio, y sello de tiempo cualificado (RFC 3161) emitido por la TSA de Viafirma, sincronizada con UTC, sobre los datos del evento. La fecha y hora acreditadas del evento son las de ese sello de tiempo, expresadas en UTC.
- Fingerprint técnico: dirección IP, user-agent, host del servidor de destino.
- Identificador único de la evidencia y de la comunicación asociada.
- Hash del contenido de la comunicación en el momento del evento (integridad).

Si el servicio de sellado de tiempo no está disponible en el momento del evento, el evento se registra con la fecha y hora de los servidores del servicio, sin sello de tiempo, y así consta en la evidencia.

5.3 Para autoridades y auditores

Bajo requerimiento legal o judicial, Viafirma puede proporcionar:

- Los ficheros XML de evidencia almacenados en S3 (inmutables desde su generación).
- Los registros de la tabla rd_evidence_metadata directamente desde la base de datos auditada.
- El informe de auditoría PDF sellado y firmado.

El proceso de entrega a autoridades se realiza bajo protocolo seguro y con registro interno de la solicitud.

6. PERÍODO DE RETENCIÓN

6.1 Plazo mínimo de retención

De conformidad con la normativa dominicana y los estándares ETSI EN 319 521 / 531, el período mínimo de retención de comunicaciones y evidencias es de 10 años desde la fecha de creación de la comunicación, alineado con el plazo de prescripción de acciones comerciales y personales en la República Dominicana.

Para comunicaciones con efectos legales de carácter permanente (según la naturaleza del documento o acuerdo contractual), la retención puede extenderse a perpetuidad bajo configuración específica.

6.2 Configuración del período de retención

El período de retención es configurable por instancia del servicio mediante variable de entorno/configuración, permitiendo adaptarlo al contexto legal del cliente o del país de operación.

6.3 Garantías de inalterabilidad

Durante todo el período de retención:

- Los ficheros XML de evidencia se almacenan con política de inmutabilidad (object lock o equivalente).
- Los registros en base de datos (rd_evidence_metadata) son de solo lectura una vez persistidos; no existe mecanismo de actualización o borrado lógico de evidencias.
- Cualquier acceso a los datos queda registrado en el log de auditoría del sistema.
- Si alguno de los algoritmos o parámetros criptográficos con los que se firman y sellan las evidencias pasa a ser insuficiente para el uso previsto que le queda, Viafirma lo comunica a los clientes y a las partes usuarias con los que tenga acuerdos u otra relación establecida para la prestación del servicio, y protege las evidencias ya emitidas con nuevos sellos de tiempo generados con algoritmos y parámetros suficientes, conforme a su plan de continuidad del negocio.

- Si la clave con la que se firman las evidencias se compromete, Viafirma lo comunica a todos los clientes, a las partes que confían en las evidencias y a las demás entidades con las que tenga acuerdos para la prestación del servicio, indicando que las evidencias firmadas con esa clave pueden dejar de ser válidas desde el momento conocido del compromiso.

6.4 Conservación de los registros de seguridad

Los registros de los eventos de seguridad de la infraestructura del servicio (registros de sistema y de aplicación, arranques y paradas, accesos y actividad de los cortafuegos) se centralizan y se conservan durante 15 años en un repositorio de archivo con acceso restringido. Este plazo no depende de la configuración del período de retención del apartado 6.2, que se aplica a las comunicaciones y las evidencias.

7. DISPOSICIONES DE TERMINACIÓN DEL SERVICIO

7.1 Terminación por el cliente

Si un cliente (organización emisora) termina su contrato con Viafirma:

- Se realiza una exportación completa de todas sus comunicaciones y evidencias antes de la baja efectiva.
- Los datos exportados se entregan al cliente en formato estándar (XML + PDF).
- Viafirma mantiene una copia custodiada de las evidencias durante el período de retención legal, incluso tras la baja del cliente, para garantizar la disponibilidad ante requerimientos legales.

7.2 Terminación del servicio por Viafirma

El cese del servicio Viafirma Delivery se rige por el Plan de Cese de Viafirma (PE-PSC-01), que se mantiene actualizado y se revisa al menos cada dos años. En un cese previsto, con al menos **seis meses de antelación** a la fecha de cese, el prestador:

a. Comunicará por escrito el cese al INDOTEL, como organismo supervisor, e indicará si el servicio se extingue o se transfiere a otro prestador.
b. Comunicará por escrito el cese a todos los clientes (organizaciones remitentes) y a las demás entidades con las que tenga acuerdos: los proveedores del cap. 1.5 y otros prestadores de servicios de confianza.
c. Publicará la información del cese en https://cps.viafirma.do para que la conozcan los destinatarios y las demás partes que confían en las evidencias.
d. Dejará de admitir nuevas comunicaciones a partir de la fecha que se indique en la comunicación del cese. Las comunicaciones en curso seguirán disponibles para sus destinatarios hasta su caducidad, y en cualquier caso hasta la fecha de cese.
e. Facilitará a cada cliente la exportación de sus comunicaciones y evidencias en los formatos del cap. 7.1.
f. Transferirá la custodia de las evidencias a un custodio fiable, que podrá ser el propio prestador o un tercero designado. El custodio las conservará durante el periodo de retención del cap. 6.1 y mantendrá los medios para verificar su firma y su sello de tiempo, o la información necesaria para ello, durante ese mismo periodo. Si no es

posible la transferencia, el prestador mantendrá esa custodia y esos medios de verificación por sí mismo.

g. Procurará acuerdos con otro prestador de servicios de entrega electrónica certificada para transferir el servicio a los clientes que lo deseen.
h. Retirará las autorizaciones a los terceros que actúen en su nombre en la prestación del servicio y destruirá o retirará de uso las claves privadas del servicio, incluidas sus copias, de forma que no puedan recuperarse.

El prestador dispone de un seguro de responsabilidad civil que cubre los costes del cese si no pudiera asumirlos por sí mismo.

En un cese imprevisto (por ejemplo, un incidente grave o la imposibilidad económica de continuar), el prestador hará estas comunicaciones en el menor plazo posible y dará prioridad a la conservación de las evidencias y a los medios para verificarlas.