CPS-ERDS - Viafirma Delivery

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

ÍNDICE

CONTROL DE DOCUMENTO

Título	Prácticas de Certificación del Servicio de Entrega Electrónica Certificada Viafirma Delivery		
Código	CPS-ERDS-DO		
Versión	1.0	**Fecha Versión Actual**	05/06/2026
Fecha Creación	05/06/2026	**Fecha Aprobación**	08/06/2026
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.

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.

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 Electronic Registered Delivery Service Providers – Procedures for electronic delivery.
- 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.

2. QUÉ CONSTITUYE UNA ENTREGA

2.1. Definición de entrega exitosa

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

- SENT: El mensaje ha sido transmitido al servidor de correo del destinatario o al proveedor SMS. Estado: Enviado.
- DELIVERED: El servidor de destino ha confirmado la recepción del mensaje (SMTP 250 OK o confirmación del proveedor). Estado: Entregado.
- ACCESSED: El destinatario ha accedido al contenido de la comunicación a través del enlace seguro con token. Estado: Accedido.
- DECISION: El destinatario ha registrado una decisión explícita (aceptación o rechazo) sobre la comunicación. Estado: Resuelto.

Cada evento genera una evidencia forense firmada con sello de tiempo, asociada de forma irrevocable a la comunicación.

2.2 Entrega fallida

Si el mensaje no puede ser entregado, se registra un evento FAILED o BOUNCED con la causa técnica del fallo. Este evento también constituye evidencia certificada y queda disponible para el emisor como prueba de intento de entrega fallida.

2.3 Evidencias generadas

Por cada evento del ciclo de vida se genera:

- XML de evidencia: almacenado de forma inmutable en S3 con la ruta YYYY/MM/DD/{deliveryId}/{EVENTO}_{evidenceId}.xml.
- Metadatos estructurados: registrados en la tabla rd_evidence_metadata (clave-valor, inmutables, con timestamp).
- Informe de auditoría PDF: disponible al cierre del ciclo, que consolida todo el trail de eventos.

3. CÓMO SE PROTEGE LA COMUNICACIÓN

3.1. AccessKey y TTL

El destinatario accede a la comunicación a través de un token de acceso seguro (AccessKey) con un tiempo de vida (TTL) configurable. Este token es de uso único y se genera mediante HMAC.

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.

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, la identidad del emisor se verifica mediante alguno de los siguientes mecanismos (según nivel de servicio contratado):

- Presencia física ante Viafirma o representante autorizado.
- Certificado electrónico avanzado o cualificado.
- Identificación remota de nivel sustancial o alto mediante los mecanismos soportados por el servidor de autorización Viafirma.

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 accede mediante un token HMAC de acceso único incluido en la notificación de email enviada a su dirección registrada.
- Este token identifica de forma unívoca al destinatario y a la comunicación concreta.
- El acceso se registra como evidencia ACCESSED con fingerprint técnico: dirección IP, user-agent y timestamp.

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 se almacenan cifradas y no se exponen en ningún dato público ni en los informes de auditoría descargables por terceros no autorizados.

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.).
- Timestamp del evento con sello de tiempo cualificado (TSA).
- 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).

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 en S3 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.

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

En caso de cese de la operación del servicio Viafirma Delivery:

- Se notificará a todos los clientes activos con un mínimo de 6 meses de antelación.
- Se facilitará la exportación de todos los datos y evidencias en los formatos definidos en este documento.
- Se designará un custodio de registros responsable de mantener las evidencias durante el período de retención legal restante, ya sea Viafirma o un tercero designado de común acuerdo con los clientes.
- Los procedimientos de transferencia de custodia seguirán lo establecido en ETSI EN 319 401 (requisitos generales para prestadores de servicios de confianza).