Microservicio MsAdaptadorFirmaDigital

Documento Versión: 1.0

Gestión de Seguridad Electrónica

Fecha generación: **30/11/2025**

CONTROL DE VERSIÓN

VERSIÓN	FECHA DE ACTUALIZACIÓN	CARGO	DESCRIPCIÓN
1.0	03/11/2025	Arquitecto de Software	Versión inicial del documento
1.1	29/11/2025	Control de Arquitectura	Corrección del documento basado en observaciones
1.2	30/11/2025	Control de Arquitectura	Revisión estructura de objetos JSON

Tabla de contenido

1 CONTEXTO

El Registro Nacional de Identificación y Estado Civil (RENIEC) es el organismo técnico autónomo encargado de la identificación de los peruanos, otorgar el Documento Nacional de Identidad (DNI) y registrar los hechos vitales. En el marco de la modernización y transformación digital del Estado peruano, RENIEC ha desarrollado el DNI Electrónico (DNIe), un documento de identidad que incorpora tecnología de chip y biometría, permitiendo la autenticación electrónica de ciudadanos y facilitando servicios digitales seguros.

2 INTRODUCCIÓN

Este documento describe el **catálogo de microservicios** identificados para la solución de Personalización del DNIe de RENIEC. El objetivo es establecer una arquitectura técnica moderna, escalable y mantenible que reemplace o complemente los sistemas monolíticos actuales mediante una transición ordenada hacia una arquitectura orientada a microservicios.

2.1 Justificación de la Arquitectura de Microservicios

La adopción de microservicios para esta solución responde a necesidades técnicas y operativas concretas:

Escalabilidad Independiente: Componentes con cargas diferenciadas pueden escalar de forma independiente según demanda real, optimizando recursos de infraestructura.

Resiliencia y Tolerancia a Fallos: El fallo de un microservicio no compromete servicios críticos. Los patrones Circuit Breaker y Retry garantizan continuidad operativa.

Agilidad en el Desarrollo: Equipos autónomos pueden desarrollar, probar y desplegar servicios de manera independiente, reduciendo tiempos de entrega.

Mantenibilidad y Evolución Tecnológica: Cada servicio puede evolucionar tecnológicamente sin afectar al ecosistema completo.

Trazabilidad y Observabilidad: Arquitectura distribuida permite implementar logging centralizado, distributed tracing y métricas granulares.

2.2 Arquitectura de Referencia

La solución se estructura en tres capas principales:

Capa de Exposición (API Management Layer): API Manager como punto único de entrada con gestión centralizada de seguridad, throttling y versionado.

Capa de Representación (Microservices Layer): Microservicios de negocio con lógica específica de dominio y responsabilidad única.

Capa de Integración (Integration Layer): Event Streaming para comunicación asíncrona y conectores a sistemas legados.

2.3 Códigos de Respuesta HTTP Estándar

Todos los microservicios implementan un conjunto estandarizado de códigos de respuesta HTTP para garantizar consistencia:

Código	Descripción
200	OK - Operación completada exitosamente
201	Created - Recurso creado exitosamente

400	Bad Request - Parámetros inválidos o datos incompletos
401	Unauthorized - Token JWT inválido, expirado o ausente
403	Forbidden - Sin permisos suficientes para ejecutar la operación
404	Not Found - Recurso no encontrado en el sistema
408	Request Timeout - Tiempo de espera agotado al conectar
409	Conflict - Conflicto con el estado actual del recurso
422	Unprocessable Entity - Datos válidos, pero no procesables por reglas de negocio
429	Too Many Requests - Límite de rate limit excedido
500	Internal Server Error - Error interno del servicio (información generalizada al exterior, detalle en logs)
502	Bad Gateway - Servicio externo no disponible o respuesta inválida
503	Service Unavailable - Servicio temporalmente no disponible o Circuit Breaker abierto
504	Gateway Timeout - Servicio externo no respondió en tiempo esperado

3 CATÁLOGO DE MICROSERVICIOS

3.1 Microservicio MsAdaptadorFirmaDigital

Microservicio especializado en la gestión exclusiva de firmas digitales PKI/X.509 dentro de la plataforma SIIRC. Orquesta el proceso completo de firma digital, desde la validación de certificados hasta la integración visual de la firma manuscrita en documentos PDF, garantizando la autenticidad, integridad y validez legal de los documentos firmados.

Centralizar la lógica de firma digital, desacoplando el resto de los componentes del sistema de la complejidad técnica de integrarse directamente con diferentes proveedores de servicios de firma digital certificados.

3.1.1 Endpoint: Firmar Documento

Firma digitalmente un documento PDF individual utilizando el certificado digital del usuario autenticado. Soporta firma simple, así como firma con representación visual manuscrita (grafo) embebida en el documento

Atributo	Valor
Path	/api/v1/firma/MsAdaptadorFirmaDigital/firmar-documento
API Gateway	Interno
Método HTTP	POST
Protocolo	REST/HTTP
Headers	Authorization String(Token JWT del usuario autenticado) X-Correlation-ID String(ID de correlación para trazabilidad generado por API Manager) X-Request-ID String(ID único de la solicitud) Content-Type String(application/json)

Entrada	{
	"tramiteId": "string",
	"documento": {
	"nombre": "string",
	"tipoDocumento": "string",
	"contenidoBase64": "string",

	"hashSHA256": "string"
	},
	"firmante": {
	"usuarioId": "string",
	"dni": "string",
	"nombreCompleto": "string",
	"cargo": "string",
	"certificadoId": "string"
	},
	"configuracionFirma": {
	"tipoCertificado": "string",
	"proveedorFirma": "string",
	"incluyeGrafo": "boolean",
	"posicionGrafo": {
	"pagina": "integer",
	"coordenadaX": "integer",
	"coordenadaY": "integer",
	"ancho": "integer",
	"alto": "integer"
	},
	"razonFirma": "string",
	"ubicacionFirma": "string",
	"validarVigenciaCertificado": "boolean"
	},
	"metadata": {
	"moduloOrigen": "string",
	"ipCliente": "string",
	"navegador": "string"
	}
	}

Respuesta	{
	"status": "string",
	"data": {
	"procesoFirmaId": "string",
	"tramiteId": "string",
	"estadoFirma": "string",
	"documentoFirmado": {
	"contenidoBase64": "string ",
	"hashSHA256": "string"
	},
	"firmaAplicada": {
	"certificadoId": "string",
	"timestampFirma": " YYYY-MM-DDThh:mm:ss±hh:mm "
	},
	"validaciones": {
	"certificadoValido": "boolean",
	"certificadoNoRevocado": "boolean"
	},
	"auditoria": {
	"idTransaccionProveedor": "string"
	}
	},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ss±hh:mm",
	"correlationId": "string",
	"version": "string"
	}
	}

Error Response	"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": "integer",
	"errores": [
	{

```
        "detalleError": "string"
      }
    ]
  }
```

3.1.1.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Longitud mínima	Longitud máxima
Trámite ID	tramiteId	String	Sí	10	50
Nombre Documento	documento.nombre	String	Sí	5	255
Tipo Documento	documento.tipoDocumento	String	Sí	3	50
Contenido Base64	documento.contenidoBase64	String (base64)	Sí	100	N/A
Hash SHA256	documento.hashSHA256	String (SHA-256)	Sí	64	64
Usuario ID	firmante.usuarioId	String	Sí	8	50
DNI Firmante	firmante.dni	String	Sí	8	8
Nombre Completo	firmante.nombreCompleto	String	Sí	10	200
Cargo	firmante.cargo	String	Sí	5	100
Certificado ID	firmante.certificadoId	String	Sí	10	100
Tipo Certificado	configuracionFirma.tipoCertificado	String	Sí	3	20
Proveedor Firma	configuracionFirma.proveedorFirma	String	Sí	5	50
Incluye Grafo	configuracionFirma.incluyeGrafo	Boolean	Sí	-	-
Página del Grafo	configuracionFirma.posicionGrafo.pagina	Integer	No	1	-
Coordenada X	configuracionFirma.posicionGrafo.coordenadaX	Integer	No	0	-
Coordenada Y	configuracionFirma.posicionGrafo.coordenadaY	Integer	No	0	-
Ancho	configuracionFirma.posicionGrafo.ancho	Integer	No	10	-
Alto	configuracionFirma.posicionGrafo.alto	Integer	No	10	-
Razón de Firma	configuracionFirma.razonFirma	String	No	5	200
Ubicación de Firma	configuracionFirma.ubicacionFirma	String	No	5	200
Validar Vigencia	configuracionFirma.validarVigenciaCertificado	Boolean	Sí	-	-
Módulo Origen	metadata.moduloOrigen	String	No	5	100

IP Cliente	metadata.ipCliente	String (IPv4/IPv6)	No	7	45
Navegador	metadata.navegador	String	No	3	100

3.1.1.2 Parámetros de Respuesta

Nombre	Tipo	Obligatorio	Descripción
status	String	Sí	Estado general de la operación (
data.procesoFirmaId	String	Sí	Identificador único del proceso de firma.
data.tramiteId	String	Sí	Identificador del trámite asociado al documento firmado.
data.estadoFirma	String	Sí	Estado actual del proceso de firma
data.documentoFirmado	Object	Sí	Contiene la información del documento resultante de la firma.
data.documentoFirmado.contenidoBase64	String (Base64)	Sí	Documento firmado codificado en formato Base64.
data.documentoFirmado.hashSHA256	String (SHA-256)	Sí	Hash SHA-256 del documento firmado, usado para verificación de integridad.
data.firmaAplicada	Object	Sí	Información sobre la firma digital aplicada.
data.firmaAplicada.certificadoId	String	Sí	Identificador del certificado digital utilizado en la firma.
data.firmaAplicada.timestampFirma	String (ISO 8601, RFC 3161)	Sí	Fecha y hora exacta en que se aplicó la firma digital.
data.validaciones	Object	Sí	Resultados de las validaciones de la firma y certificado.
data.validaciones.certificadoValido	Boolean	Sí	Indica si el certificado digital es válido.
data.validaciones.certificadoNoRevocado	Boolean	Sí	Indica si el certificado no se encuentra revocado
data.auditoria	Object	Sí	Información de trazabilidad y auditoría del proceso de firma.
data.auditoria.idTransaccionProveedor	String	Sí	Identificador de la transacción registrada por el proveedor externo de firma.
metadata	Object	Sí	Metadatos asociados a la operación realizada.

metadata.correlationId	String	Sí	Identificador único de correlación para trazabilidad distribuida.
metadata.timestamp	String (ISO 8601 UTC)	Sí	Fecha y hora de procesamiento de la operación.
metadata.version	String	Sí	Versión del servicio (ejemplo: 1.0.0).
error	Object	No	Información sobre un posible error ocurrido durante la operación.
error.tipo	String	No	Tipo de error detectado
error.titulo	String	No	Título o descripción breve del error.
error.estado	Integer	No	Código de estado o código HTTP del error.
error.errores	Array[Object]	No	Lista de errores específicos detectados.
error.errores[].detalleError	String	No	Descripción detallada del error individual.

3.1.1.3 Valores para el Atributo de statusCode

Código	Respuesta	Descripción
200	OK	Documento firmado exitosamente.
400	Bad Request	Documento inválido o parámetros incompletos.
401	Unauthorized	Token JWT inválido.
403	Forbidden	Usuario sin permisos para firmar documentos.
408	Request Timeout	Timeout al conectar con el proveedor de firma.
422	Unprocessable Entity	Certificado revocado o expirado.
500	Internal Server Error	Error interno al procesar la firma.
502	Bad Gateway	Error al comunicarse con el proveedor de firma.
503	Service Unavailable	Proveedor de firma no disponible.

3.1.2 Endpoint: Firmar Lote de Documentos

Firma digitalmente un lote de documentos PDF en una sola transacción, optimizando el proceso cuando múltiples documentos deben ser firmados por el mismo usuario con el mismo certificado.

Atributo	Valor
Path	/api/v1/firma/MsAdaptadorFirmaDigital/firmar-lote
API Gateway	Interno
Método HTTP	POST
Protocolo	REST/HTTP
Headers	Authorization String(Token JWT del usuario autenticado) X-Correlation-ID String(ID de correlación para trazabilidad generado por API Manager)

	X-Request-ID String(ID único de la solicitud) Content-Type String(application/json)

Entrada	<pre>{
	"loteId": "string",
	"descripcionLote": "string",
	"documentos": [
	{
	"documentoId": "string",
	"tramiteId": "string",
	"nombre": "string",
	"tipoDocumento": "string",
	"contenidoBase64": "string",
	"hashSHA256": "string"
	}
	],
	"firmante": {
	"usuarioId": "string",
	"dni": "string",
	"nombreCompleto": "string",
	"cargo": "string",
	"certificadoId": "string"
	},
	"configuracionFirma": {
	"tipoCertificado": "string",
	"proveedorFirma": "string",
	"incluyeGrafo": "boolean",
	"posicionGrafo": {
	"pagina": "integer",
	"coordenadaX": "integer",
	"coordenadaY": "integer",
	"ancho": "integer",
	"alto": "integer"
	},
	"procesarEnParalelo": "boolean",
	"maximoParalelo": "integer",
	"validarVigenciaCertificado": "boolean"
	},
	"metadata": {
	"moduloOrigen": "string",
	"ipCliente": "string”
	}
	}</pre>

Respuesta	<pre>{
	"loteId": "string",
	"procesoLoteId": "string",
	"estadoLote": "string",
	"totalDocumentos": "integer",
	"documentosFirmados": "integer",
	"documentosFallidos": "integer",
	"resultadosDocumentos": [
	{
	"documentoId": "string",
	"tramiteId": "string",
	"estado": "string",
	"procesoFirmaId": "string",
	"documentoFirmado": {
	"nombre": "string",
	"hashSHA256": "string",
	"tamanoBytes": "integer"
	},
	"timestampFirma": "string"
	}
	],
	"firmante": {</pre>

	"usuarioId": "string",
	"nombreCompleto": "string",
	"certificadoId": "string"
	},
	"auditoria": {
	"loteIniciado": "string ",
	"loteCompletado": "string “,
	"tiempoProcesamientoMs": "integer",
	"proveedorUtilizado": "string"
	},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ss±hh:mm",
	"correlationId": "string",
	"tiempoRespuestaMs": "integer"
	}
	}

Error Response	"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": "integer",
	"errores": [
	{
	"detalleError": "string"
	}
	]
	}

3.1.2.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Longitud mínima	Longitud máxima
Nombre Documento	documento.nombre	String	Sí	5	255
Contenido Base64	documento.contenidoBase64	String (base64)	Sí	100	N/A
Hash SHA256	documento.hashSHA256	String (SHA-256)	Sí	64	64
Verificar Certificado	validaciones.verificarCertificado	Boolean	No	-	-
Verificar Revocación	validaciones.verificarRevocacion	Boolean	No	-	-
Verificar Cadena de Confianza	validaciones.verificarCadenaConfianza	Boolean	No	-	-
Verificar Timestamp	validaciones.verificarTimestamp	Boolean	No	-	-
Verificar Integridad	validaciones.verificarIntegridad	Boolean	No	-	-
Módulo Origen	metadata.moduloOrigen	String	No	5	100
Motivo de Validación	metadata.motivoValidacion	String	No	5	200

3.1.2.2 Parámetros de Respuesta:

Nombre	Tipo	Obligatorio	Descripción
loteId	String	Sí	Identificador único del lote procesado.
procesoLoteId	String	Sí	Identificador del proceso de firma asociado al lote.
estadoLote	String	Sí	Estado actual del proceso de firma del lote.
totalDocumentos	Integer	Sí	Cantidad total de documentos incluidos en el lote.
documentosFirmados	Integer	Sí	Cantidad de documentos firmados exitosamente.
documentosFallidos	Integer	Sí	Cantidad de documentos que fallaron durante el proceso de firma.
resultadosDocumentos	Array[Object]	Sí	Lista detallada de resultados por cada documento procesado.
resultadosDocumentos[].documentoId	String	Sí	Identificador único del documento dentro del lote.
resultadosDocumentos[].tramiteId	String	Sí	Identificador del trámite asociado al documento.
resultadosDocumentos[].estado	String	Sí	Estado final del proceso de firma para el documento.
resultadosDocumentos[].procesoFirmaId	String	Sí	Identificador del proceso de firma individual del documento.

resultadosDocumentos[].documentoFirmado	Object	Condicional	Información del documento firmado
resultadosDocumentos[].documentoFirmado.nombre	String	Sí	Nombre del documento firmado.
resultadosDocumentos[].documentoFirmado.hashSHA256	String (SHA-256)	Sí	Hash del documento firmado, usado para verificación de integridad.
resultadosDocumentos[].documentoFirmado.tamanoBytes	Integer	Sí	Tamaño del documento firmado en bytes.
resultadosDocumentos[].timestampFirma	String (ISO 8601 UTC)	Sí	Fecha y hora de la firma digital aplicada.
firmante	Object	Sí	Información del firmante que ejecutó el proceso.
firmante.usuarioId	String	Sí	Identificador del usuario firmante.
firmante.nombreCompleto	String	Sí	Nombre completo del firmante.
firmante.certificadoId	String	Sí	Identificador del certificado digital utilizado para la firma.
auditoria	Object	Sí	Información de auditoría del proceso de firma por lote.
auditoria.loteIniciado	String (ISO 8601 UTC)	Sí	Fecha y hora de inicio del proceso de firma del lote.
auditoria.loteCompletado	String (ISO 8601 UTC)	Sí	Fecha y hora de finalización del proceso de firma.
auditoria.tiempoProcesamientoMs	Integer	Sí	Tiempo total de procesamiento del lote en milisegundos.

auditoria.proveedorUtilizado	String	Sí	Nombre del proveedor de firma digital utilizado.
metadata	Object	Sí	Metadatos asociados al procesamiento del lote.
metadata.timestamp	String (ISO 8601 UTC)	Sí	Marca de tiempo del procesamiento del lote.
metadata.correlationId	String	Sí	Identificador de correlación para trazabilidad distribuida.
metadata.tiempoRespuestaMs	Integer	Sí	Tiempo total de respuesta de la operación
error	Object	No	Objeto que describe los errores ocurridos durante la operación.
error.tipo	String	No	Tipo de error detectado.
error.titulo	String	No	Título o descripción breve del error.
error.estado	Integer	No	Código de estado HTTP o interno del error.
error.errores	Array[Object]	No	Listado de errores específicos ocurridos.
error.errores[].detalleError	String	No	Descripción detallada del error específico.

3.1.2.3 Valores para el atributo statusCode:

Código	Respuesta	Descripción
200	OK	Lote procesado exitosamente
400	Bad Request	Lote inválido o supera el límite permitido de documentos.
401	Unauthorized	Token JWT inválido o no autorizado.
403	Forbidden	Usuario sin permisos para realizar firma masiva.

422	Unprocessable Entity	Certificado digital inválido o no verificado.
500	Internal Server Error	Error crítico durante el procesamiento del lote.
503	Service Unavailable	Proveedor de firma no disponible temporalmente.

3.1.3 Endpoint: Validar Firma Digital

Valida la autenticidad e integridad de un documento PDF firmado digitalmente, verificando el certificado, la cadena de confianza, el estado de revocación y el timestamp.

Atributo	Valor
Path	/api/v1/firma/MsAdaptadorFirmaDigital/validar
API Gateway	Interno
Método HTTP	POST
Protocolo	REST/HTTP
Headers	Authorization String(Token JWT del usuario autenticado) X-Correlation-ID String(ID de correlación para trazabilidad generado por API Manager) X-Request-ID String(ID único de la solicitud) Content-Type String(application/json)
Entrada	{ "documento": { "nombre": "string", "contenidoBase64": "string", "hashSHA256": "string" }, "validaciones": { "verificarCertificado": "boolean", "verificarRevocacion": "boolean", "verificarCadenaConfianza": "boolean", "verificarTimestamp": "boolean", "verificarIntegridad": "boolean" }, "metadata": { "moduloOrigen": "string", "motivoValidacion": "string" } }
Resultado	{ "validacionId": "string", "documento": { "nombre": "string", "hashSHA256": "string", "tamanoBytes": "integer" }, "resultadoValidacion": { "esValido": "boolean", "resumenValidacion": "string", "firmasEncontradas": "integer", "firmasValidas": "integer", "firmasInvalidas": "integer" }, "detallesFirmas": [{ "numeroFirma": "integer", "firmante": {

	"nombreCompleto": "string",
	"dni": "string",
	"cargo": "string",
	"email": "string"
	},
	"certificado": {
	"numeroSerie": "string",
	"emisor": "string",
	"vigenciaDesde": "string ",
	"vigenciaHasta": "string",
	"algoritmo": "string",
	"longitudClave": "integer"
	},
	"validaciones": {
	"firmaValida": "boolean",
	"certificadoValido": "boolean",
	"certificadoVigente": "boolean",
	"certificadoNoRevocado": "boolean",
	"cadenaConfianzaVerificada": "boolean",
	"timestampValido": "boolean",
	"integridadDocumento": "boolean"
	},
	"timestamp": {
	"fechaHoraFirma": "string",
	"autoridadTimestamp": "string",
	"algoritmoTimestamp": "string"
	},
	"detallesValidacion": {
	"revocacion": {
	"metodoVerificacion": "string",
	"urlOCSP": "string",
	"estadoCertificado": "string ",
	"fechaVerificacion": "string "
	},
	"cadenaConfianza": {
	"certificadosEnCadena": "integer",
	"raizConfiable": "string",
	"todosVerificados": "boolean"
	}
	}
	}
	],
	"advertencias": ["string"],
	"errores": ["string"],
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ss±hh:mm",
	"correlationId": "string",
	"tiempoValidacionMs": "integer"
	}
	}

Error Response	"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": "integer",
	"errores": [
	{
	"detalleError": "string"
	}
	]
	}

3.1.3.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Longitud mínima	Longitud máxima
Nombre Documento	documento.nombre	String	Sí	1	255
Contenido Base64	documento.contenidoBase64	String	Sí	10	-
Hash SHA256	documento.hashSHA256	String	Sí	64	64
Verificar Certificado	validaciones.verificarCertificado	Boolean	No	-	-
Verificar Revocación	validaciones.verificarRevocacion	Boolean	No	-	-
Verificar Cadena Confianza	validaciones.verificarCadenaConfianza	Boolean	No	-	-
Verificar Timestamp	validaciones.verificarTimestamp	Boolean	No	-	-
Verificar Integridad	validaciones.verificarIntegridad	Boolean	No	-	-
Módulo Origen	metadata.moduloOrigen	String	No	1	100
Motivo de Validación	metadata.motivoValidacion	String	No	1	255

3.1.3.2 Parámetros de Respuesta:

Nombre	Tipo	Obligatorio	Descripción
validacionId	String	Sí	ID único de la validación realizada
documento.nombre	String	Sí	Nombre del documento validado
documento.hashSHA256	String	Sí	Hash del documento en formato SHA-256
documento.tamanoBytes	Integer	Sí	Tamaño del archivo en bytes
resultadoValidacion.esValido	Boolean	Sí	Indica si el documento es válido globalmente
resultadoValidacion.resumenValidacion	String	No	Resumen textual del resultado de la validación
resultadoValidacion.firmasEncontradas	Integer	Sí	Cantidad de firmas detectadas en el documento

resultadoValidacion.firmasValidas	Integer	Sí	Cantidad de firmas válidas encontradas
resultadoValidacion.firmasInvalidas	Integer	No	Cantidad de firmas no válidas
detallesFirmas[].numeroFirma	Integer	Sí	Número de orden de la firma analizada
detallesFirmas[].firmante.nombreCompleto	String	Sí	Nombre completo del firmante
detallesFirmas[].firmante.dni	String	No	DNI del firmante
detallesFirmas[].firmante.cargo	String	No	Cargo o rol del firmante
detallesFirmas[].firmante.email	String	No	Correo electrónico del firmante
detallesFirmas[].certificado.numeroSerie	String	Sí	Número de serie del certificado digital
detallesFirmas[].certificado.emisor	String	Sí	Autoridad emisora del certificado
detallesFirmas[].certificado.vigenciaDesde	String (ISO 8601 UTC)	Sí	Fecha de inicio de vigencia del certificado
detallesFirmas[].certificado.vigenciaHasta	String (ISO 8601 UTC)	Sí	Fecha de expiración del certificado
detallesFirmas[].certificado.algoritmo	String	Sí	Algoritmo criptográfico usado en la firma
detallesFirmas[].certificado.longitudClave	Integer	Sí	Longitud de la clave en bits
detallesFirmas[].validaciones.firmaValida	Boolean	Sí	Indica si la firma digital es válida
detallesFirmas[].validaciones.certificadoValido	Boolean	Sí	Indica si el certificado es válido
detallesFirmas[].validaciones.certificadoVigente	Boolean	Sí	Indica si el certificado no ha expirado
detallesFirmas[].validaciones.certificadoNoRevocado	Boolean	Sí	Indica si el certificado no

			está revocado
detallesFirmas[].validaciones.cadenaConfianzaVerificada	Boolean	Sí	Verifica si la cadena de confianza está completa
detallesFirmas[].validaciones.timestampValido	Boolean	No	Indica si el sello de tiempo es válido
detallesFirmas[].validaciones.integridadDocumento	Boolean	Sí	Indica si la integridad del documento fue preservada
detallesFirmas[].timestamp.fechaHoraFirma	String (ISO 8601 UTC)	No	Fecha y hora en que se realizó la firma
detallesFirmas[].timestamp.autoridadTimestamp	String	No	Autoridad que emitió el sello de tiempo
detallesFirmas[].timestamp.algoritmoTimestamp	String	No	Algoritmo utilizado para el sello de tiempo
detallesFirmas[].detallesValidacion.revocacion.metodoVerificacion	String	No	Método utilizado para verificar la revocación
detallesFirmas[].detallesValidacion.revocacion.urlOCSP	String	No	URL del servicio OCSP utilizado
detallesFirmas[].detallesValidacion.revocacion.estadoCertificado	String	No	Estado del certificado según la verificación
detallesFirmas[].detallesValidacion.revocacion.fechaVerificacion	String (ISO 8601 UTC)	No	Fecha y hora de la verificación de revocación
detallesFirmas[].detallesValidacion.cadenaConfianza.certificadosEnCadena	Integer	No	Número de certificados en la cadena de confianza
detallesFirmas[].detallesValidacion.cadenaConfianza.raizConfiable	String	No	Nombre de la autoridad raíz confiable
detallesFirmas[].detallesValidacion.cadenaConfianza.todosVerificados	Boolean	No	Indica si todos los certificados de la cadena

			fueron verificados
advertencias	Array[String]	No	Lista de advertencias o avisos emitidos durante la validación
errores	Array[String]	No	Lista de errores generales detectados
metadata.timestamp	String (ISO 8601 UTC)	Sí	Marca de tiempo de la validación
metadata.correlationId	String	Sí	Identificador único de correlación para trazabilidad
metadata.tiempoValidacionMs	Integer	Sí	Tiempo total de validación en milisegundos
error.tipo	String	No	Tipo de error en caso de fallo del proceso
error.titulo	String	No	Título o resumen del error
error.estado	Integer	No	Código HTTP o interno asociado al error
error.errores[].detalleError	String	No	Descripción detallada del error ocurrido

3.1.3.3 Valores para el atributo statusCode:

Código	Respuesta	Descripción
200	OK	Validación realizada exitosamente
400	Bad Request	El documento no es un PDF válido o está dañado.
401	Unauthorized	Token JWT inválido o no autorizado.
422	Unprocessable Entity	El documento no contiene firmas digitales válidas.
500	Internal Server Error	Error interno al procesar o validar el documento.