



# **Microservicio MsCoreogCertificadosDigitales**

Documento Versión: 1.0

Gestión de Seguridad Electrónica



Fecha generación: **01/12/2025**

**CONTROL DE VERSIÓN**

| VERSIÓN | FECHA DE ACTUALIZACIÓN | CARGO                  | DESCRIPCIÓN                   |
|---------|------------------------|------------------------|-------------------------------|
| 1.0     | 03/11/2025             | Arquitecto de Software | Versión inicial del documento |
| 1.1     | 01/12/2025             | Arquitecto de Software | Revisar flujo de pasos        |
|         |                        |                        |                               |
|         |                        |                        |                               |
|         |                        |                        |                               |

## Tabla de contenido

|       |  |   |
|-------|--|---|
| 1     | CONTEXTO .....   | 4 |
| 2     | INTRODUCCIÓN .....                                       | 4 |
| 2.1   | Justificación de la Arquitectura de Microservicios ..... | 4 |
| 2.2   | Arquitectura de Referencia .....                         | 4 |
| 2.3   | Códigos de Respuesta HTTP Estándar .....                 | 4 |
| 3     | CATÁLOGO DE MICROSERVICIOS .....                         | 5 |
| 3.1   | Microservicio MsCoreogCertificadosDigitales .....        | 5 |
| 3.1.1 | Endpoint: Obtener Certificado Digital .....              | 5 |

# 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 MsCoreogCertificadosDigitales

El MsCoreogCertificadosDigitales es un microservicio de coreografía encargado de coordinar el flujo técnico de emisión del Certificado Digital DNle.

Este microservicio actúa como un intermediario de negocio, aislando al SIIRC de la complejidad de la infraestructura PKI y ejecutando una secuencia garantizada de dos pasos obligatorios mediante el consumo directo de los siguientes endpoints del MsAdaptadorPKI:

- Paso 1 – Generar Identificadores PKI

POST /api/v1/adaptador/MsAdaptadorPKI/generarNumerosSolicitud2

- Paso 2 – Emitir Certificado Digital DNle

POST /api/v1/adaptador/MsAdaptadorPKI/generarCertificadoDigitalDniE

El coreógrafo administra los estados intermedios (solicitudPkild), registra los tiempos por paso, el manejo de fallas y entrega el certificado emitido.

#### 3.1.1 Endpoint: Obtener Certificado Digital

Coordina el proceso completo de obtención de certificados digitales para un ciudadano, ejecutando secuencialmente la generación de par de claves y la emisión de certificados a través del sistema PKI.

| Atributo    | Valor   |
|-------------|---|
| Path        | /api/v1/coreog/MsCoreogCertificadosDigitales/obtener-certificado-digital  |
| API Gateway | Interno   |
| Método HTTP | POST  |
| Protocolo   | REST/HTTP   |
| Headers     | Authorization String(Bearer token JWT para autenticación)<br>Content-Type String("application/json")<br>X-Correlation-ID UUID(Identificador único de correlación para trazabilidad distribuida) |

|                  |  |
|------------------|--|
|                  | X-Request-ID    UUID(Identificador único de la solicitud)<br>X-Office-Code   String(Código de oficina donde se realiza la solicitud)<br>X-Device-ID    String(ID del dispositivo desde donde se origina la solicitud)<br>X-Channel       String(Canal de origen)   |
| <b>Entrada</b>   | <pre>{   "solicitud": {     "numeroDocumento": "string",     "tipoDocumento": "string",     "codigoSolicitudTramite": "string",     "numeroTramite": "string"   },   "ciudadano": {     "nombres": "string",     "apellidoPaterno": "string",     "apellidoMaterno": "string",     "fechaNacimiento": "YYYY-MM-DD",     "sexo": "string",     "correoElectronico": "string (email)",     "departamento": "string",     "provincia": "string",     "distrito": "string"   },   "configuracionCertificados": {     "tipoCertificados": ["string"],     "vigenciaAnios": "integer",     "usoExtendido": "boolean",     "nivelSeguridad": "string"   },   "metadatos": {     "oficinaOrigen": "string",     "usuarioRegistrador": "string",     "ipOrigen": "string (IPv4/IPv6)",     "timestampSolicitud": "YYYY-MM-DDThh:mm:ssZ"   } }</pre>                 |
| <b>Respuesta</b> | <pre>{   "success": true,   "statusCode": 0,   "message": "string",   "data": {     "transaccion": {       "transaccionId": "string",       "codigoSolicitudTramite": "string",       "estado": "string",       "fechaInicio": "YYYY-MM-DDThh:mm:ssZ",       "fechaFin": "YYYY-MM-DDThh:mm:ssZ",       "tiempoProcesamientoMs": 0     },     "ciudadano": {       "numeroDocumento": "string",       "nombreCompleto": "string"     },     "certificados": [       {         "tipoCertificado": "string",         "certificadoId": "string",         "numeroSerie": "string",         "fechaEmision": "YYYY-MM-DDThh:mm:ssZ",         "fechaVencimiento": "YYYY-MM-DDThh:mm:ssZ",         "vigenciaAnios": 0,         "estadoCertificado": "string",         "algoritmoFirma": "string",         "longitudClave": 0,         "subjectDN": "string", </pre> |

```

    "huellaCertificado": "string",
    "certificadoBase64": "string"
  },
],
"pasosProceso": {
  "paso1GeneracionClaves": {
    "estado": "string",
    "solicitudPkild": "string",
    "fechaInicio": "YYYY-MM-DDThh:mm:ssZ",
    "fechaFin": "YYYY-MM-DDThh:mm:ssZ",
    "intentos": 0
  },
  "paso2EmisionCertificado": {
    "estado": "string",
    "fechaInicio": "YYYY-MM-DDThh:mm:ssZ",
    "fechaFin": "YYYY-MM-DDThh:mm:ssZ",
    "intentos": 0
  }
},
"auditoria": {
  "registroAuditorialId": "string",
  "usuarioEjecutor": "string",
  "oficinaEjecucion": "string",
  "ipCliente": "string"
}
},
"metadata": {
  "timestamp": "YYYY-MM-DDThh:mm:ssZ",
  "correlationId": "string",
  "version": "1.0.0",
  "tiempoRespuesta": "string"
},
"error": {
  "tipo": "string",
  "titulo": "string",
  "estado": 0,
  "errores": [
    {
      "detalleError": "string"
    }
  ]
}
}
}

```

### 3.1.1.1 Parámetros de entrada

| Dato      | Atributo               | Tipo          | Obligatorio | Long. Mín. | Long. Máx. |
|-----------|------------------------|---------------|-------------|------------|------------|
| solicitud | numeroDocumento        | String        | Sí          | 8          | 12         |
| solicitud | tipoDocumento          | String        | Sí          | 2          | 3          |
| solicitud | codigoSolicitudTramite | String        | Sí          | 1          | 30         |
| solicitud | numeroTramite          | String        | Sí          | 1          | 30         |
| ciudadano | nombres                | String        | Sí          | 1          | 100        |
| ciudadano | apellidoPaterno        | String        | Sí          | 1          | 50         |
| ciudadano | apellidoMaterno        | String        | No          | 1          | 50         |
| ciudadano | fechaNacimiento        | String (Date) | Sí          | 10         | 10         |

|                           |                    |                      |    |    |     |
|---------------------------|--------------------|----------------------|----|----|-----|
| ciudadano                 | sexo               | String               | Sí | 1  | 1   |
| ciudadano                 | correoElectronico  | String               | No | 5  | 100 |
| ciudadano                 | departamento       | String               | Sí | 1  | 50  |
| ciudadano                 | provincia          | String               | Sí | 1  | 50  |
| ciudadano                 | distrito           | String               | Sí | 1  | 50  |
| configuracionCertificados | tipoCertificados   | Array[String]        | Sí | 1  | 3   |
| configuracionCertificados | vigenciaAnios      | Integer              | Sí | 1  | 4   |
| configuracionCertificados | usoExtendido       | Boolean              | No | -  | -   |
| configuracionCertificados | nivelSeguridad     | String               | No | 4  | 10  |
| metadatos                 | oficinaOrigen      | String               | Sí | 1  | 50  |
| metadatos                 | usuarioRegistrador | String               | Sí | 1  | 30  |
| metadatos                 | ipOrigen           | String               | No | 7  | 45  |
| metadatos                 | timestampSolicitud | String<br>(DateTime) | Sí | 20 | 30  |

### 3.1.1.2 Respuesta

| Dato             | Atributo               | Tipo                 | Obligatorio | Descripción   |
|------------------|------------------------|----------------------|-------------|---|
| success          | –                      | Boolean              | Sí          | Indica si la operación fue exitosa                        |
| statusCode       | –                      | Integer              | Sí          | Código HTTP de respuesta                                  |
| message          | –                      | String               | Sí          | Mensaje descriptivo del resultado                         |
| data.transaccion | transaccionId          | String               | Sí          | Identificador único de la transacción de certificados     |
| data.transaccion | codigoSolicitudTramite | String               | Sí          | Código de la solicitud origen                             |
| data.transaccion | estado                 | String               | Sí          | Estado de la transacción: COMPLETADO, FALLIDO, EN_PROCESO |
| data.transaccion | fechaInicio            | String<br>(DateTime) | Sí          | Fecha/hora de inicio del proceso                          |
| data.transaccion | fechaFin               | String<br>(DateTime) | Sí          | Fecha/hora de finalización del proceso                    |
| data.transaccion | tiempoProcesamientoMs  | Integer              | Sí          | Tiempo total de procesamiento en milisegundos             |



|  |                   |                   |    |  |
|--|-------------------|-------------------|----|--|
| <b>data.ciudadano</b>                            | numeroDocumento   | String            | Sí | Número de documento del titular        |
| <b>data.ciudadano</b>                            | nombreCompleto    | String            | Sí | Nombre completo del titular            |
| <b>data.certificados[]</b>                       | tipoCertificado   | String            | Sí | FIRMA_DIGITAL, AUTENTICACION, CIFRADO  |
| <b>data.certificados[]</b>                       | certificadoId     | String            | Sí | Identificador único del certificado    |
| <b>data.certificados[]</b>                       | numeroSerie       | String            | Sí | Número de serie del certificado        |
| <b>data.certificados[]</b>                       | fechaEmision      | String (DateTime) | Sí | Fecha de emisión del certificado       |
| <b>data.certificados[]</b>                       | fechaVencimiento  | String (DateTime) | Sí | Fecha de vencimiento del certificado   |
| <b>data.certificados[]</b>                       | vigenciaAños      | Integer           | Sí | Años de vigencia                       |
| <b>data.certificados[]</b>                       | estadoCertificado | String            | Sí | Estado: ACTIVO, REVOCADO, SUSPENDIDO   |
| <b>data.certificados[]</b>                       | algoritmoFirma    | String            | Sí | Algoritmo de firma utilizado           |
| <b>data.certificados[]</b>                       | longitudClave     | Integer           | Sí | Longitud de la clave (bits)            |
| <b>data.certificados[]</b>                       | subjectDN         | String            | Sí | Distinguished Name del certificado     |
| <b>data.certificados[]</b>                       | huellaCertificado | String            | Sí | Fingerprint del certificado            |
| <b>data.certificados[]</b>                       | certificadoBase64 | String            | Sí | Certificado X.509 codificado en Base64 |
| <b>data.pasosProceso.paso1GeneracionClaves</b>   | estado            | String            | Sí | Estado del paso 1                      |
| <b>data.pasosProceso.paso1GeneracionClaves</b>   | solicitudPkId     | String            | Sí | ID de la solicitud PKI                 |
| <b>data.pasosProceso.paso1GeneracionClaves</b>   | fechaInicio       | String (DateTime) | Sí | Inicio del paso 1                      |
| <b>data.pasosProceso.paso1GeneracionClaves</b>   | fechaFin          | String (DateTime) | Sí | Fin del paso 1                         |
| <b>data.pasosProceso.paso1GeneracionClaves</b>   | intentos          | Integer           | Sí | Intentos del paso 1                    |
| <b>data.pasosProceso.paso2EmisionCertificado</b> | estado            | String            | Sí | Estado del paso 2                      |

|  |                      |                   |    |  |
|--|----------------------|-------------------|----|--|
| <b>data.pasosProceso.paso2EmisionCertificado</b> | fechaInicio          | String (DateTime) | Sí | Inicio del paso 2                      |
| <b>data.pasosProceso.paso2EmisionCertificado</b> | fechaFin             | String (DateTime) | Sí | Fin del paso 2                         |
| <b>data.pasosProceso.paso2EmisionCertificado</b> | intentos             | Integer           | Sí | Intentos del paso 2                    |
| <b>data.auditoria</b>                            | registroAuditorialId | String            | Sí | ID del registro de auditoría           |
| <b>data.auditoria</b>                            | usuarioEjecutor      | String            | Sí | Usuario que ejecutó la operación       |
| <b>data.auditoria</b>                            | oficinaEjecucion     | String            | Sí | Oficina donde se ejecutó               |
| <b>data.auditoria</b>                            | ipCliente            | String            | No | IP del cliente                         |
| <b>metadata</b>                                  | timestamp            | String (DateTime) | Sí | Timestamp del procesamiento            |
| <b>metadata</b>                                  | correlationId        | String (UUID)     | Sí | ID de correlación                      |
| <b>metadata</b>                                  | version              | String            | Sí | Versión del API                        |
| <b>metadata</b>                                  | tiempoRespuesta      | String            | Sí | Tiempo total de respuesta              |
| <b>error</b>                                     | –                    | Object            | No | Objeto que detalla el error si ocurrió |
| <b>error.tipo</b>                                | tipo                 | String            | No | Tipo de error                          |
| <b>error.titulo</b>                              | titulo               | String            | No | Título o mensaje principal del error   |
| <b>error.estado</b>                              | estado               | Integer           | No | Código de estado del error             |
| <b>error.errores[]</b>                           | –                    | Array             | No | Lista de errores detallados            |
| <b>error.errores[].detalleError</b>              | detalleError         | String            | No | Mensaje específico del error           |

### 3.1.1.3 Valores para el atributo statusCode

| Código     | Respuesta    | Descripción  |
|------------|--------------|--|
| <b>200</b> | OK           | Certificados obtenidos exitosamente (cuando ya existían) |
| <b>201</b> | Created      | Certificados emitidos exitosamente                       |
| <b>400</b> | Bad Request  | Parámetros de entrada inválidos o incompletos            |
| <b>401</b> | Unauthorized | Token JWT inválido, expirado o ausente                   |
| <b>403</b> | Forbidden    | Usuario sin permisos para solicitar certificados         |
| <b>404</b> | Not Found    | Ciudadano no encontrado en el sistema                    |

|            |                       |  |
|------------|-----------------------|--|
| <b>409</b> | Conflict              | Ya existe una solicitud de certificados en proceso para este ciudadano |
| <b>422</b> | Unprocessable Entity  | Datos válidos pero ciudadano no cumple requisitos para certificados    |
| <b>429</b> | Too Many Requests     | Límite de rate limit excedido  |
| <b>500</b> | Internal Server Error | Error interno del microservicio  |
| <b>502</b> | Bad Gateway           | Error de comunicación con MsAdaptadorPKI                               |
| <b>503</b> | Service Unavailable   | Servicio PKI temporalmente no disponible                               |
| <b>504</b> | Gateway Timeout       | Timeout en comunicación con servicio PKI                               |