



Microservicio MsDominioProteccionDocumentos

Documento Versión: 1.0

Gestión de Seguridad Electrónica



Fecha generación: **01/12/2025**

CONTROL DE VERSIÓN

VERSIÓN	FECHA DE ACTUALIZACIÓN	CARGO	DESCRIPCIÓN
1.0	24/11/2025	Arquitecto de Software	Versión inicial del documento

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 MsDominioProteccionDocumentos	5
3.1.1	Endpoint: Comprimir y Proteger Documento	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 MsDominioProteccionDocumentos

El Microservicio Protección Documentos es un componente de soporte y utilidad dentro de la plataforma SIIRC, esencial para la seguridad y el manejo eficiente de archivos. Su propósito principal es implementar la política de seguridad de distribución documental, encargándose de comprimir los documentos sensibles y generar y asignar una contraseña al archivo comprimido resultante. Esto asegura que cualquier documento creado pueda ser protegido con clave de acceso al momento de su distribución, conforme a la configuración del sistema.

3.1.1 Endpoint: Comprimir y Proteger Documento

Endpoint que permite comprimir un documento PDF firmado digitalmente y protegerlo con una contraseña generada criptográficamente

Atributo	Valor
Path	/api/v1/documentos/MsProteccionDocumentos/comprimir-proteger
API Gateway	Interno
Método HTTP	POST
Protocolo	REST/HTTP
Headers	Authorization String (Bearer token JWT para autenticación del usuario) Content-Type String ("application/json") X-Correlation-ID UUID (Identificador único de correlación para trazabilidad end-to-end) X-Office-Code String (Código de oficina o sede desde donde se realiza la operación) X-User-Role String (Rol del usuario que realiza la operación) X-Request-Source String (Origen de la solicitud: WEB, MOBILE, KIOSK, API_EXTERNA) X-Idempotency-Key UUID (Clave para evitar operaciones duplicadas)
Entrada	{ "solicitudId": "string", "tipoDocumento": "string", "nombreArchivo": "string", "fuentesDocumento": { "tipo": "string", "contenidoBase64": "string",

	<pre> "referenciaRepositorio": { "repositorioId": "string", "documentoId": "string", "versionId": "string" }, "metadatos": { "tipoTramite": "string", "numeroSolicitud": "string", "dniSolicitante": "string", "fechaGeneracion": "YYYY-MM-DDThh:mm:ssZ" }, "configuracionProteccion": { "usarConfiguracionPorDefecto": "boolean", "algoritmoCompresion": "string", "nivelCompresion": "string" }, "destinatario": { "email": "string", "telefono": "string", "nombreCompleto": "string" } } </pre>
Respuesta	<pre> { "success": "boolean", "data": { "proteccionId": "string", "solicitudId": "string", "archivoProtegido": { "repositorioId": "string", "documentoId": "string", "nombreArchivo": "string", "tamanioBytes": "integer", "formatoSalida": "string", "checksumSHA256": "string" }, "seguridad": { "passwordHashSHA512": "string", "algoritmoUtilizado": "string", "longitudPassword": "integer", "fechaGeneracion": "YYYY-MM-DDThh:mm:ssZ", "fechaExpiracion": "YYYY-MM-DDThh:mm:ssZ" }, "compresion": { "algoritmo": "string", "nivelCompresion": "string", "tamanioOriginal": "integer", "tamanioComprimido": "integer", "ratioCompresion": "number" }, "estado": "string", "fechaProcesamiento": "YYYY-MM-DDThh:mm:ssZ", "_links": { "self": "string", "descargar": "string", "verificar": "string" } }, "metadata": { "timestamp": "YYYY-MM-DDThh:mm:ssZ", "correlationId": "string", "version": "string", "tiempoRespuesta": "string" } } </pre>

Error Response	<pre> } "error": { "tipo": "string", "titulo": "string", "estado": "integer", "errores": [{ "detalleError": "string" }] } </pre>
----------------	--

3.1.1.1 Parámetros por Entrada

Dato	Atributo	Tipo	Obligatorio	Longitud Mínima	Longitud Máxima
ID de Solicitud	solicitudId	String	Sí	36	36
Tipo de Documento	tipoDocumento	String	Sí	3	50
Nombre del Archivo	nombreArchivo	String	Sí	5	200
Fuente del Documento	fuenteDocumento	Object	Sí	NA	NA
Tipo de Fuente	fuenteDocumento.tipo	String	Sí	5	20
Contenido Base64	fuenteDocumento.contenidoBase64	String	Condicional	1	NA
Referencia Repositorio	fuenteDocumento.referenciaRepositorio	Object	Condicional	NA	NA
ID Repositorio	fuenteDocumento.referenciaRepositorio.repositorioId	String	Condicional	3	50
ID Documento	fuenteDocumento.referenciaRepositorio.documentId	String	Condicional	36	36
ID Versión	fuenteDocumento.referenciaRepositorio.versionId	String	No	1	20
Metadatos	metadatos	Object	Sí	NA	NA
Tipo de Trámite	metadatos.tipoTramite	String	Sí	3	50
Número de Solicitud	metadatos.numeroSolicitud	String	Sí	5	30
DNI Solicitante	metadatos.dniSolicitante	String	Sí	8	8
Fecha Generación	metadatos.fechaGeneracion	String (Date ISO 8601)	Sí	NA	NA

Configuración Protección	configuracionProteccion	Object	No	NA	NA
Usar Config. Por Defecto	configuracionProteccion.usarConfiguracionPorDefecto	Boolean	No	NA	NA
Algoritmo Compresión	configuracionProteccion.algoritmoCompresion	String	No	3	20
Nivel Compresión	configuracionProteccion.nivelCompresion	String	No	4	10
Destinatario	destinatario	Object	No	NA	NA
Email Destinatario	destinatario.email	String	No	5	254
Teléfono Destinatario	destinatario.telefono	String	No	7	15
Nombre Completo	destinatario.nombreCompleto	String	No	3	200

3.1.1.2 Parámetros de Respuesta

Nombre	Tipo	Obligatorio	Descripción
success	Boolean	Sí	Indica si la operación fue exitosa
data	Object	Sí	Cuerpo principal de la respuesta
data.proteccionId	String	Sí	UUID único de la operación de protección
data.solicitudId	String	Sí	ID de la solicitud procesada
data.archivoProtegido	Object	Sí	Información del archivo protegido generado
data.archivoProtegido.repositorioId	String	Sí	ID del repositorio donde se almacenó
data.archivoProtegido.documentoId	String	Sí	ID del documento en el repositorio
data.archivoProtegido.nombreArchivo	String	Sí	Nombre del archivo ZIP generado
data.archivoProtegido.tamanoBytes	Integer	Sí	Tamaño del archivo protegido en bytes
data.archivoProtegido.formatoSalida	String	Sí	Formato del archivo (ZIP)
data.archivoProtegido.checksumSHA256	String	Sí	Hash SHA-256 del archivo para verificación
data.seguridad	Object	Sí	Información de seguridad aplicada
data.seguridad.passwordHashSHA512	String	Sí	Hash SHA-512 de la contraseña generada

data.seguridad.algoritmoUtilizado	String	Sí	Algoritmo de cifrado aplicado
data.seguridad.longitudPassword	Integer	Sí	Longitud de la contraseña generada (16 caracteres)
data.seguridad.fechaGeneracion	String (Date ISO 8601)	Sí	Fecha de generación de la contraseña
data.seguridad.fechaExpiracion	String (Date ISO 8601)	No	Fecha de expiración de la contraseña
data.compresion	Object	Sí	Estadísticas de compresión
data.compresion.algoritmo	String	Sí	Algoritmo de compresión usado
data.compresion.nivelCompresion	String	Sí	Nivel de compresión aplicado
data.compresion.tamanoOriginal	Integer	Sí	Tamaño original del documento en bytes
data.compresion.tamanoComprimido	Integer	Sí	Tamaño después de comprimir en bytes
data.compresion.ratioCompresion	Number	Sí	Ratio de compresión logrado
data.estado	String	Sí	Estado del proceso (COMPLETADO, ERROR)
data.fechaProcesamiento	String (Date ISO 8601)	Sí	Fecha y hora del procesamiento
data._links	Object	Sí	Enlaces HATEOAS relacionados
data._links.self	String	Sí	URL del recurso actual
data._links.descargar	String	Sí	URL para descargar el archivo
data._links.verificar	String	Sí	URL para verificar integridad
metadata	Object	Sí	Metadatos de la respuesta
metadata.timestamp	String (Date ISO 8601)	Sí	Marca de tiempo del procesamiento
metadata.correlationId	String	Sí	Identificador de correlación para trazabilidad
metadata.version	String	Sí	Versión del servicio
metadata.tiempoRespuesta	String	Sí	Tiempo total de respuesta
error	Object	No	Objeto que especifica algún error existente
error.tipo	String	No	Tipo de error
error.titulo	String	No	Título del error
error.estado	Integer	No	Código del estado de error
error.errores	Array	No	Listado de errores
error.errores[].detalleError	String	No	Detalle del error generado

3.1.1.3 Valores para el Atributo de statusCode

Código	Respuesta	Descripción
201	Created	Documento comprimido y protegido exitosamente
400	Bad Request	Datos inválidos o formato de documento incorrecto
401	Unauthorized	Token JWT inválido o expirado
403	Forbidden	Usuario sin permisos para proteger documentos
404	Not Found	Documento de origen no encontrado en repositorio
409	Conflict	El documento ya fue protegido anteriormente
413	Payload Too Large	El documento excede el tamaño máximo permitido
422	Unprocessable Entity	Documento válido pero no procesable (ej: no es PDF, no está firmado)
429	Too Many Requests	Límite de rate limit excedido
500	Internal Server Error	Error interno del servidor
502	Bad Gateway	Error de comunicación con MsDatosConfiguracion o MsGestorDocumentos
503	Service Unavailable	Servicio temporalmente no disponible