ANÁLISIS FUNCIONAL NUEVA API REST

P3.A1.R1.EC3

Manual de integración API REST

Financiado por la Unión Europea
NextGenerationEU
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
IGAE
INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO
OFICINA DE INFORMÁTICA PRESUPUESTARIA

CONTROL DE VERSIONES

Versión	Apartado	Descripción	Fecha	Elaborado	Revisado
1.0		Generación del documento	12/11/2024	AYESA	OIP
1.1	2.1 Operaciones internas	Se eliminan las referencias a operaciones internas de la API.	11/03/2025	AYESA	OIP
1.1	2. Listado de operaciones	Se incluye enlace al Portal Web para consultar información más detallada de las operaciones.	11/03/2025	AYESA	OIP
1.1	3.1 Ejemplo de consumo de las operaciones de la API	Se recogen los pasos que ha de realizar un integrador externo para hacer uso de la API mediante API Key. Se eliminan los pasos que ha de realizar un integrador externo para hacer uso de la API mediante API Key.	08/04/2025	AYESA	OIP
1.1	5. Solicitud de acceso	Se reestructuran los apartados y se incluyen detalles sobre cómo los integradores y usuarios externos deben solicitar el acceso al API REST SOROLLA2 para su consumo.	11/03/2025	AYESA	OIP
1.1	Todos	Las referencias al proyecto eProcurement se sustituyen por sistema API REST SOROLLA2.	11/03/2025	AYESA	OIP
1.2	Todos	Se referencia a la API REST SOROLLA2 siempre en femenino. Se referencia SOROLLA2 siempre en mayúsculas y con la versión. Se sustituyen los tiempos verbales futuros por presentes. Se reorganizan los apartados según las indicaciones. Se incluye la información indicada y se elimina la información incorrecta o innecesaria.	22/05/2025	AYESA	
1.3	4. Solicitud de acceso	Se incorpora la información facilitada por la OIP.	02/10/2025	AYESA	
1.4	2.1. Ejemplos de consumo de las operaciones	Se actualiza la información de uso del cliente Feign a raíz de las pruebas realizadas con el cliente eProc.	27/11/2025	AYESA	
1.5	Todos	Corrección de errores	19/12/2025	OIP	OIP

INDICE

1. INTRODUCCIÓN AL API REST 4

2. FUNCIONALIDAD OFRECIDA POR LA API REST SOROLLA2 4

2.1. EJEMPLOS DE CONSUMO DE LAS OPERACIONES: 9
2.1.1. Mediante Curl 9
2.1.2. Mediante Swagger 10
2.1.3. Mediante Cliente Feign 12
2.1.4. Requisito para el uso del cliente Feign 13
2.1.5. Ejemplo de interceptor de cliente Feign con API Key 13
2.1.6. Ejemplo de interfaz de cliente Feign 14
2.1.7. Ejemplo de invocación a una operación del cliente Feign 14
2.1.8. Ejemplo de tests usando el cliente Feign 15

3. SEGURIDAD 15

3.1. MODALIDAD DE USO DE SSL SOBRE HTTP 15
3.2. OBTENCIÓN Y USO DE TOKENS JWT 16
3.3. OBTENCIÓN Y USO DE API KEYS 16

4. SOLICITUD DE ACCESO 17

4.1. PRIMER CONTACTO CON EL EQUIPO DE SOROLLA2. 18
4.2. SOLICITUD DE ACCESO VÍA RADIX SERVICIOS WEB. 18
4.3. CONFIRMACIÓN DE LA AUTORIZACIÓN DE ACCESO. 21
4.4. CONFIGURACIÓN PRELIMINAR DE LA INTEGRACIÓN. 21

1. Introducción al API REST

La implantación de una nueva Interfaz de programación de aplicaciones REST (API REST Sorolla2) se justifica en cumplimiento de la legislación vigente, y para responder a las necesidades detectadas por la Intervención General de la Administración del Estado, en adelante IGAE, y por los centros adheridos referentes a:

- Impulsar la interoperabilidad con otros sistemas y soluciones de tramitación, según el art. 3.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Reforzar los servicios de interoperabilidad que ya ofrece actualmente SOROLLA2, a través de una renovación tecnológica de los mismos y una ampliación de su alcance, que permitan una respuesta adecuada a las demandas planteadas por los centros adheridos.
- Exponer los negocios más relevantes del núcleo de la aplicación, sentando así las bases para una renovación tecnológica del sistema en su conjunto a futuro.

Este Interfaz de programación de aplicaciones REST *(Transferencia de estado representacional*) expone una capa de servicios que proporciona acceso a las principales funcionalidades y procesos de negocio que soporta SOROLLA2, facilitando la reutilización de información recabada ya en el sistema, evitando duplicidades de trabajos y esfuerzos y aumentando la productividad y la eficiencia en todas las fases de la gestión Económico - Presupuestaria en el entorno de la IGAE y, adicionalmente, ofrece nuevas operaciones que cubren las funcionalidades requeridas en el ámbito del sistema API REST Sorolla2, proporcionando las bases tecnológicas para añadir funcionalidades futuras.

Para la implementación de esta nueva API REST se han tenido en cuenta las siguientes consideraciones:

- Aplicación de buenas prácticas para un diseño claro y organizado, incluyendo la definición de recursos y endpoints de manera lógica, un sistema de versionado y una documentación detallada para facilitar su uso.
- Comunicación con aplicaciones externas de forma segura a través de unos mecanismos de autenticación basados en certificados, tokens JWT y API Keys, y uso de HTTPS para el cifrado de la información.
- Optimización de la eficiencia con el empleo de técnicas como el cacheo, la compresión de datos y la paginación para grandes volúmenes de datos.
- Respuestas consistentes en formato estándar JSON y mensajes de error claros y detallados para facilitar la comprensión y la depuración, mejorando así la experiencia del desarrollador.
- Pruebas consistentes unitarias y de integración, así como la monitorización con registro de errores para el mantenimiento de la calidad y la detección de problemas.
- Escalabilidad orientada al crecimiento y basada en una arquitectura flexible independiente del interfaz de usuario capaz de adaptarse a nuevas demandas.

NOTA: Es responsabilidad del cliente o consumidor de la API de servicios la adaptación de sus aplicaciones o soluciones informáticas para llevar a cabo la integración con la API REST SOROLLA2. Queda fuera del alcance de IGAE, cualquier desarrollo o adaptación en la parte cliente.

2. Funcionalidad ofrecida por la API REST SOROLLA2

La API REST SOROLLA2 se expone como un conjunto de servicios REST a los clientes a través de la red SARA y proporciona un interfaz JSON para el intercambio de datos. Los clientes pueden enviar solicitudes HTTPs a dichos servicios (previa obtención de credenciales de acceso), cumpliendo las especificaciones técnicas que en este documento se detallan en materia de seguridad y protocolos de comunicación.

Las operaciones serán de carácter público, orientadas a la comunicación entre los sistemas externos y la API REST SOROLLA2.

El detalle ampliado del conjunto de las operaciones ofrecidas por la API REST SOROLLA2 puede ser consultado en las fichas de los recursos correspondientes, disponibles en el apartado *Fichas de recursos* del portal de la API REST SOROLLA2.

Las operaciones estarán agrupadas en un conjunto de recursos definidos en la API REST SOROLLA2. Los principales recursos y el sentido de las operaciones permitidas en cada caso son las siguientes:

- **EXPEDIENTES**:
    - Permite la operación POST de expedientes teniendo en cuenta los datos mínimos obligatorios. Y adicionalmente se permite el alta de documentos, contratos, pagos y justificantes asociados a un expediente.
    - Permite las operaciones GET de expedientes:
        - Del conjunto total de expedientes acotando el resultado por el órgano gestor y la unidad tramitadora del sistema externo conectado.
        - De un conjunto de expedientes mediante criterios de búsqueda (incluyendo el identificador del expediente en Sorolla2, distinto del UUID usado en el API REST SOROLLA2).
        - De un expediente a través de su identificador universal único.
        - También se permite la consulta de documentos, documentos contables, documentos no contables, licitación, adjudicación, contratos, pagos y justificantes asociados a un expediente.

      Entre la información consultada se muestran los datos generales, los datos administrativos, los datos económicos y los datos presupuestarios del expediente, así como el listado de sus contratos asociados, los datos de proyecto de gasto, las asignaciones, la licitación, la adjudicación y los documentos contables y no contables.
    - Permite la operación PUT de expedientes sobre el recurso completo, de modo que habrá que informar todos los campos existentes para su actualización.
    - Permite la operación DELETE de expedientes:
        - Para dar de baja un documento.
        - Para dar de baja un contrato asociado.
        - Para dar de baja una asignación asociada.
        - Para dar de baja un pago asociado a un contrato.
        - Para dar de baja un justificante asociado a un pago.

- **JUSTIFICANTES**:
    - Permite la operación POST de justificantes incluyendo los datos generales y las líneas justificativas. Y adicionalmente se permite el alta de documentos e imputaciones asociados a un justificante.
    - Permite las operaciones GET de justificantes:
        - Del conjunto total de justificantes acotando el resultado por el órgano gestor y la unidad tramitadora del sistema externo conectado.
        - De un conjunto de justificantes mediante criterios de búsqueda.
        - De un justificante a través de su identificador universal único.
        - También se permite la consulta de documentos e imputaciones asociados a un justificante.

Entre la información consultada se muestran los datos generales y las líneas justificativas, así como la imputación y el contrato de caja asociados al justificante.

- Permite la operación PUT de justificantes sobre el recurso completo, de modo que habrá que informar todos los campos existentes para su actualización.
- Permite la operación DELETE de justificantes:
  - Para dar de baja un justificante.
  - Para dar de baja un contrato de caja asociado.

- **TERCEROS**:
  - Permite la operación POST de terceros informando los datos generales, las cuentas, las direcciones y los datos de personal.
  - Permite la operación GET de terceros:
    - De todos los terceros acotando el resultado por el órgano gestor y la unidad tramitadora del sistema externo conectado.
    - De un conjunto de terceros mediante criterios de búsqueda.
    - De un tercero a través de su identificador universal único.

    Entre la información consultada se muestran los datos generales, las cuentas, las direcciones y los datos de personal.
  - Permite la operación PUT de terceros sobre el recurso completo, de modo que habrá que informar todos los campos existentes para su actualización.
  - Permite la operación DELETE de terceros:
    - Para dar de baja un tercero.

- **CONTRATOS DE CAJA**:
  - Permite la operación POST de contratos de caja informando los datos generales y los contratos unidad. Y adicionalmente se permite el alta de documentos y justificantes asociados a un contrato de caja.
  - Permite la operación GET de contratos de caja:
    - De todos los contratos de caja acotando el resultado por el órgano gestor y la unidad tramitadora del sistema externo conectado.
    - De un conjunto de contratos de caja mediante criterios de búsqueda.
    - De un contrato de caja a través de su identificador universal único.
    - También se permite la consulta de documentos, contratos unidades y registros históricos asociados a un contrato de caja.

    Entre la información consultada se muestran los datos generales y los contratos unidad, así como los justificantes asociados al contrato de caja. Se permitirá la operación de baja un justificante y de un contrato de caja asociado a un justificante.
  - Permite la operación PUT de contratos de caja sobre el recurso completo, de modo que habrá que informar todos los campos existentes para su actualización.
  - Permite la operación DELETE de contratos de caja:
    - Para dar de baja un contrato de caja.
    - Para dar de baja un documento asociado.
    - Para dar de baja un justificante asociado.

- **DOCUMENTOS**:
  - Permite la operación GET de documentos:
    - De todos los documentos acotando el resultado por el órgano gestor y la unidad tramitadora del sistema externo conectado.
    - De un conjunto de documentos mediante criterios de búsqueda.
    - De un documento a través de su identificador universal único.
    - También se permite la consulta de versiones y etiquetas asociadas a un documento.

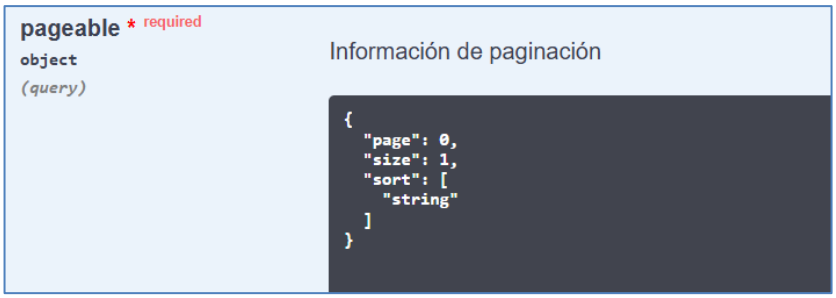
    Entre la información consultada se muestran los datos generales y el documento en formato base 64 obtenido del gestor documental, así como las distintas versiones asociadas al documento.

- **CATÁLOGOS**:
  - Permite la operación GET de los diversos catálogos (información disponible en el sistema almacenada en tablas tipo):
    - De todos los tipos de un catálogo concreto, acotando el resultado en algunos casos por el órgano gestor y la unidad tramitadora del sistema externo conectado.
    - De un conjunto de tipos de un catálogo concreto mediante criterios de búsqueda.
    - De un tipo específico a través de su identificador universal único.

    Entre la información consultada se muestran el tipo y la descripción.

Entre las distintas utilidades generales ofrecidas por las operaciones del API REST SOROLLA2 se destacan las siguientes:

- **Paginación**: si la operación lo permite, se puede acotar y ordenar el resultado de las operaciones GET mediante el uso de los parámetros identificados en el objeto *pageable* de la solicitud:
  - page (opcional): Número de página del resultado.
  - size (opcional): Número de registros por página.
  - sort (opcional): Listado de campos y su ordenación (ASC por defecto).

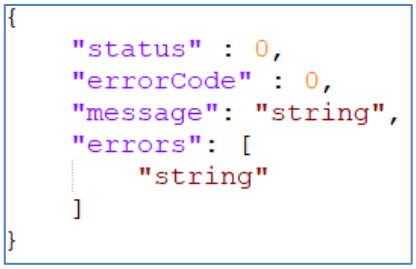


1. Ilustración del objeto paginación en swagger.

- **Catálogo de errores**: cuando una operación no se puede completar con éxito, debido a errores de validación o a errores propios del sistema, se producirá la siguiente respuesta:

Respuesta error	Valor
status	Código HTPP de la respuesta de error.
errorCode	Código del error correspondiente.
message	Descripción del mensaje de error devuelto por la operación.

errors[]	Listado de descripciones de error devueltos por el sistema.



2. *Ilustración del JSON de respuesta de error.*

- **Criterios de búsqueda**: si la operación GET lo permite, se puede acotar el resultado mediante el uso de los criterios de búsqueda definidos para la operación e identificados en el objeto *criteria* de la solicitud:

3. *Ilustración del objeto criteria en swagger.*

Los estados HTTP del resultado de las operaciones se resumen en la siguiente tabla:

Estado (Código HTTP)	Significado
200	Operación Exitosa/Objeto de respuesta actualizado
201	Recurso creado satisfactoriamente
204	Recurso borrado físicamente (Respuesta sin contenido)
400	Error en la petición
401	Error autenticación
403	Acceso prohibido (autenticación necesaria)
404	Recurso no encontrado
405	Operación no permitida
413	Contenido demasiado grande
500	Error inesperado. Contacte con el administrador
501	El método no está implementado

2.1. Ejemplos de consumo de las operaciones:

Se incluyen, en los siguientes subapartados, ejemplos de consumo de las operaciones de la API REST SOROLLA2 a través de distintas tecnologías.

2.1.1. Mediante Curl

Para ejecutar una operación mediante Curl es necesario que:

1. El proveedor de la API gestione la creación de una API Key asociada a uno o varios órganos gestores.
2. El proveedor de la API facilite la API Key al cliente externo. Las API Key empleadas son estables, no obstante, en caso de que se produzca una renovación de estas, se avisará a los clientes afectados con la debida antelación.
3. El cliente externo obtendrá una autorización (token JWT) a través del servicio de generación de tokens proporcionado por el proveedor de la API. La obtención de esta autorización en el entorno de pre-producción está disponible en la dirección: https://serpubpre.igae.hacienda.gob.es/auth/realms/Iden_aplicaciones_X509/protocol/openid-connect/token
4. El cliente externo configurará la autorización (Bearer + token JWT) y la API Key para utilizarlas en cada llamada al API Manager que invocará a las operaciones protegidas publicadas en la API previa validación del token proporcionado.

   Curl

   curl -X 'GET' \

   https://serpubpre.igae.hacienda.gob.es/sorolla/api/v1/organos-gestores?page=0&size=10' \

   -H 'accept: application/json' \

   -H '**authorization**: Bearer
   eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJRdDFETzQzMkNzNWZmMmZfblZJc2NMZGMyOTZoRFY3NnlVV1p0UlYySGZjIn0.eyJleHAiOjE3NDk4MDEwNTksImlhdCI6MTc0OTc5OTI1OSwianRpIjoiNTA5ZTI5OGUtODkyYy00MWNkLWJiMGEtNDM5YzhjM2NhYmMyIiwiaXNzIjoiaHR0cHM6Ly9tb2xhci5pZ2FlLmhhY2llbmRhLmdvYi5lcy9hdXRoL3JlYWxtcy9JZGVuX2FwbGljYWNpb25lc19YNTA5Iiwic3ViIjoiNzBjNzViZTgtY2M2NS00MjdkLWFkYTQtNGM1OTMxNTljNzhiIiwidHlwIjoiQmVhcmVyIiwiYXpwIjoiVUVQUk9DVVJFRUEwMDQ2Mzg5IiwiYWNyIjoiMSIsImNuZiI6eyJ4NXQjUzI1NiI6Ild6dkVzY1o5SktPTm1JWUpQYmdxOUFSa3JqdWFJS1Z5M0lRNWVtWGJDWUEifSwic2NvcGUiOiJFUFJPQ1VSRSIsImNsaWVudEhvc3QiOiIxOC4xMDAuMjEuNzIiLCJjbGllbnRBZGRyZXNzIjoiMTguMTAwLjIxLjcyIiwiY2xpZW50X2lkIjoiVUVQUk9DVVJFRUEwMDQ2Mzg5In0.ozdJle-yuM3yGcL1Np2kmlmjgflJHKe_7P09RUNIgyJMfmkBYMF1AEObP-OO9kT5EsAXBPfknq0SdU7rXhlyhHp1Ve3PlSiReuHUeACVAmrMM9_fDL2kRo7QjCo5H6EgrijyWyZd8F1F8oMZ9-3SMrtH38Nc9DHUD03HWFEdJNyD1pieZFLPIfwlWYs2_I0x8Jxu1HusSRN7tCqdy3luPfoG90NftdBGSGjo7jaHeQ3vGYTd-BAmRhkC-KIgjj3ZjQqXKitVi-A8RZXLu_SQz0S3YWKfJqYAVYFQ-1NANeuwIfp3DNACKEys6bKVRM7iWOvKJ6CwV7hZbTb0jkaIDQ' \

   -H ' **x-apikey**: c5ebedca-4580-408a-ae84-3f00a7c00b42'

   Request URL

   https://serpubpre.igae.hacienda.gob.es/sorolla/api/v1/organos-gestores?page=0&size=10

   Server response (200 OK)

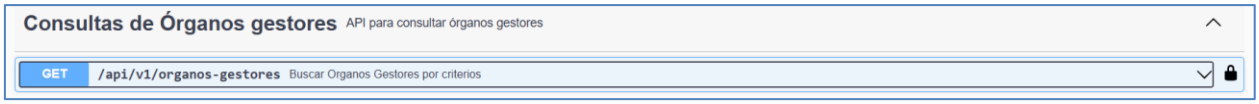
   [

```
{
   "id": "557e2d88-117d-43a8-b5a7-f55647b7fabe",
   "codigo": "10000001",
   "descripcion": "SUBSECRETARÍA DE HACIENDA",
   "descripcionOriginal": "SUBSECRETARÍA DE HACIENDA"
},
{
   "id": "5cf61cda-c822-4155-bf2a-eaa2c79bff4b",
   "codigo": "10000002",
   "descripcion": "INSTITUTO DE LA JUVENTUD",
   "descripcionOriginal": "INSTITUTO DE LA JUVENTUD"
},
{
   "id": "faf04659-00c4-4621-8782-ca09789b7f05",
   "codigo": "10000003",
   "descripcion": "COMISIONADO PARA EL MERCADO DE TABACOS",
   "descripcionOriginal": "COMISIONADO PARA EL MERCADO DE TABACOS"
},
[…]
]
```


2.1.2. Mediante Swagger

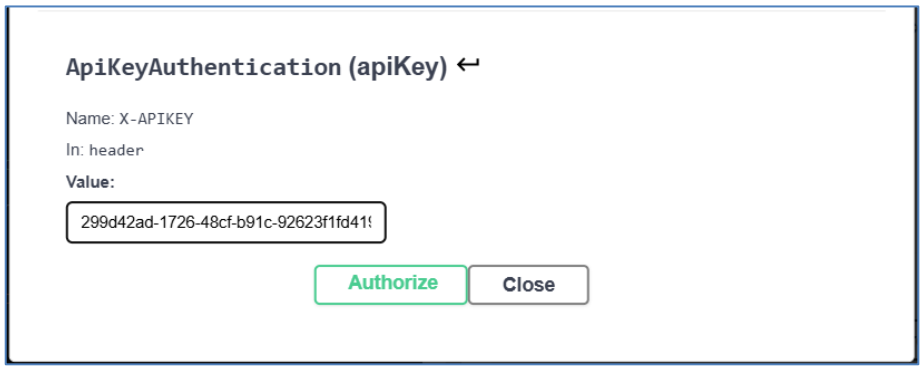
Para ejecutar una operación mediante Swagger es necesario que:

1. El proveedor de la API gestione la creación de una API Key asociada a uno o varios órganos gestores.
2. El proveedor de la API facilite la API Key al cliente externo. Las API Key empleadas son estables, no obstante, en caso de que se produzca una renovación de estas, se avisará a los clientes afectados con la debida antelación.
3. El cliente externo acceda a la operación que desea ejecutar:



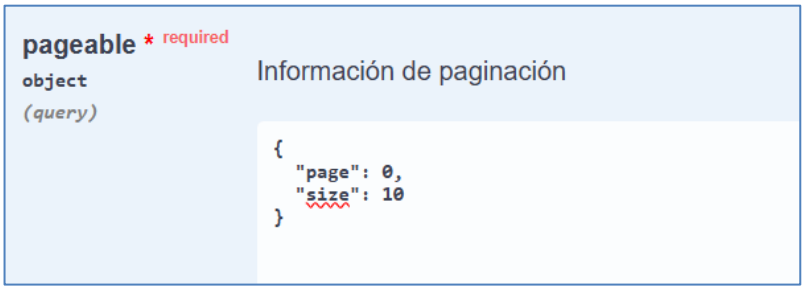
1. *Ilustración de la operación de consulta de Órganos gestores en Swagger.*

4. El cliente externo proceda a autorizarse, haciendo clic en el icono del candado junto a la operación correspondiente e informando la API Key proporcionada por el proveedor de la API:



2. *Ilustración de la autorización mediante ApiKeyAuthentication en swagger.*

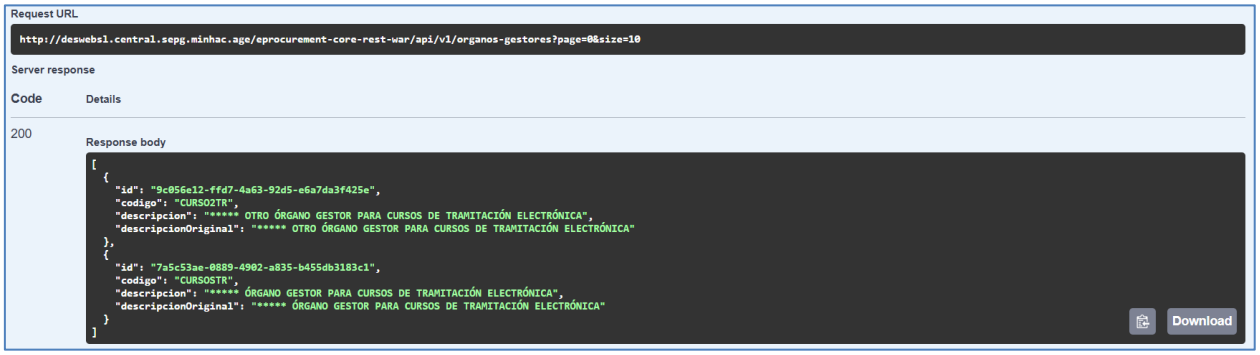
5. El cliente externo informa los parámetros de consulta deseados:



3. *Ilustración de los parámetros de la operación de consulta de Órganos gestores en swagger.*

6. En cada solicitud, el servidor desencripta el API Key y comprueba si el cliente tiene permisos para acceder a la operación:

   a. Si el cliente está autorizado, dispone de permiso y la operación se ejecuta correctamente, el resultado de la consulta será el siguiente:

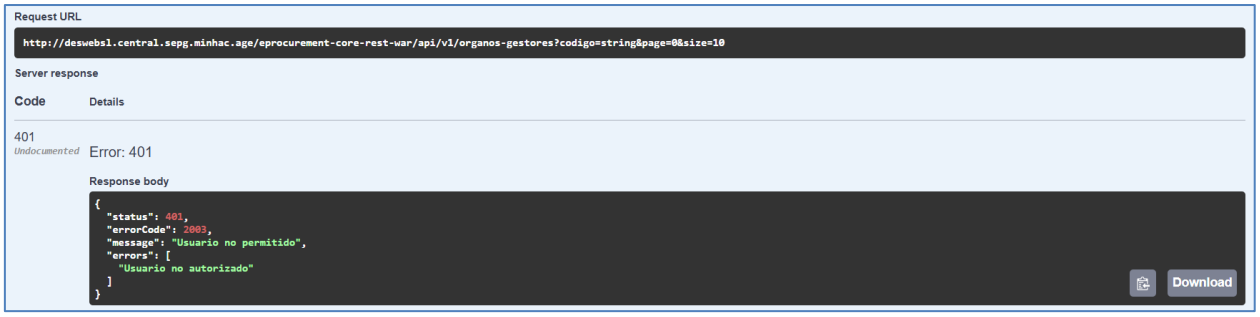


4. *Ilustración de respuesta HTTP 200 a la operación de consulta de Órganos gestores en swagger.*

   b. Si el cliente no está autorizado, el resultado de la consulta será el siguiente:

5. Ilustración de respuesta HTTP 403 a la operación de consulta de Órganos gestores en swagger.

c. Si el cliente está autorizado y no dispone de permiso para ejecutar la operación, el resultado de la consulta será el siguiente:



6. Ilustración de respuesta HTTP 401 a la operación de consulta de Órganos gestores en swagger.

d. Si la operación no se ejecuta correctamente, el resultado de la consulta será el siguiente:

7. Ilustración de respuesta HTTP 404 a la operación de consulta de Órganos gestores en swagger.

2.1.3. Mediante Cliente Feign

Para ejecutar una operación mediante un cliente Feign es necesario lo indicado en los siguientes puntos.

2.1.4. Requisito para el uso del cliente Feign

Será necesario incluir una versión estable del cliente REST en el proyecto para implementar en código Java las llamadas a las operaciones de la API REST SOROLLA2:

```
<dependency>
        <groupId>es.gob.hacienda.oip.eprocurement.core</groupId>
        <artifactId>eprocurement-client-core-rest</artifactId>
        <version>xx.xx.xx</version>
</dependency>
```

2.1.5. Ejemplo de interceptor de cliente Feign con API Key

El interceptor del cliente Feign requerirá el valor del API Key proporcionado por el proveedor de la API REST SOROLLA2. Este identificador universal único (UUID) deberá incluirse en la variable **eprocurement.api.apiKey**

```
public class FeignHandler implements RequestInterceptor {
  @Value("${eprocurement.api.apiKey}")
  private String apikey;
  @Override
  public void apply(RequestTemplate template) {
    template.header("X-APIKEY", apikey);
  }
}
```

2.1.6. Ejemplo de interfaz de cliente Feign

En el cliente Feign se exponen, mediante interfaz, el conjunto de operaciones disponibles en la API REST SOROLLA2:

```
@FeignClient(name = "terceros", url = "${eprocurement.api.rest}", path = "/api/v1/terceros")
public interface TerceroFeignRepository extends TerceroAPIRepository {

   @GetMapping("/{id}")
   Tercero findById(@PathVariable UUID id);

   @GetMapping("")
   List<Tercero> findByAll(Pageable page);

   @GetMapping("/findByCriteria")
   SimplePage<Tercero> findAllByCriteria(@SpringQueryMap TerceroCriteria criteria, Pageable page);

   @PostMapping("")
   Tercero altaTercero(@RequestBody Tercero request);

   @PutMapping("/{id}")
   Tercero modificacionTercero(@RequestBody Tercero tercero, @PathVariable UUID id);

   @DeleteMapping("/{id}")
   void delete(@PathVariable UUID id);
}
```

2.1.7. Ejemplo de invocación a una operación del cliente Feign

Ejemplo de la llamada a la consulta del conjunto completo de Terceros del sistema:

```
@Autowired
private TerceroService terceroService;

List<Tercero> result = terceroService.findByAll(PageRequest.of(0, 2));
```

2.1.8. Ejemplo de tests usando el cliente Feign

Ejemplo de implementación de la consulta del conjunto completo de Terceros usando el cliente Feign:

```
public class TerceroClientTest extends BaseClientTest {

    private final TerceroService terceroService;
    private static final UUID TEST_TERCERO_ID =
            UUID.fromString("19dac053-df1b-4d1a-b698-69c26576edd9");

    @Autowired
    public TerceroClientTest(TerceroService terceroService) {
        this.terceroService = terceroService;
    }

    public void testFindByAll() {
        runTest(
                "findByAll",
                () -> {
                    Pageable pageable = PageRequest.of(0, 2);
                    List<Tercero> result = terceroService.findByAll(pageable);
                });
    }
}
```

3. Seguridad

Los servicios web que ofrece la Administración Presupuestaria a clientes externos están securizados de forma que se requiere el acceso a los mismos a través de una fachada de seguridad.

El acceso a este API REST SOROLLA2, desde aplicaciones externas, se hará de manera segura, a través de un mecanismo de autenticación basada en certificados, tokens JWT y API Keys.

3.1. Modalidad de uso de SSL sobre HTTP

A nivel de capa de transporte HTTP, los clientes de la API REST SOROLLA2 se autenticarán mediante HTTPS con un certificado de sello electrónico emitido por alguno de los prestadores de servicios de certificación reconocidos por el servicio web @Firma, cuya parte pública habrá sido debidamente registrada como parte del proceso de solicitud

de acceso (ver apartado 4), y deberá ser también debidamente mantenida por el centro adherido, actualizándola siempre que resulte preciso.

3.2. Obtención y uso de tokens JWT

A continuación, se detalla el modo en que se obtienen y se utilizan los tokens JWT:

1. El cliente externo obtendrá una autorización (token JWT) a través del servicio de generación de tokens proporcionado por el proveedor de la API. La obtención de esta autorización en el entorno de pre-producción está disponible en la dirección: https://serpubpre.igae.hacienda.gob.es/auth/realms/Iden_aplicaciones_X509/protocol/openid-connect/token
2. El cliente externo configurará la autorización (Bearer + token JWT) en la cabecera de cada llamada al API Manager.
3. El API Manager validará el token JWT mediante un servicio de gestión de accesos y, si la validación es satisfactoria, redireccionará la llamada a la operación solicitada de la API REST SOROLLA2.

3.3. Obtención y uso de API Keys

A continuación, se detalla el modo en que se obtienen y se utilizan las API Key:

1. El proveedor de la API facilitará la API Key al cliente externo. Las API Key empleadas son estables y estarán asociadas a uno o varios órganos gestores, no obstante, en caso de que se produjese una renovación de estas, se avisaría a los clientes afectados con la debida antelación.
2. El cliente externo obtendrá una autorización (token JWT) a través del servicio de generación de tokens proporcionado por el proveedor de la API. La obtención de esta autorización en el entorno de pre-producción está disponible en la dirección: https://serpubpre.igae.hacienda.gob.es/auth/realms/Iden_aplicaciones_X509/protocol/openid-connect/token
3. El cliente externo configurará la autorización (Bearer + token JWT) y la API Key para utilizarlas en cada llamada al API Manager que invocará a las operaciones protegidas publicadas en la API previa validación del token proporcionado.

   Curl

   curl -X 'GET' \

   https://serpubpre.igae.hacienda.gob.es/sorolla/api/v1/organos-gestores?page=0&size=10' \

   -H 'accept: application/json' \

   -H **'authorization**: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJRdDFETzQzMkNzNWZmMmZfblZJc2NMZGMyOTZoRFY3NnlVV1p0UlYySGZjIn0.eyJleHAiOjE3NDk4MDEwNTksImlhdCI6MTc0OTc5OTI1OSwianRpIjoiNTA5ZTI5OGUtODkyYy00MWNkLWJiMGEtNDM5YzhjM2NhYmMyIiwiaXNzIjoiaHR0cHM6Ly9tb2xhci5pZ2FlLmhhY2llbmRhLmdvYi5lcy9hdXRoL3JlYWxtcy9JZGVuX2FwbGljYWNpb25lc19YNTA5Iiwic3ViIjoiNzBjNzViZTgtY2M2NS00MjdkLWFkYTQtNGM1OTMxNTljNzhiIiwidHlwIjoiQmVhcmVyIiwiYXpwIjoiVUVQUk9DVVJFRUEwMDQ2Mzg5IiwiYWNyIjoiMSIsImNuZiI6eyJ4NXQjUzI1NiI6Ild6dkVzY1o5SktPTm1JWUpQYmdxOUFSa3JqdWFJS1Z5M0lRNWVtWGJDWUEifSwic2NvcGUiOiJFUFJPQ1VSRSIsImNsaWVudEhvc3QiOiIxOC4xMDAuMjEuNzIiLCJjbGllbnRBZGRyZXNzIjoiMTguMTAwLjIxLjcyIiwiY2xpZW50X2lkIjoiVUVQUk9DVVJFRUEwMDQ2Mzg5In0.ozdJle-yuM3yGcL1Np2kmlmjgflJHKe_7P09RUNIgyJMfmkBYMF1AEObP-OO9kT5EsAXBPfknq0SdU7rXhlyhHp1Ve3PlSiReuHUeACVAmrMM9_fDL2kRo7QjCo5H6EgrijyWyZd8F1F8oM

Z9-3SMrtH38Nc9DHUD03HWFEdJNyD1pieZFLPIfwlWYs2_I0x8Jxu1HusSRN7tCqdy3luPfoG90NftdBGSGjo7jaHeQ3vGYTd-BAmRhkC-KIgjj3ZjQqXKitVi-A8RZXLu_SQz0S3YWKfJqYAVYFQ-1NANeuwIfp3DNACKEys6bKVRM7iWOvKJ6CwV7hZbTb0jkaIDQ' \

-H '**x-apikey**: c5ebedca-4580-408a-ae84-3f00a7c00b42'

Request URL

https://serpubpre.igae.hacienda.gob.es/sorolla/api/v1/organos-gestores?page=0&size=10

Server response (200 OK)


```
[
  {
    "id": "557e2d88-117d-43a8-b5a7-f55647b7fabe",
    "codigo": "10000001",
    "descripcion": "SUBSECRETARÍA DE HACIENDA",
    "descripcionOriginal": "SUBSECRETARÍA DE HACIENDA"
  },
  {
    "id": "5cf61cda-c822-4155-bf2a-eaa2c79bff4b",
    "codigo": "10000002",
    "descripcion": "INSTITUTO DE LA JUVENTUD",
    "descripcionOriginal": "INSTITUTO DE LA JUVENTUD"
  },
  {
    "id": "faf04659-00c4-4621-8782-ca09789b7f05",
    "codigo": "10000003",
    "descripcion": "COMISIONADO PARA EL MERCADO DE TABACOS",
    "descripcionOriginal": "COMISIONADO PARA EL MERCADO DE TABACOS"
  },
  […]
]
```


4. Solicitud de acceso

El siguiente apartado del manual tiene como objetivo describir los pasos que se deben llevar a cabo para comenzar la integración con la API REST de SOROLLA2. Los pasos en los que consta este proceso se resumen a continuación:

1. Primer contacto con el equipo de SOROLLA2
2. Solicitud de acceso vía RADIX Servicios Web
3. Confirmación de la autorización de acceso

4. Configuración preliminar de la integración

4.1. Primer contacto con el equipo de SOROLLA2.

Para hacer uso de la API REST SOROLLA2 es condición necesaria que el centro se encuentre adherido previamente al sistema SOROLLA2. Igualmente, será necesario contactar con el equipo responsable de SOROLLA2 antes de proceder a solicitar el acceso a la API REST SOROLLA2. Mediante esta comunicación previa se definirá el objetivo y alcance de la integración.

Si un centro se encuentra interesado en integrar sus sistemas con la API REST SOROLLA2, se recomienda, en primer lugar, constituir un equipo de proyecto de integración en el que participe tanto personal del ámbito del negocio como personal técnico. En segundo lugar, en el propio portal de la API REST SOROLLA2, las pestañas Formatos de Intercambio y Enlaces de interés, proporcionan la información necesaria para, por un lado, comprender la funcionalidad ofrecida por la API REST SOROLLA2 y, por otro lado, conocer los detalles más técnicos de los servicios ofrecidos.

4.2. Solicitud de acceso vía RADIX Servicios Web.

Una vez establecida la primera comunicación entre ambos equipos y acordada la integración, se debe realizar la solicitud formal de acceso a la API REST SOROLLA2. Para llevar a cabo esta operación, el centro solicitante, a través de la persona que designen como responsable, deberá acceder al sistema RADIX Servicios Web.

¿Cómo se accede a RADIX Servicios Web?

Para acceder a RADIX Servicios Web, en primer lugar se tiene que acceder al Catálogo de Servicios Web y buscar, en el propio catálogo, el Servicio Web denominado API REST SOROLLA2.


Inicio > Sistemas de Información > Catálogo de Servicios Web

Catálogo de Servicios Web

Se ofrece en esta página el catálogo de servicios web ofrecidos por la Secretaría de Estado de Presupuestos y Gastos y la Intervención General de la Administración del estado para facilitar la interoperabilidad con los sistemas de otras entidades y administraciones públicas.

Se puede encontrar información específica de cada de uno de los servicios pulsando sobre el nombre del mismo, en caso de que estuviera activa esta función, o de lo contrario se puede solicitar información adicional remitiendo un correo electrónico a la dirección que aparece en la página principal de esta web.

Procedimiento de solicitud de acceso de entidades externas a los servicios WEB corporativos de la Oficina de Informática Presupuestaria (pdf)

Acceda a los formularios que permiten realizar distintas operaciones (alta de uno o varios servicios en la misma solicitud, seguimiento del estado de las solicitudes anteriormente creadas, autogestión de certificados) en: Acceso de Entidades Externas a Servicios Web

Nota: se encuentra disponible una presentación de ayuda para la autogestión de certificados en el siguiente enlace: presentación de ayuda.

Para crear una solicitud para uno de los servicios web mostrados en el listado de abajo, pulse en el enlace mostrado en la columna derecha (Solicitar este servicio web).

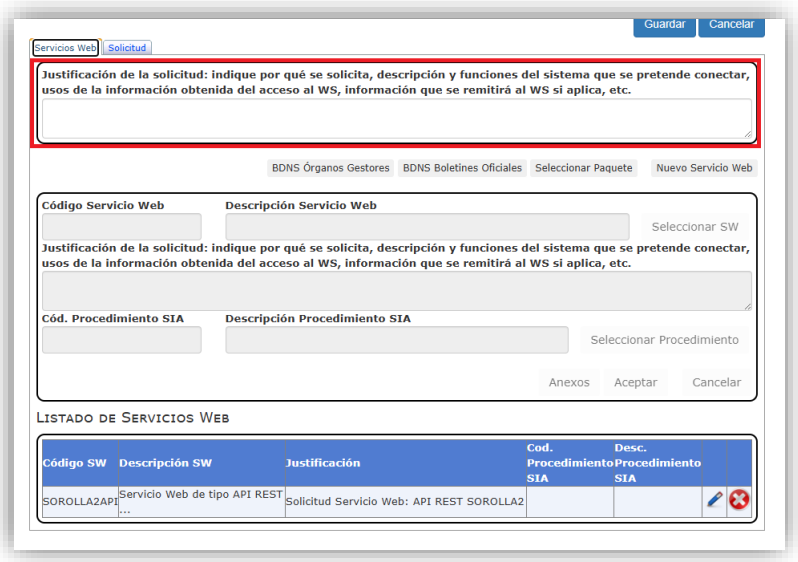
Servicio Web	Descripción del servicio	Sistema de Información asociado	Contacto	Solicitar este servicio web
API REST SOROLLA2	Servicio Web de tipo API REST que permite la integración de SOROLLA2 con otros sistemas de los centros adheridos para la consulta de información y la realización de diversas gestiones (por ej., consulta de expedientes, alta de expedientes, alta de documentos, alta de justificantes, etc.). Antes de solicitar, el responsable de negocio o del sistema a integrar deberá remitir un correo al buzón indicando entidad solicitante, sistema a conectar y objetivo de la integración, para acordar la forma de proceder.	SOROLLA 2	sorolla2@igae.hacienda.gob.es	

8. Catálogo de Servicios Web – API REST SOROLLA2

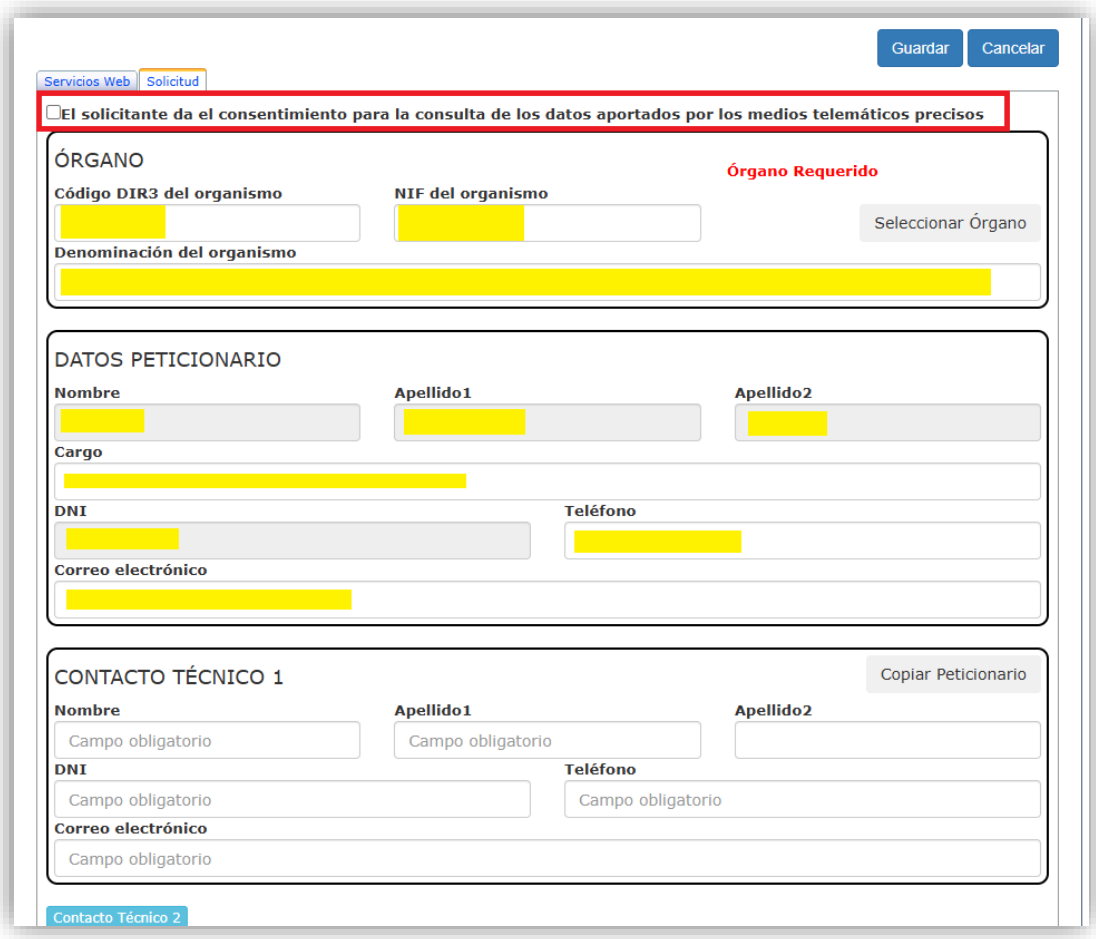
Tal y como se puede ver en la imagen anterior, la última columna denominada **Solicitar este servicio web**. En esta columna, aparece el botón *Solicitar*, el cual conecta con la aplicación RADIX Servicios Web. Para acceder a esta aplicación será necesario utilizar un certificado electrónico.

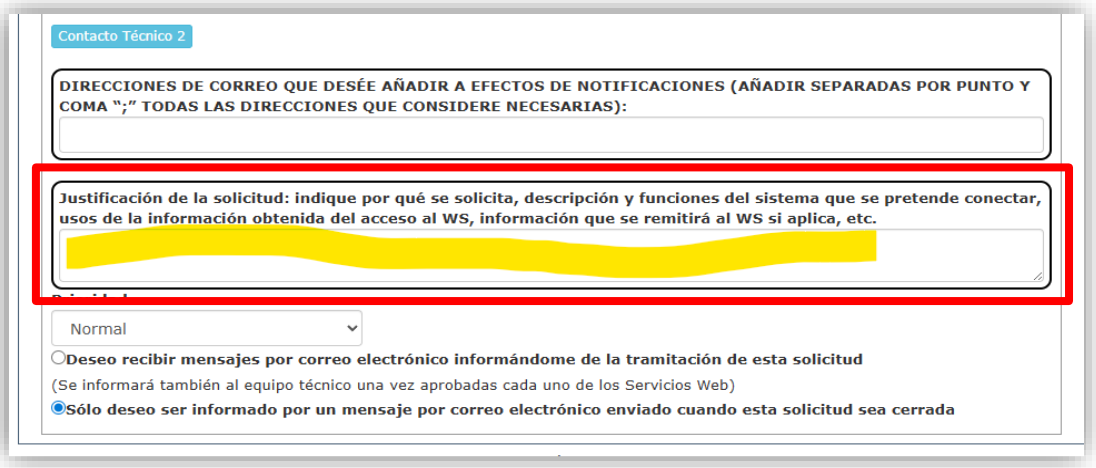
Una vez accedido al sistema RADIX Servicios Web el propio sistema pedirá una serie de datos para cumplimentar la solicitud. Es importante recalcar que es **obligatorio** cumplimentar el campo **justificación** tanto en la pestaña

Servicios web como en la pestaña Solicitud. Igualmente, es obligatorio marcar el *check* del consentimiento en la parte superior del contenido de la pestaña Solicitud. El formulario que se muestra tendrá el siguiente formato:



9. Solicitud RADIX Servicios Web – Pestaña Servicios Web





10. Solicitud RADIX Servicios Web – Pestaña Solicitud

Para cumplimentar la solicitud, será necesaria la intervención de las siguientes personas:

1. Peticionario del centro cliente: será la persona encargada de rellenar y firmar electrónicamente el formulario de solicitud. Igualmente, será quien registre, en su caso, las incidencias de carácter administrativo en el curso

del ciclo de vida completo de la solicitud. Entre la información que debe proporcionar al registrar la solicitud, se incluirán los datos de contacto de hasta 2 técnicos.

2. Técnicos designados por el peticionario del centro cliente: serán las personas encargadas de suministrar la parte pública de los certificados electrónicos cliente a través de la propia herramienta RADIX Servicios web. Igualmente, serán los responsables del desarrollo de la integración con la API REST SOROLLA2 en el ámbito de sus sistemas. Es decir, de los desarrollos a realizar para que el sistema *cliente* pueda utilizar la API REST SOROLLA2.
3. Responsables de la API REST SOROLLA2: una vez enviada la solicitud, ésta será remitida al equipo de SOROLLA2 para que determine si se autoriza o deniega dicha solicitud.

4.3. Confirmación de la autorización de acceso.

Una vez enviada la solicitud, si el equipo de SOROLLA2 está de acuerdo y autoriza la solicitud, el contacto técnico recibirá un correo electrónico donde se detallarán una serie de cuestiones técnicas a tener en cuenta para comenzar la integración con la API REST SOROLLA2. Entre otros aspectos, se indica la URL de acceso a RADIX Servicios Web para poder dar de alta el certificado electrónico a emplear en las comunicaciones. Igualmente, de cara a identificar al sistema que se está integrando con la API REST SOROLLA2, se incluye en el mismo correo electrónico.

4.4. Configuración preliminar de la integración.

Dado que SOROLLA2 es un sistema de categoría MEDIA según lo indicado en el Esquema Nacional de Seguridad, las comunicaciones entre los sistemas externos y la API REST SOROLLA2 están securizadas para cumplir los requisitos indicados para los sistemas incluidos en esta categoría.

A continuación, se describen los aspectos a tener en cuenta para poder establecer de forma correcta la comunicación entre ambos sistemas.

Incorporación certificado electrónico

El primero de los aspectos a tener en cuenta, el cual se menciona en apartados anteriores, es la necesidad de contar con un certificado electrónico para poder establecer la comunicación. La parte pública de este certificado electrónico deberá registrarse, por parte del contacto técnico, en el sistema RADIX Servicios Web. Dicho sistema cuenta con una sección denominada Listado de Certificados donde se recoge, para cada usuario dado de alta el certificado electrónico registrado. El usuario que aparece en el listado de certificados se corresponde con el usuario recibido en el correo electrónico con los detalles técnicos.

11. RADIX Servicios Web - Listado de certificados

Establecer comunicación Sistema externo – API REST SOROLLA2

Una vez registrada la parte pública del certificado electrónico en RADIX Servicios Web, el siguiente paso sería el establecimiento, propiamente dicho, de la comunicación entre el sistema externo y la API REST SOROLLA2. Para ello, lo primero que hay que tener en cuenta es que la comunicación entre ambos sistemas deberá realizarse empleando mTLS. Para ello, se hará uso del certificado electrónico cuya parte pública se ha registrado previamente. Además, para poder consumir la API REST SOROLLA2, será necesario contar con un token de acceso JWT el cual se deberá obtener utilizando la información recibida mediante correo electrónico por el contacto técnico (URL, client id y scope).

Una vez obtenido el token JWT como último paso para poder consumir la API REST SOROLLA2 se deberá emplear el token JWT en la cabecera Authorization de cada petición que se realice a la API REST SOROLLA2. Además de este token de acceso, será necesario contar con una segunda cabecera obligatoria cuya clave es X-APIKEY. El valor de esta clave se proporcionará al contacto técnico una vez se haya autorizado el uso de la API REST SOROLLA2 al centro gestor.