



Eusko Jauriaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

[Administración Digital]

Servicios de construcción y despliegue de los componentes de interoperabilidad para la plataforma NIRE

NIRE – Interoperabilidad

Expediente de Contratación EJIE-007-2025 – NIRE-Interop

Documento de especificaciones Técnicas

Febrero 2025

Este documento es propiedad de Eusko Jauriaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A. (EJIE) y su contenido es CONFIDENCIAL. Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otras partes, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.

Dokumentu honen jabea Eusko Jauriaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A. (EJIE) da eta ISILPEKO edukia du. Dokumentu hau ezin da errepikatu, ez guztiz ez zatika, ezta beste pertsona batzuei erakutsi ere, ezta bere ematea kausatu duten helburuetatik kanpo erabili ere, EJIEk aldeztu aurretik eta idatziz baimendu ezik. Kontratu baten ondorioz ematekotan, bakarrik kontratu horretan espresuki baimenduta dagoenerako erabil daiteke. EJIEri ezin izango zaio inola ere leporatu dokumentuaren edizioan balizko akatsak edo omisioak egonez gero.

Bertsioa Versión	Data Fecha	Aldaketetako laburpena Resumen de cambios	Nork eginda Elaborado por	Nork onartuta Aprobado por
1.0	Febrero 2025	Versión Inicial	Alex Lara	Juanjo Villa

Contenido		
	Capítulo/sección	Página
	1 Introducción	8
	1.1 Proyecto NIK / NIRE	8
	1.2 Visión general de NIK / NIRE	11
	1.2.1 NIK	11
	1.2.1.1 Reglamento [eIDAS]	11
	1.2.1.2 [eIDAS 2] y los [wallet digitales]	12
	1.2.2 NIRE	14
	2 Contexto	16
	2.1 Contexto General	16
	2.1.1 Atención integral multicanal a la ciudadanía y el acceso a los servicios públicos por medios electrónicos	16
	2.1.2 Plan Estratégico de Gobernanza, Innovación Pública y Gobierno Digital (ARDATZ 2030) 17	
	2.1.3 Modelo de Gestión TIC del Sector Público Vasco: Plan Estratégico TIC del Gobierno Vasco	18
	2.1.4 Estrategia de Gobernanza de los Datos del Sector Público de la CAE	19
	2.1.5 Plan de proyectos NIK-NIRE	21
	2.2 Contexto de [EJIE]	22
	3 Descripción del proyecto y los [productos] a construir	24
	3.1 Visión de alto nivel de la arquitectura de interoperabilidad	25
	3.2 CORE de interoperabilidad persona – administración en [NIRE]	28
	3.2.1 API Gateway	30
	3.2.2 Middleware + conectores	31
	3.2.3 Retrieve Rules API & DB	32
	3.3 Identidad y autenticación	35
	3.3.1 User Authentication: Autenticación en la app / web [NIRE]	37
	3.3.2 App authentication	40

3.3.3	Autenticación mutua [NIRE] ↔ [Admin]	41
3.3.3.1	Clave compartida	42
3.3.3.2	Par [clave pública] – [clave privada]	42
3.3.3.3	Certificados X509	42
3.3.3.4	Solución Zero-trust basada en un [Access Management System].	43
3.3.4	Extensión de la autenticación desde el [dispositivo cliente] a la [sede electrónica] de la [administración]	43
3.4	Datos del sistema	45
3.4.1	Monitorización / Observabilidad / Traza	46
3.4.2	Audit	48
3.4.3	Datos Analíticos para el Observatorio de Administración Digital	49
3.5	Consentimientos	50
3.6	Datos que se interoperan	53
3.6.1	NIRE Datuak	55
3.6.1.1	Datos básicos: contacto y bancarios	55
3.6.1.2	Representaciones y Autorizaciones	63
3.6.1.3	Certificados / carnets / títulos / etc	65
3.6.2	NIRE Karpeta	66
3.6.2.1	Datos asociados a expedientes	66
3.6.2.2	Otros datos de asociados a la tramitación de [expedientes]	67
3.6.2.3	Datos asociados a pagos	68
3.6.3	Calendario	69
3.6.4	Servicios	70
3.7	Interfaz de persona usuaria de administración de NIRE	72
3.7.1	Descripción general de la interfaz de administración	72
3.7.2	Gestión de Autorizaciones	74
3.8	Mensajería PUSH	75
3.8.1	Enrollment de [app]	76

3.8.1.1	Dispositivo móvil	76
3.8.1.2	App Web (desktop)	78
3.8.2	Envío de mensajes	79
3.8.3	Mensajes PUSH interactivos	81
3.8.4	Suscripciones: multicast a múltiples dispositivos	82
3.8.5	Datos del sistema	83
3.8.5.1	Monitorización / Observabilidad	83
3.8.5.2	Datos analíticos	83
3.8.5.3	Audit	83
3.8.6	Interfaz de personas usuaria de administración del sistema de mensajería PUSH	84
3.9	Seguridad y confidencialidad	85
3.10	Privacidad desde el diseño y por defecto	86
4	Ciclo de vida del trabajo para la integración de un [dato interoperable] en [NIRE]	87
5	Vistazo general al prototipo de la UI	90
6	Objeto del contrato	95
6.1	Visión de alto nivel	95
6.2	Detalle actividades identificadas a día de hoy	97
6.2.1	Actividades Transversales	97
6.2.2	CORE de interoperabilidad persona < - > administraciones	99
6.2.3	Identidad y Autenticación	100
6.2.3.1	User Authentication	100
6.2.3.2	App Authentication	101
6.2.3.3	NIRE – Admin mutual authentication	101
6.2.3.4	Extensión de la autenticación desde el [dispositivo cliente] a la [sede electrónica] de la [administración]	102
6.2.4	Datos Básicos	103
6.2.5	Datos del sistema	104
6.2.6	Consentimientos	105

6.2.7	Datos que se interoperan	106
6.2.7.1	Construcción del [middleware] para un determinado [dato interoperable]	107
6.2.7.2	Construcción del [conector] para un [origen de datos]	108
6.2.8	Interfaz de persona usuaria de administración de NIRE	110
6.2.9	Mensajería PUSH	111
6.2.10	Auditoría	112
6.2.11	Actividades de Gestión	113
7	Planificación	114
7.1	Alcance	116
7.2	Calendario	118
7.3	Recursos	119
7.4	Coste	4
7.5	Productos Entregables	5
7.5.1	Infraestructura y entornos	5
7.5.2	CORE Interoperabilidad	6
7.5.3	Identidad y autenticación	7
7.5.4	Datos Básicos	7
7.5.5	Datos del sistema	8
7.5.6	UI de Administración del sistema	8
7.5.7	Consentimientos	9
7.5.8	Mensajería PUSH	9
7.5.9	Middleware y conectores con los [órigenes de datos] en las [administraciones]	10
7.5.10	Documentación para desarrolladores y entorno sandbox	10
7.5.11	Auditoría	11
7.6	Calidad	12
7.7	Comunicaciones	13
7.7.1	Stakeholders	13

7.7.2	Estructuras de control y comunicaciones	14
7.7.2.1	Comité Director: visión del proyecto a nivel de dirección	
14		
7.7.2.2	Seguimiento Funcional / Técnico	14
7.8	Riesgos	15
8	Contenido de la Oferta Técnica	16

1 Introducción

1.1 Proyecto NIK / NIRE

La estrategia de **[Gobierno Digital]** del **[Gobierno Vasco]** pone el foco en la **generación de valor público mediante el uso de la tecnología** para lograr:

- Una **administración plenamente digital**
- **Optimizar las capacidades analíticas y predictivas** para tomar **decisiones ágiles basadas en datos**

... con el objetivo final de mejorar en:

- **Eficiencia:** trámites e información ágiles que generan ahorros
- **Calidad** de servicio público
- Acceso a la información y **transparencia**
- **Innovación** y generación de nuevas oportunidades de valor público
- **Empoderamiento de la ciudadanía:** oportunidades de participar y colaborar

En este contexto general de **[Gobierno Digital]**, se materializa una **visión sobre la provisión de servicios por parte de la administración** en la que:



- Las **personas usuarias** son el centro
- Se ofrecen servicios de manera **omnicanal**
- Se ofrecen servicios de forma **proactiva**
- La toma de decisiones se basa en los **datos**
- Se trabaja con **otras administraciones** en ofrecer servicios comunes
- Se **gestionan** los servicios de forma **eficiente** y **ágil** mejorando de forma continua los procesos internos y externos

Para materializar esta **visión**, el **[Gobierno Vasco]** trabaja en múltiples proyectos, y en concreto, en lo que afecta más directamente al presente expediente, **en 2024 ha puesto en marcha una [Oficina Técnica](#)** que tiene como objetivo dar soporte al **[programa de proyectos NIK-NIRE]** para:

- 1 Mejorar y simplificar el **acceso** de las personas a los [servicios digitales]: **NIK**
- 2 **Dar el control de los datos a las personas:** facilitar el acceso de las personas a los datos que sobre ellas tienen las [Administraciones Vascas]: **NIRE**
- 3 Ofrecer **información y servicios proactivos**



El **[producto]** del [proyecto] es una **[app móvil]** y **[web]** donde las personas podrán encontrar cualquier dato que sobre ellas tengan las [Administraciones Vascas] e interactuar con los [servicios] de la [administración]

El **[proyecto]** es fundamentalmente un **gran esfuerzo de todas las [Administraciones Vascas]** que **trabajan en común** en tres grandes áreas:

1. Definición del [producto]: diseñar la [app móvil] y [web]
2. Construir los sistemas de [interoperabilidad] que *proporcionan* los [datos] que se muestran en la [app]/[web]
3. Mejorar la usabilidad de los sistemas de [identificación]
4. Difundir la iniciativa

Aunque el nombre definitivo del [producto] **va a ser definido mediante un trabajo en común por las [Administraciones Vascas]**, inicialmente y para **delimitar los ámbitos** en el [programa], éste se ha denominado [NIK]/[NIRE]:

NIK	▪ Identidad digital ▪ Credenciales verificables (<i>títulos, carnets, etc</i>) / atributos de una persona ▪ Firma
NIRE	▪ Datos sobre una persona en cada administración - NIRE-Datuak: datos que las [administraciones] “tienen” - Datos básicos de contacto / bancarios - Representaciones - Certificados / carnets / títulos, etc - ... - NIRE Karpeta: datos asociados a [expedientes] - Expedientes - Notificaciones y avisos - Pagos - Multas - ... - Calendario: citas, eventos relevantes, etc - Servicios: préstamos bibliotecarios, reservas de instalaciones deportivas, etc



Ambos proyectos son **complementarios** y **no se concibe uno sin el otro**.

- **[NIK]** está asociado a un **[wallet]** digital donde *residen* la **[identidades]** y las **[credenciales]** y donde se pueden realizar operaciones de **[firma]**
- **[NIRE]** está asociado a un **[sitio web]** y **[app móvil]** desde donde las personas tendrán acceso a cuantos **datos** sea posible de todas las [administraciones]

Ambos ámbitos **se realimentan**: Para **identificarse** en [NIRE] con toda seguridad se utilizará [NIK] y posiblemente [NIRE] pueda ser el **origen de [credenciales]** que se almacenan en [NIK]

En cualquier caso, es importante recalcar que **[NIK]/[NIRE] son conceptos que ayudan en la gestión del proyecto delimitando alcances**; aún hay que trabajar en:

- La(s) “**marca(s)**” final(es)
- Si se construirá una [app]/[web] única o se mantienen iniciativas separadas

En este ámbito la [Oficina Técnica NIK/NIRE] tiene como propósito las siguientes funciones:

Gestión	Secretaría técnica	Coordina los trabajos en común de las [Administraciones Vascas]
	PMO supportive	Soporte en la gestión de los [sub-proyectos] en el ámbito [NIK/NIRE]
Conceptualización	Diseño de producto	Definir el [producto] [NIK]/[NIRE] trabajando colaborativamente entre todas las [Administraciones Vascas]
	Marca	Definición de la [marca]
	Road-Map	Creación, publicación y mantenimiento de una [hoja de ruta] (<i>road-map</i>) donde se detallarán los [datos] que cada [Administración] publicará en [NIRE] y cuándo
Ejecución	Soporte a proyectos [NIK]/[NIRE]	Soporte experto en diferentes áreas: - Funcional - Técnica - User-experience - Legal
	Sitio web del desarrollador	Construcción de un [sitio web] que <i>centralice</i> toda la información funcional y técnica del proyecto
Gestión del Cambio	Difusión	Difusión del [producto]

Por lo tanto, y en lo que afecta al presente [expediente de contratación], la [Oficina Técnica] ayudará en:

1. El **diseño** del [producto] a construir > [Diseño de Producto]
2. El **impulso** los [proyectos] que den lugar a los [productos] anteriormente diseñados
3. **La gestión de la ejecución** de los [proyectos]
4. El **soporte técnico / funcional / normativo**



El [proyecto] objeto del presente [expediente de contratación] de centra en los **datos de las personas (NIRE)**

[NIRE] es fundamentalmente un **[sistema de interoperabilidad Administración-Ciudadanía]** del que se “alimentan” la [app móvil] y [web]

... por lo tanto, el primer [proyecto] a construir es precisamente este **[sistema de interoperabilidad]** y que constituye el **objeto del presente [expediente de contratación]**

... en otro [expediente de contratación] diferente del actual se contratará la construcción de la [interfaz de usuario (UI)] en forma de [app móvil] y [web] en dos [lotes] (*uno para la [app móvil] y otro para la versión [web]*) y que se basarán en la [interoperabilidad] para obtener los datos de las personas en las diferentes [Administraciones Vascas]

1.2 Visión general de NIK / NIRE

Para introducir lo que es [NIRE] conviene introducir también la iniciativa [NIK] de cara a delimitar el ámbito de cada una de las iniciativas.

En una primera visión de muy alto nivel:

1.2.1 NIK

[NIK] como ya se ha introducido tiene que ver con la [identidad] en su sentido más amplio y en particular con la [identidad] (y la [autenticación]) y las [credenciales verificables] (títulos, carnets, etc).

[NIK] se *sustancia* en un [wallet] donde residen esta [identidad] y [credenciales verificables] controladas por la persona propietaria del [wallet] que decide qué datos comparte en los servicios electrónicos.

En este contexto, hay que tener en cuenta:

1.2.1.1 Reglamento [eIDAS]

El reglamento [UE 910/2014] del Parlamento y Consejo Europeos del 23 de Julio de 2014 [eIDAS = Electronic Identification and Thrust Services] y que entró en vigor en 2016 define los estándares y normas para facilitar las interacciones electrónicas en la Unión Europea utilizando [firma electrónica]

Firma Electrónica Simple (SES)	▪ Nivel más básico de firma electrónica ▪ Puede ser una firma manuscrita escaneada, marcar una casilla o introducir un PIN ▪ No permite identificar a la persona firmante de forma inequívoca ▪ No asegura la autenticidad e integridad de los datos firmados
Firma Electrónica Avanzada (AES)	▪ Tiene un nivel de seguridad más alto que la [firma electrónica simple] ▪ Requiere una identificación de la persona ▪ La [firma] debe cumplir algunos requisitos básicos: 1. Estar vinculada a la [persona firmante] de forma inequívoca 2. Permitir identificar a la [persona firmante] 3. Estar creada utilizando medios bajo el control exclusivo de la [persona firmante] como su teléfono, PC o rasgos biométricos. 4. Garantizar la autenticidad e integridad de los datos firmados ▪ Una infraestructura PKI (<i>Public Key Infrastructure</i>) cumple los requisitos anteriores, pero también se pueden utilizar tecnologías biométricas u otras más sencillas. ▪ En caso de disputa, es la parte <i>disputada</i> (la que ve cuestionada la [firma]) la que tiene que demostrar su validez (o no)
Firma Electrónica Cualificada (QES)	▪ Nivel más alto de seguridad y confianza (<i>vincula legalmente</i>); equivalente a la firma manuscrita ▪ Requiere una identificación cara a cara (o por video) ▪ Se basa en los estándares de una [firma electrónica avanzada AES] pero el [requisito 3] de los anteriores es más estricto y requiere de la utilización de un dispositivo [SQCD=Qualified Signature Creation Device] que genere la firma utilizando un [certificado cualificado] que únicamente puede ser emitido por un [(Q)TSP = (Qualified) Trusted Service Providers] como IZENPE ▪ En caso de disputa, es la parte <i>disputante</i> (la que impugna la validez de la [firma]) la que tiene que demostrar su validez (o no)

1.2.1.2 [eIDAS 2] y los [wallet digitales]

Si bien [eIDAS] ha supuesto un gran avance en el área de la [firma electrónica], **no lo ha sido tanto en cuanto a la [identificación electrónica]**, así que la [UE] ha trabajado en una nueva versión del reglamento ([eIDAS 2](#)) que se enfoca en la [identidad digital] promoviendo que toda la ciudadanía europea tenga la posibilidad de tener un [wallet digital] ([EU Digital Wallet](#)) que permita el **acceso a los servicios on-line públicos o privados** asegurando la [protección de los datos personales] que estarán bajo el control de las personas que decidirán si los comparten o no.



Las [VLOPs](#)=Very Large Online Platforms] (Facebook, Amazon, Instagram, Booking, Alibaba...) y [VLOSEs](#)=Very Large Online Search Engines] (Google, Bing, ...) designados en la [Digital Services Act](#) estarán obligados a autenticar a sus usuarios y a aceptar el [EU Digital Identity Wallet] para acceder a los servicios.



Los estados miembros de la [UE], en los 24 meses siguientes a la puesta en vigor de [eIDAS2] (*20 de mayo de 2024*), están obligados a emitir un [EU Digital Wallet] que puede ser emitido por el propio [estado miembro] o por un tercero reconocido por el [estado miembro]

El [EU Digital Identity Wallet] no solo servirá para almacenar (*y presentar*) la [identidad] ([eID](#)) sino que servirán también para:

- Contener **credenciales** digitales como: certificados profesionales o títulos (*ej: título universitario*), licencias (*ej: carnet de conducir*), carnets (*ej: carnet de la biblioteca*)
- Contener **documentos** como una receta médica o un ticket de viaje
- Realizar **pagos**

[eIDAS2] se encuadra en el marco general del [futuro digital para Europa](#) que se plasma en iniciativas y proyectos relevantes para la implementación del [EU Digital ID Wallet]:

1. [EBSI](#) (European Blockchain Services Infrastructure)

La infraestructura [blockchain] europea tiene como objetivo aprovechar el potencial de la [blockchain] en el ámbito de la [unión europea] en tres grandes dominios de [casos de uso]

1. Credenciales verificables > aplicable en el [EU Digital Wallet]
2. Seguimiento y traza
3. Intercambio de datos confiable

2. [Proyectos Piloto](#)

Con el objetivo de testear el [EU Digital Wallet] la [UE] está impulsando varios [pilotos] en escenarios reales como entre otras:

- Acceso a servicios de la administración
- Recetas médicas electrónicas
- Credenciales educativas y profesionales
- Seguridad Social
- Contratación y activación de tarjetas SIM para redes móviles
- Apertura de cuentas en entidades financieras
- Pagos
- Viajes
- etc

Son especialmente importantes los siguientes [pilotos]:

EWC (EU Digital Wallet Consortium)	Viajes	Almacenamiento en el [EU Digital Wallet] de documentos necesarios para viajar como [pasaporte], [visados], [tickets de transporte], etc
	Identidades digitales en el ámbito de las organizaciones	Utilización del [EU Digital Wallet] para acreditar la pertenencia a una organización, así como de autorizaciones en este ámbito
	Pago	Utilización del [EU Digital Wallet] para la realización de pagos
DC4EU (Digital Credentials for Europe) Centrada en [educación] y la [seguridad social]	Credenciales educativas	Educación
	Autorizaciones profesionales	
	Certificado que demuestra que una persona cotiza a la [seguridad social] en otro país de la UE en calidad de trabajador desplazado (<i>Portable Document A1</i>)	Seguridad Social
	Tarjeta Sanitaria Europea (European Health Insurance Card)	
WE-BUILD consortium Wallet for Europe Centrado en la [persona legal] (LPID)	Business	Legal Person Wallet Declaración de tasas / impuestos Acreditación de poder de representación (PoA) Pruebas de residencia Micro-credenciales
	Payments	Consumer Payments Business Payments
	Logistics & Supply Chain	Control de mercancías eInvoicing



[NIK] se ve directamente implicado por el marco regulatorio [eIDAS 2] y su evolución traccionada por los proyectos piloto del [EU Digital Wallet], en particular [WE-BUILD]

1.2.2 NIRE

Enfocando más sobre [NIRE] (**datos**), como se ha introducido, es un *concepto* que intenta “aglutinar” todo lo que tiene que ver con los **datos de una persona** (*física o jurídica*) en cualquier [Administración Vasca], entre otras muchas cosas:

NIRE Datuak Datos que la administración “tiene” sobre las personas	▪ Datos básicos – Datos básicos de identificación: nombre, apellidos, documentos identificativos, etc – Datos de contacto: empadronamiento, dirección(es), teléfono(s), email(s), etc – Datos bancarios: número de cuenta corriente ▪ Apoderamientos / representaciones ▪ Carnets / Autorizaciones: <i>familia numerosa, manipulador de alimentos, pesca, etc</i> ▪ Certificados: matrimonio, pareja de hecho, fiscales, penales, discapacidad, familia numerosa, etc ▪ Credenciales de formación ▪ Títulos educativos / Historial académico ▪ Inscripción como demandante de empleo ▪ ...
NIRE Karpeta Datos asociados a [expedientes]	▪ Expedientes con cualquier Administración (<i>ayudas/subvenciones, premios, autorizaciones, etc</i>) ▪ Documentación registrada ▪ Notificaciones ▪ Pagos ▪ Multas ▪ Procesos de selección pública (OPEs) ▪ ...
Calendario	▪ Citas con diferentes servicios ▪ Caducidad de registros, carnets, etc ▪ Fechas límite para presentar una ayuda, hacer un pago pendiente, presentar impuestos, etc ▪ Fechas de exámenes ▪ Devolución de préstamos bibliotecarios ▪ Reserva de instalaciones deportivas municipales
Servicios	▪ NIRECard ▪ Transporte ▪ Préstamos bibliotecarios ▪ Reserva de instalaciones deportivas municipales ▪ ...

En algunos casos esta visión de un punto común de los **datos** asociados una persona se denomina **citizen data hub** o **visión 360** pero quizá estas definiciones vienen de un punto de vista asociado a los sistemas CRM (*customer relationship management*) de las [administraciones] que **NO son objeto principal de la presente iniciativa** puesto que el *destinatario* del [producto] son las [personas] (*y no tanto las [administraciones]*)

[NIRE], en definitiva, es un **esfuerzo común** de las [Administraciones Vascas] por **dar el control de sus datos a las personas** y como tal tiene como ambición dar respuesta entre otras a las siguientes preguntas:

- **En qué sistemas** de la(s) Administración(es) hay datos sobre mí: expedientes, notificaciones, pagos, citas, etc
- **Qué datos** tiene sobre mí la(s) Administración(es) en estos sistemas
- **Cómo puedo actualizar** algunos datos comunes como los [datos de contacto] o la [cuenta corriente] desde un punto común y que este dato actualizado se *comunique* automáticamente a otras entidades y administraciones
- **Cómo puedo recibir comunicaciones** de la [Administración] de una forma unificada y personalizada
- ... en un futuro **cómo puede hacer algunos trámites**
- etc

A nivel estratégico, a largo plazo [NIRE] es una iniciativa que *enlaza* de alguna forma con la [transparencia] y la [Gobernanza del Dato]

Transparencia Se da la posibilidad a las personas de:

- **Saber** en qué [bases de datos] de qué [Administraciones] hay datos relacionados a una [identidad].
- En algunos casos **consultar** los datos e incluso **actualizarlos**



El caso más paradigmático es el de los [datos básicos] de [contacto] y [cuenta corriente] que están en decenas de [bases de datos] de diferentes [Administraciones Públicas] y cuya actualización supone un enorme esfuerzo para la persona interesada.

Gobernanza del Dato

La ambición de [NIRE] es constituirse en una **referencia** en algunos datos importantes como los [datos de contacto] o la [cuenta corriente] (*entre otros*) puesto que serían datos **“curados”** por la propia persona interesada.

Este hecho habilita la **construcción de sistemas derivados** en base a estos datos *curados*.

Por ejemplo:

- Un sistema para **contactar** con las personas que debería utilizar los [datos de contacto] más *fiables* disponibles (*y mejor si es la propia persona la que los determina utilizando [NIRE]*)
- Sistemas de [relación con las personas] (CRM)



El objetivo de [NIRE] NO es sustituir a los servicios ofrecidos por otras administraciones, Osakidetza, Lanbide, etc para sus personas usuarias sino únicamente ofrecer un punto común (*un hub*) desde donde poder acceder a los datos y desde ahí dirigirse a los servicios específicos.

En este sentido, [NIRE] puede verse como un esfuerzo de [interoperabilidad] para crear un **punto común de consulta**.

Unos [servicios electrónicos] centrados en la ciudadanía no pueden pensarse desde cada administración de forma independiente, sino que deben abordarse desde una perspectiva de **funcionamiento en red del conjunto de las [Administraciones Públicas]**.

La **colaboración interadministrativa** en este ámbito responde a dos objetivos:

- Dar un **servicio integrado** a la ciudadanía, evitándole, por ejemplo, la necesidad de recorrer las diversas sedes electrónicas para acceder a las notificaciones remitidas por cada administración pública o la solicitud de documentación que ya obra en poder de cualquier administración pública.
- **Utilizar con racionalidad los recursos públicos.**

2 Contexto

2.1 Contexto General

[EJIE] como el [órgano gestor tecnológico] del [Gobierno Vasco], ejecuta este proyecto en un contexto influenciado por:

1. La [Atención integral y multicanal a la ciudadanía y el acceso a los servicios públicos por medios electrónicos]
2. El [Plan Estratégico de Gobernanza, Innovación Pública y Gobierno Digital] (ARDATZ 2030)
3. El [Plan Estratégico TIC] del [Gobierno Vasco] (PETIC) derivado del [Modelo de Gestión TIC del Sector Público Vasco]
4. La [Estrategia de Gobernanza del Dato] en el [Gobierno Vasco]
5. El [Mecanismo de Recuperación y Resiliencia] dentro del Plan [Next Generation EU]



Este [expediente de contratación **NO** está financiado]

A continuación, se da una visión general de cada uno de estos *factores ambientales* y de su influencia en el presente proyecto.

2.1.1 Atención integral multicanal a la ciudadanía y el acceso a los servicios públicos por medios electrónicos

El 20 de junio de 2023 el Gobierno Vasco publicó el [DECRETO 91/2023, de 20 de junio, de atención integral y multicanal a la ciudadanía y acceso a los servicios públicos por medios electrónicos](#) que tiene como objeto regular:

- La **atención e información** a la ciudadanía
- El **derecho** de la ciudadanía a **relacionarse** con la Administración por **medios electrónicos** para:
 - **Acceder** a los servicios públicos
 - **Tramitar** procedimientos administrativos
- La gobernanza, la organización y los medios tecnológicos necesarios

El decreto en su preámbulo reconoce que la existencia de servicios electrónicos per-se no produce eficiencia, sino que la digitalización debe basarse en:

- Una **reingeniería de procesos**
- La **simplificación administrativa**: reducción de cargas para la ciudadanía
- **Normalización de documentos** con lenguaje claro y de lectura fácil
- **Oferta proactiva de servicios** más personalizados
- Una visión de **servicio digital basado en los datos** de los que la Administración dispone para personalizar el acceso de la ciudadanía al mismo o para ofrecerlo de forma proactiva

2.1.2 Plan Estratégico de Gobernanza, Innovación Pública y Gobierno Digital (ARDATZ 2030)

El [Gobierno Vasco] lleva años avanzando en lo que en un principio se vino en llamar la [Administración Digital] y que en los últimos años ha ampliado el alcance para hablarse de [Gobierno Digital] en el contexto de la [transformación digital] a la que inevitablemente está obligada toda la sociedad.

La transición digital se ha articulado en base a sucesivas planificaciones estratégicas en materia de **gobernanza e innovación pública** que en todos los casos han tenido como uno de los ejes estratégicos, aunque con diferentes denominaciones, la [administración electrónica] y los [servicios digitales]:

- Plan de Innovación Pública, PIP 2011-2013
- Plan de Innovación Pública [PIP 2014-2016](#)
- Plan Estratégico de Gobernanza e Innovación Pública, [PEGIP 2020](#)
- ...y en la actualidad, el [\[Plan Estratégico de Gobernanza e Innovación Pública y Gobierno Digital\]](#) (ARDATZ 2030) es uno de los [\[planes estratégicos para la XII Legislatura\]](#) y constituye la materialización del compromiso para la puesta en marcha de la [Estrategia Vasca de Gobierno Digital] incluida en el [\[Programa de Gobierno vasco 2020-2024\]](#) para la [XII Legislatura]

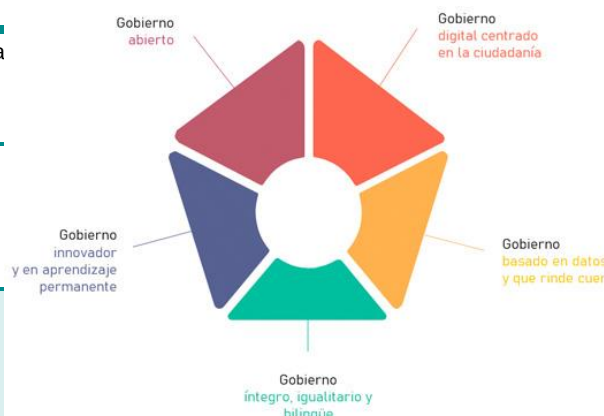
La [Organización para la Cooperación y el Desarrollo Económico-OCDE] ha definido el [Marco normativo para el Gobierno Digital \(Digital Government Policy Framework- DGPF\)](#) que está constituido por seis dimensiones:

1. **digital** desde el diseño
2. **sector público basado en datos**
3. **gobierno como plataforma**
4. **abierto** por defecto
5. **centrado en las personas usuarias**
6. **proactivo**



Con esta referencia, [ARDATZ] se estructura en los siguientes ámbitos y ejes estratégicos, situando a la **ciudadanía en el centro**:

Ámbito Estratégico	Eje
GOBIERNO ÍNTEGRO, IGUALITARIO Y BILINGÜE	Cultura de gestión y cultura organizacional Igualdad de mujeres y hombres Euskera lengua de trabajo y servicio
GOBIERNO INNOVADOR Y EN APRENDIZAJE PERMANENTE	Normativa Personas Organización Infraestructuras
GOBIERNO DIGITAL CENTRADO EN LA CIUDADANÍA	Atención a la ciudadanía integral y multicanal Servicios digitales Gobernanza de los datos y de la información
GOBIERNO BASADO EN DATOS Y QUE RINDE CUENTAS	Gobernanza de los datos y de la información Planificación Evaluación y rendición de cuentas Gobernanza multinivel
GOBIERNO ABIERTO	Comunicación pública Transparencia Participación y colaboración de la ciudadanía



El presente expediente de contratación se encuadra en los [ámbitos estratégicos] dedicados a:

- Gobierno Digital Centrado en la Ciudadanía]
- Gobierno Basado en Datos y que rinde cuentas

2.1.3 Modelo de Gestión TIC del Sector Público Vasco: Plan Estratégico TIC del Gobierno Vasco

El [DECRETO 36/2020, de 10 de marzo, regula el \[Modelo de Gestión de las Tecnologías de la Información y la Comunicación\] \(TIC\) en el \[Sector Público de la Comunidad Autónoma de Euskadi\]](#), decreto que permite establecer una **estrategia compartida** para impulsar la **convergencia**, la **calidad** y la **eficiencia** en el ámbito TIC del [Sector Público Vasco] y posibilitar su **[transformación digital]**

Los retos a los que responde el [Modelo de Gestión TIC] son:

- Poner a disposición de la ciudadanía una **administración proactiva** que ofrece sus servicios por todos los canales disponibles (**administración omnicanal**), prestando especial atención a los medios electrónicos con el objetivo de **habilitar la posibilidad de realizar todas las gestiones y trámites administrativos** a través de Internet, de manera sencilla, *independientemente de la capacitación de la persona usuaria*, utilizando cualquier dispositivo y tanto en euskera como en castellano
- Disponer de unos **sistemas y servicios TIC modernos y eficientes**, alineados con las necesidades reales de la organización y que aporten valor en el marco de la prestación de unos [servicios públicos] de calidad.
- Favorecer la **mejora continua** en la calidad de los servicios
- Avanzar hacia una **organización más colaborativa y participativa**

El [Decreto 36/2020](#) recoge la necesidad de **planificar** los proyectos necesarios para **materializar la transición y transformación a un nuevo [modelo de gestión TIC]**, planificación que se materializó en el [\[Consejo de Gobierno Vasco\] el 28 de septiembre de 2021](#) mediante la aprobación del [\[Plan Estratégico TIC\]](#) (PETIC) para el período 2021-2024 que debe **sentar las bases para la modernización cohesionada del [Sector Público Vasco]** *(y que próximamente será revisado para crear el nuevo [Plan de Transformación Digital para el Sector Público de la CAE])*

Los **[ejes estratégicos]** del [PETIC 2021-2024] son cinco:

- | | | |
|---|------------------------------------|--|
| 1 | Modelo de gobernanza TIC | <ul style="list-style-type: none"> ▪ Estructurar y organizar la gestión de las TIC en el Sector Público Vasco, incidiendo de forma específica en el despliegue de las funciones y órganos de gobernanza TIC |
| 2 | Soluciones y servicios TIC | <ul style="list-style-type: none"> ▪ Evolucionar de las soluciones y servicios TIC que se prestan desde y para el Sector Público Vasco en cuatro ámbitos: <ul style="list-style-type: none"> – infraestructura – comunicaciones – puesto de trabajo – servicios corporativos |
| 3 | Tecnologías avanzadas e innovación | <ul style="list-style-type: none"> ▪ Incorporar las tecnologías avanzadas (Big Data, Inteligencia Artificial, tecnología Cloud, ciberseguridad, blockchain, etc.) en la actividad del Sector Público Vasco ▪ Facilitar la innovación basada en tecnología |
| 4 | Organización TIC y personas | <ul style="list-style-type: none"> ▪ Incorporación y desarrollo de nuevos roles TIC ▪ Capacitación digital de los recursos humanos, de cara a su adaptación a las nuevas funciones o competencias asociadas al uso de las TIC. |
| 5 | Gestión avanzada de las TIC | <ul style="list-style-type: none"> ▪ Incorporar principios de [gestión avanzada] en la gestión y desarrollo de proyectos TIC, impulsando para ello la utilización de metodologías comunes que contribuyan a: <ul style="list-style-type: none"> – Armonizar la implementación de las TIC – El despliegue de los estándares tecnológicos del Sector Público Vasco |



El presente expediente de contratación se encuadra en el proyecto [Impulso de la **Estrategia del Dato del Sector Público Vasco**]

En este ámbito, la [\[Dirección de Estrategia Digital\]](#) ha puesto en marcha la [\[Oficina del Dato\]](#) que es un factor contextual importante para este proyecto y que se describe a continuación

2.1.4 Estrategia de Gobernanza de los Datos del Sector Público de la CAE

El 19 de diciembre de 2023 el [Consejo de Gobierno Vasco aprobó](#) la [Estrategia de gobernanza de los datos del sector público de la CAE](#) cuyo propósito es avanzar en la **madurez de los datos**, de forma que sea posible un sector público de la CAE

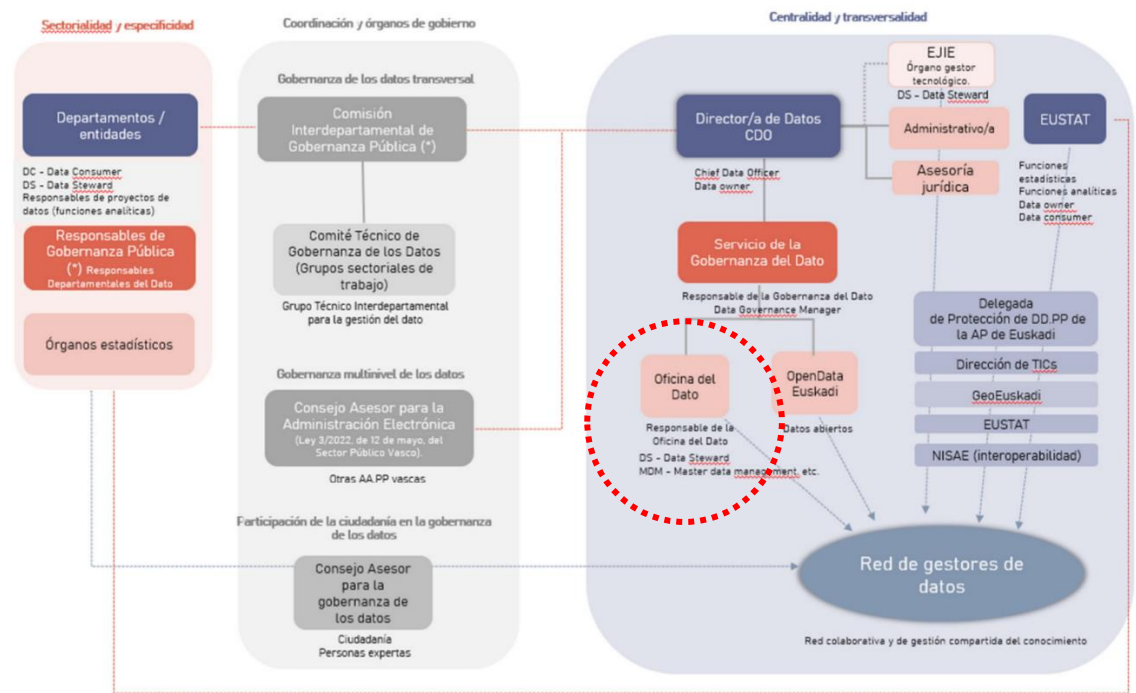
- Con altas **capacidades analíticas y predictivas** que permitan tomar **decisiones ágiles basadas en datos** («Gobierno data-driven» o Gobierno guiado por los datos)
- Que haga un **uso generalizado e inteligente de los datos** (*uso institucionalizado y transversal*)

La [Estrategia de Gobernanza de los Datos] se aplicará a todos los datos que se ajusten a las siguientes categorías:

- Datos de ciudadanía
- Datos de personas empleadas
- Datos de servicios y procedimientos
- Datos de hechos digitales, feedback de usuarios/as de los servicios públicos, etc.
- Datos para la confección de información presupuestaria y contable.
- Datos referidos al cumplimiento de obligaciones legales y/o ejercicio de potestades administrativas.
- Datos recogidos por dispositivos de sensorización (IoT), redes de sensores y de medición.
- Datos de encuestas y sondeos.
- Datos geográficos.
- Datos y recursos lingüísticos, en especial aquellos relacionados con el euskera.
- Datos para informes regulatorios ad-hoc o periódicos.
- Datos para su apertura y reutilización pública (*opendata*)
- Datos estadísticos determinados en las leyes y programas estadísticos
- Cuadros de mando
- Observatorios.
- Datos obtenidos de fuentes externas a la organización.
- Cualquier otro dato que se determine.



La entidad responsable de la [gobernanza de los datos y de la información] es la [\[Oficina del Dato\]](#) dependiente de la [\[Dirección de Estrategia Digital\]](#) del [\[Departamento de Gobernanza, Administración Digital y Autogobierno\]](#) y que tiene la siguiente estructura organizativa:



En este ámbito de la [Gobernanza del Dato], el [proyecto] objeto del presente [expediente de contratación] y con la ayuda de la [Oficina Técnica NIK/NIRE] tiene que tener en cuenta dos iniciativas:

1 Oficina del Dato

- La [Oficina del Dato] proporcionará **directrices** en este ámbito y para ello dispone de una [Oficina Técnica] específica
- El [proyecto NIRE-Interop] por su parte deberá **integrar meta-información** sobre los datos objeto de [NIRE] en los sistemas relacionados con la [Gobernanza del Dato]

2 Observatorio de la Administración Digital

El objetivo del [Observatorio de la Administración Digital] es:

- Tener **información de [cuadro de mando]** como soporte para la **toma de decisiones** informadas en base a datos (*indicadores*)
- Difundir datos e información sobre el uso** de los servicios de la [Administración Digital]

... es por lo tanto, **un punto único** (*un sistema común*) que concentrará y facilitará el acceso a datos e información **procedentes de diferentes sistemas** utilizados en la [Administración Digital].

El **uso** de este [Observatorio de la Administración Digital] es doble:

Uso		Objetivo
Cuadro de Mando	Toma de decisiones informadas en base a datos (<i>indicadores</i>)	→ Mejora de la calidad de los servicios públicos y los procesos inter
Difusión de datos e información	Publicar datos e información del uso de los sistemas	→ Transparencia y monitorización del uso

El [proyecto NIRE-Interop] deberá:

- Colaborar con el [Observatorio de Administración Digital] para identificar los [indicadores] relevantes para ser medidos y publicados
- Proporcionar los [datos] base de los [indicadores] para que sean almacenados en el [data-storage] del [Observatorio de Administración Digital]

El proyecto [Observatorio de la Administración Digital] se estructura en tres lotes con los que será necesario trabajar:

LOTE 1 Oficina Técnica	- Gobernanza del Proyecto - Coordinación Técnica y Funcional - Gestión del Cambio
LOTE 2 Conformación del almacenamiento de datos	Responsable de crear el [data-lake] / [data-warehouse] con los datos procedentes de los diferentes [orígenes] (<i>presencia web, tramitación electrónica, atención a la ciudadanía, opendata, interoperabilidad, firma, etc</i>)
LOTE 3 Cuadro de mando y visualización	Responsable de visualizar los [datos] del almacenamiento en [cuadros de mando] a diferentes niveles

2.1.5 Plan de proyectos NIK-NIRE

El presente [expediente de contratación] [NIRE-Interop] se enmarca en un [plan de proyectos] gestionados de forma conjunta para maximizar los resultados.

Como soporte a este [plan de proyectos], [EJIE] en el año 2024 ha contratado una [Oficina Técnica NIK/NIRE] (EJIE-145-2023) que ha empezado a trabajar en [Mayo 2024] y que tiene el siguiente [alcance]:

Gestión	- Secretaría técnica - PMO supportive alineada con la PMO PRTR	- Apoyar en la relación con las [administraciones] - Apoyar en la gestión de los [proyectos] del [programa]
Conceptualización	- Diseño de la marca - Creación y gestión de la hoja de ruta - Diseño de servicios	- Crear la [marca] y el [branding] del [producto] (o productos) <i>[NIRE] o [NIK] de momento son "ámbitos" de trabajo y NO tienen por qué ser [marcas]</i> - Trabajar con las [administraciones vascas] en tener un [calendario] con compromisos para incorporar [servicios] en [NIK-NIRE] - Diseñar los [productos] de forma colaborativa (co-creación) con todas las [administraciones]
Ejecución (soporte a proyectos NIRE)	- Soporte experto funcional - Soporte experto técnico-tecnológico - Soporte experto en user experience - Soporte experto legal	- Proporcionar [soporte técnico / funcional] en diferentes áreas a: - Los [proyectos] del [programa] - Las [administraciones]
Gestión del cambio	- Difusión - Sitio web del desarrollador/a - Soporte y asistencia a iniciativas que se integran con NIRE y NIK	- Hacer difusión del [proyecto] (NO del [producto]) y sus objetivos - Crear un [sitio web del desarrollador] con toda la documentación y entornos de [sandbox]

El presente proyecto [NIRE-Interop] es la base responsable de *obtener* los [datos] de las [administraciones] que permitirán construir a continuación las [interfaces de usuario] (UI) web y móvil del [producto] que se está diseñando de forma colaborativa entre las [administraciones vascas] con la ayuda de la [OT NIK-NIRE]

En [expedientes de contratación] futuros diferentes a este se contratará la construcción de estas [interfaces de usuario] web y móvil

[NIRE-Interop] proporcionará los datos a las [UI] web y móvil



La [Oficina Técnica NIK-NIRE] está financiada por el [Mecanismo de Recuperación y Resiliencia] (fondos NEXT)

El presente proyecto [NIRE-Interop] NO está financiado con [fondos NEXT]

2.2 Contexto de [EJIE]

La ley establece a [EJIE] como el [órgano gestor tecnológico] del [Gobierno Vasco] que facilita la digitalización de los servicios públicos y garantiza la calidad, seguridad y continuidad de las tecnologías de la información y la comunicación que los soportan. Por ello, el [Gobierno Vasco] encarga a [EJIE] aquellos proyectos que le competen en materia [TIC] y en particular *-y en lo que se refiere al presente expediente de contratación-*, los [proyectos] del [programa de proyectos] que se deriva de:

- El [PETIC] (que próximamente será revisado para crear el nuevo [Plan de Transformación Digital para el Sector Público de la CAE])
- La [Atención integral multicanal a la ciudadanía y el acceso a los servicios públicos por medios electrónicos](#)

Dentro de [EJIE], la [Sub-Dirección de Administración Digital], es el área que dentro de la dirección de [Soporte al Negocio], analiza, construye, despliega y dinamiza las iniciativas y [proyectos] para impulsar los [servicios electrónicos] para la ciudadanía utilizando los enfoques TIC más innovadores con el objetivo final de avanzar en la [transformación digital] de la Administración y que en concreto será responsable del presente expediente de contratación.

El área de [Soporte al Negocio] de [EJIE] tiene dos sub-direcciones que son importantes en el contexto del presentar [proyecto]:

Transformación Digital

- Proporciona soporte técnico a la [Oficina del Dato]
- Es responsable de la [Oficina de Proyectos de Transformación Digital] (OP-TX) que ofrece servicios a todos los proyectos en el marco de:

- La [inversión 3] del [componente 11] (C11.I3) del [PRTR]

LE1	Administración orientada a la ciudadanía
LE2	Operaciones inteligentes
LE3	Gobierno del dato
LE4	Infraestructuras digitales
LE5	Ciberseguridad

- El [Plan Estratégico TIC] (PETIC 2021-2024) liderado por la [Dirección de Tecnologías de la Información y la Comunicación] (que próximamente será revisado para crear el nuevo [Plan de Transformación Digital para el Sector Público de la CAE])

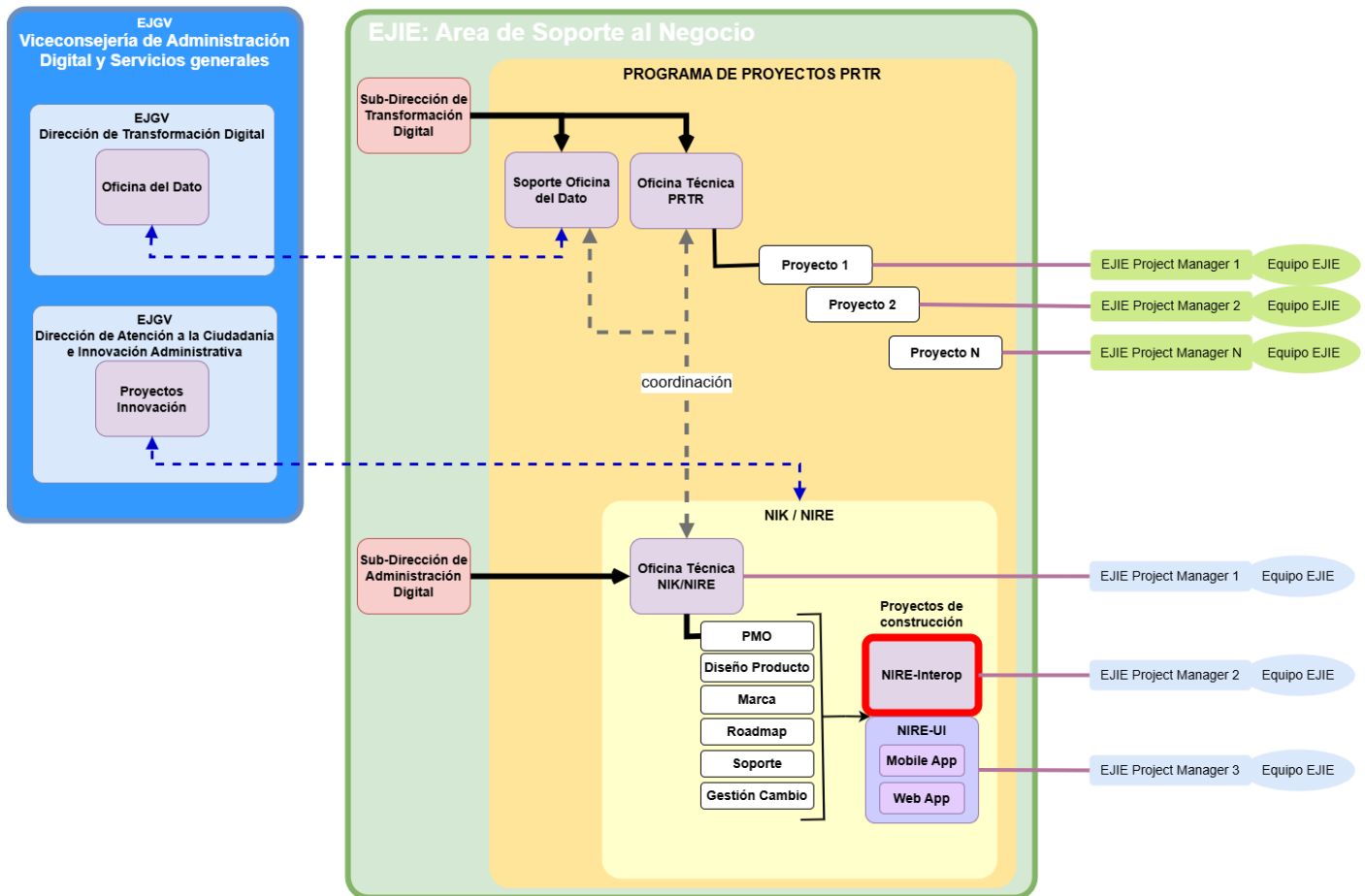
Administración Digital

- Responsable de los sistemas comunes de la [Administración Digital]:
 - Presencia Web
 - Tramitación Electrónica
 - Atención a la Ciudadanía
 - Interoperabilidad con otras administraciones, entidades financieras, etc
 - Transparencia
 - OpenData
- Impulsa el [Observatorio de la Administración Digital]
- Impulsa los proyectos del [programa NIK-NIRE] que se enmarcan en la [Línea Estratégica 1] (Administración Orientada a la Ciudadanía) del C11.I3 del [PRTR] y para cuyo impulso se contrató la [Oficina Técnica NIK/NIRE] (EJIE-145-2023)



Este [expediente de contratación] **NO está financiado con [fondos NEXT]** pero forma parte del [programa de proyectos NIK-NIRE] cuya [Oficina Técnica] sí que ha recibido [financiación MRR].

El siguiente diagrama resume el **contexto** en el que se desarrolla el presente [proyecto] (*señalado en rojo*)



Específicamente:

- El [proyecto NIRE-Interop], utilizará los servicios contratados en la [Oficina Técnica NIK/NIRE] (EJE-145-2023) para:
 - Gestión del proyecto: PMO
 - Obtener soporte funcional / técnico
 - Coordinar la relación con la [Oficina de Proyectos de Transformación Digital] (OP-TX), responsable del reporte de los proyectos financiados con [fondos europeos MRR=Mecanismo de Recuperación y Resiliencia]
 - Coordinar la relación con la [Oficina del Dato]
 - Coordinar la relación con el [Observatorio de la Administración Digital]
- Cada uno de los proyectos del [programa de proyectos NIK-NIRE] será **liderado por un [responsable de proyecto] de [EJE]** normalmente adscrito funcionalmente al [Área de Soporte al Negocio]

3 Descripción del proyecto y los [productos] a construir

En el presente punto se hace una descripción de **lo que se sabe del [producto] a construir en este momento**, después de unos meses de trabajo conjunto en [diseño de producto] con todas las [administraciones vascas].

El conocimiento actual NO es completo y con total seguridad durante la fase inicial de diseño y en los años restantes del [proyecto], durante la ejecución del presente [expediente de contratación], aparecerán [cambios] cuyo impacto habrá que manejar con una adecuada [gestión de riesgos].

En cualquier caso, en este momento se tiene un conocimiento del [producto] suficiente como para que una empresa pueda hacer una **estimación del esfuerzo que supone la construcción** y para ello, en este apartado se detallan a un nivel de abstracción medio-alto los **componentes del sistema** y para cuya construcción se requiere de la ejecución del [proyecto NIRE-Interop].



La descripción NO pretende (ni es posible en este momento) ser precisa (*exacta*) o exhaustiva (detallar el 100% de funcionalidad o detalles técnicos o escenarios / casos que se pueden dar)

Los objetivos de este punto son:

- Describir a un nivel medio-alto el sistema para que la empresa ofertante entienda el problema y la solución diseñada para que pueda hacer una oferta técnica detallada y una estimación lo más ajustada posible
- Empezar con el trabajo de construcción tan pronto como sea posible

Durante el tiempo que se las [administraciones vascas] llevan trabajando en el [proyecto] se ha acumulado un conocimiento que se entiende que posibilitará un inicio de proyecto y ejecución más rápida.

En este punto se describirán:

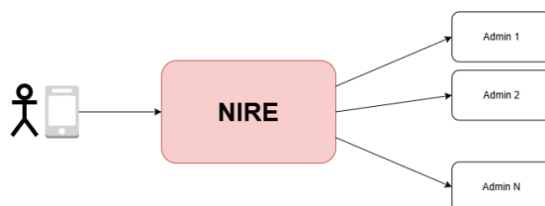
- Visión de alto nivel de la interoperabilidad
- CORE de la interoperabilidad persona – administración
- Identidad y autenticación
- Datos del sistema: monitorización / observabilidad, auditoria y datos analíticos
- Consentimientos
- Datos que se interoperan
- Interfaz de usuario para las personas administradoras del sistema
- Mensajería PUSH

3.1 Visión de alto nivel de la arquitectura de interoperabilidad

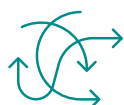
La parte **[NIRE] (datos)** del [proyecto NIK/NIRE] se *sustancia* en una [app móvil] / [web] que va a permitir a las personas consultar **SUS datos** en las [Administraciones Vascas], entre otras muchas cosas:

NIRE Datuak Datos que la administración “tiene” sobre las personas	▪ Datos básicos: identificación / contacto / bancarios ▪ Apoderamientos / representaciones ▪ Carnets / Autorizaciones: <i>familia numerosa, manipulador de alimentos, pesca, etc</i> ▪ Certificados: matrimonio, pareja de hecho, fiscales, penales, discapacidad, familia numerosa, etc ▪ Credenciales / títulos de formación ▪ Inscripción como demandante de empleo ▪ ...
NIRE Karpeta Datos asociados a [expedientes]	▪ Expedientes con cualquier Administración (<i>ayudas/subvenciones, premios, autorizaciones, etc</i>) ▪ Documentación registrada ▪ Notificaciones ▪ Pagos ▪ Multas ▪ Procesos de selección pública (OPEs) ▪ ...
Calendario	▪ Citas con diferentes servicios ▪ Caducidad de registros, carnets, etc ▪ Fechas límite para presentar una ayuda, hacer un pago pendiente, presentar impuestos, etc ▪ Fechas de exámenes ▪ Devolución de préstamos bibliotecarios ▪ Reserva de instalaciones deportivas municipales ▪ ...
Servicios	▪ NIRECard ▪ Transportes ▪ Préstamos bibliotecarios ▪ Reserva de instalaciones deportivas municipales ▪ ...

A nivel técnico, en una primera visión de muy alto nivel, [NIRE] es fundamentalmente un **[sistema de interoperabilidad ciudadanía – administración]**:



Básicamente [NIRE] es un **[hub]** que *distribuye* múltiples [peticiones de datos] desde la [app] de la persona usuaria a las [administraciones] correspondientes. [NIRE] por lo tanto “simplemente” *proporciona* SUS datos en las [administraciones] a las personas usuarias *propietarias* de los mismos.



Es importante **NO confundir [NIRE] con [NISAE]** (*nodo de interoperabilidad de las administraciones vascas*)

- **NISAE** **[interoperabilidad administración – administración]** para automatizar y simplificar procesos de la [administración]
- **NIRE** **[interoperabilidad ciudadanía – administración]** para que las personas tengan acceso a todos SUS datos en cualquier [administración]

[NIRE] tiene **dos principios básicos**:

NO se almacenan datos de las personas en [NIRE]



[NIRE] **NO** es una [DB] que “contenga” todos los datos de las personas procedentes de las [administraciones vascas]

[NIRE] **NO** almacena ningún dato de la persona; simplemente **hace de “intermediario”** entre la persona y la [administración] **SIN almacenar los datos que se intercambian**.

Ej: Si una persona en su [app] quiere consultar el estado de SUS [expedientes] en las [administraciones], la [app] hará una llamada a [NIRE] que se encargará de **recolectar** datos de [expedientes] en todas las [administraciones] para enviarlos de vuelta a la [app] **SIN almacenar ningún dato relevante**



Las únicas excepciones a este principio son:

- Los datos del [perfil NIRE]: datos de contacto “curados” por la propia persona usuaria *(en cualquier caso, aún está pendiente de definir definitivamente si va a existir un [perfil NIRE])*
- Consentimientos
- Otros datos comunes que se puedan identificar durante la ejecución del proyecto



[NIRE] NO sustituye a las [sedes electrónicas] de las [Administraciones Vascas]

Las [app móvil] y [web] de [NIRE] simplemente son un **acceso común a los [datos]** de la persona en las [administraciones vascas]: en [NIRE] una persona **puede VER** por ejemplo que:

- Tiene a su disposición una [notificación] de una [administración]
- Ha ocurrido algún cambio en el estado de un [expediente] en tramitación en una [administración]
- Tiene una multa de [tráfico]
- Puede descargarse el [carnet de familia numerosa]
- ...

...si a partir de esta información “de cabecera” de [NIRE], la persona necesita ampliar la información:

- Acceder al detalle de la [notificación]
- Ver el detalle del [expediente]
- Ver la multa de [tráfico]
- Descargarse el [carnet de familia numerosa]
- ...

... **será redirigido desde [NIRE] a la [sede electrónica] de la [administración] correspondiente**



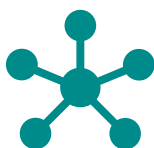
Obviamente, la persona **NO tendrá que identificarse de nuevo en la [sede electrónica]** ya que “viene identificada” de [NIRE]



El concepto [NIRE] es un primer paso dentro de un camino más largo y con objetivos más ambiciosos.

[NIRE] sin embargo, sienta las primeras bases al ofrecer servicios comunes a la ciudadanía que en esta primera fase se centran en el **acceso a los [datos]**, aunque **se incorpora algún elemento de transaccional** como la posibilidad de *solicitar* el cambio de [datos básicos] de domicilio o cuenta bancaria en varias [administraciones] desde un sitio común (NIRE)

A partir de este primer hito, poco a poco se avanzará en ofrecer servicios más transaccionales



Otro aspecto importante en el que [NIRE] puede jugar un papel relevante es la **interoperabilidad con los sistemas de la [Administración General del Estado] (AGE)**

Las [administraciones vascas] tienen la voluntad (*y en muchos casos la obligación*) de *sindicar* datos con sistemas de la [Administración General del Estado] (AGE)

- Catálogo de Servicios en el [SIA]
- Notificaciones a [DEHÚ]
- Apoderamientos / representaciones / autorizaciones en [Apodera]
- Registro en [SIR]
- Datos abiertos [opendata] en [datos.gob]
- etc

Para hacer esta sindicación, las [administraciones] tienen dos alternativas:

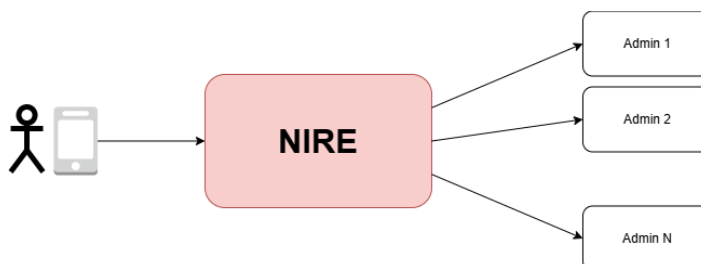
1. Trabajar **independientemente** en las diferentes *sindicaciones* con la [AGE]
2. Trabajar en **común** creando [puntos comunes] de *sindicación* de los [datos] en el ámbito de [euskadi] que posteriormente se *sindican* en la [AGE] de forma que:
 - a. Se pueden dar servicios comunes a nivel *local* en [euskadi]
 - b. Se *sindica* en la [AGE] desde un único sitio simplificando esta integración y su mantenimiento para las dos partes

[NIRE] es una “pieza” más en estos [servicios comunes] que pueden *facilitar* la *sindicación* de algunos [datos] en la [AGE]

A continuación, se detalla la solución técnica que *sustenta* estos dos principios básicos:

3.2 CORE de interoperabilidad persona – administración en [NIRE]

El primero de los [principios básicos] de [NIRE] es que **NO se almacenan datos en [NIRE]** así que, en principio, **cada vez** que la persona “pide” [datos] (*expedientes, notificaciones, multas...*) **hay que “consultar”** a los [orígenes de datos] en las diferentes [administraciones] por estos datos:



... esta aproximación técnica, por razones obvias **NO es eficiente**, así que hay “optimizarla” utilizando al menos dos estrategias:

1 Device LOCAL cache

El dispositivo que utiliza la persona (*móvil / web*) utilizará una [cache local] para almacenar datos y **evitar consultar a los [orígenes de datos]** si no ha habido cambios desde la última consulta.

[NIRE] proporcionará mecanismos para “**validar**” la [cache local] teniendo en cuenta la “naturaleza” del [dato]:

- | | | |
|---|---|--|
| <ul style="list-style-type: none"> ▪ Hay datos que NO cambian y como mucho únicamente “expiran” (<i>tienen una validez limitada</i>) como un [carnet de pesca] | ➔ | <p>NO tiene sentido “validar” nada contra [NIRE]: el [dato] estará disponible mientras sea válido</p> <p>Ej: el [carnet de pesca] aparecerá en [NIRE] mientras sea válido</p> |
| <ul style="list-style-type: none"> ▪ Hay datos que cambian (<i>evolucionan</i>) con el tiempo como, por ejemplo, los [expedientes] | ➔ | <p>Es necesario “consultar” contra [NIRE] si ha habido algún cambio en el [dato]</p> <p>Ej: el [expediente] cambia de estado</p> |



Esta aproximación es la que utilizan muchas aplicaciones como [whatsapp] o [linkedin] que mantiene en una [db local] las conversaciones que se sincronizan cuando se “abre” la [app móvil] o [web]

2 Reglas para minimizar las consultas a los [orígenes de datos] en las [administraciones]

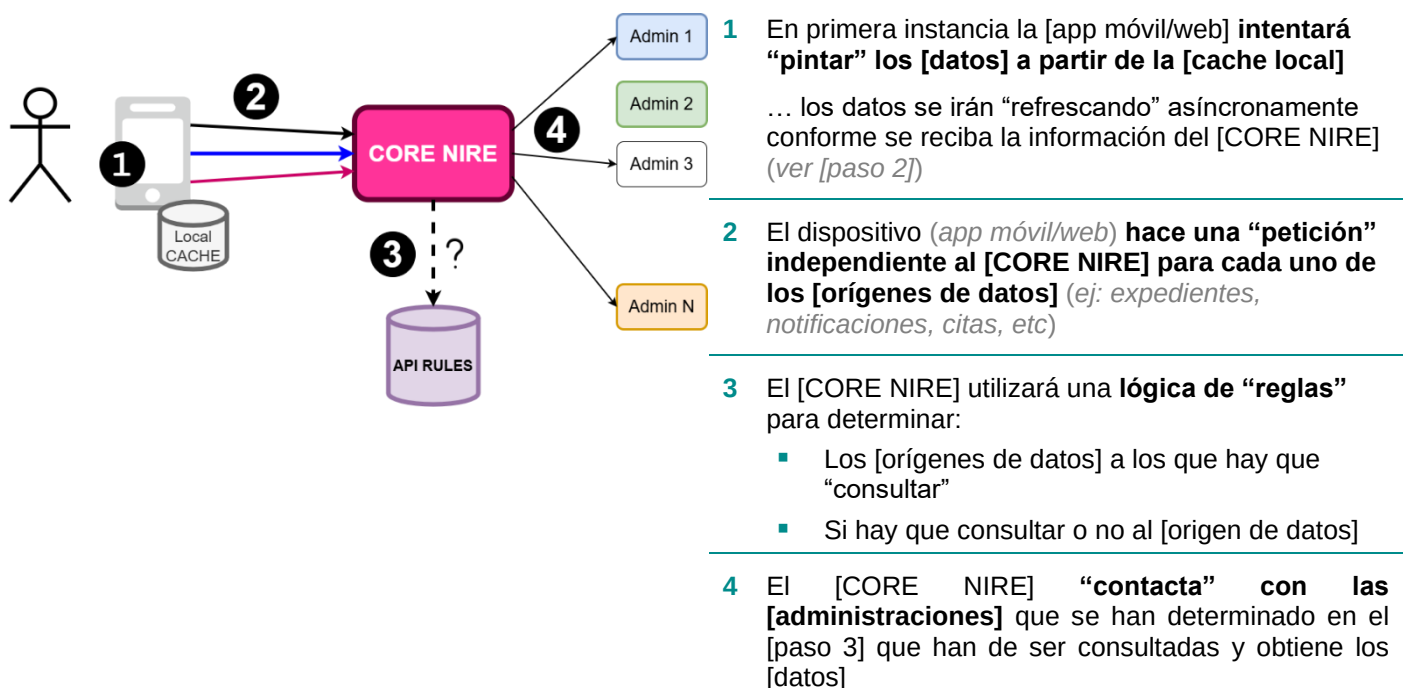
Si es necesario consultar los [orígenes de datos] hay que tener en cuenta que **NO tiene sentido hacerlo para todos los disponibles** ya que:

- NO todas las [administraciones] tienen datos de una determinada “naturaleza” sobre una persona ya que **no todas las [administraciones] son competentes**
Ej: [certificados de familia numerosa] que son competencia del [Gobierno Vasco] o [permisos de estacionamiento] que son competencia de [ayuntamientos]
- Una persona **NO tiene datos en todas las [administraciones]**
Ej: Una persona solo tendrá [datos] en un uno o unos pocos [ayuntamientos] o en una [diputación foral]
- El [dato] **NO se ha actualizado**
Ej: El [expediente] **NO ha cambiado de estado**

En definitiva, hay que utilizar [estrategias] de optimización y minimizar las [consultas] a las [administraciones] y evitar “consultar” indiscriminadamente a todas las [administraciones] o “consultar” si no es necesario.

Es importante recordar que en el [CORE NIRE] **NO se almacenan datos**: únicamente se [cachean] localmente en el [dispositivo cliente] de la persona usuaria

Una primera aproximación del funcionamiento del sistema sería el que se muestra en el siguiente gráfico:



En una segunda aproximación, en realidad el [dispositivo] cliente hará **dos llamadas** al [CORE NIRE] para obtener los [datos] de cada [origen de datos]

1 Initialization

El [dispositivo] hace una **primera invocación** al [CORE NIRE] en la que incluirá:

- El [identificador de la persona] (*personId*)
- Los OID de cada uno de los [datos] que el [dispositivo] tiene en la [cache local]



El [CORE NIRE] asignará un [identificador único] (OID) a cada uno de los [datos] (*cada expediente, cada notificación, cada carnet, etc*)

La [cache local] en el [dispositivo] contendrá una [table key-value] en la que:

Key = [identificador único] (OID) del [dato] asignado por [NIRE] (*dataOID*)

Value = el [dato], típicamente en formato JSON y que será utilizado por la [app] para “pintarlo” en la [UI]

Es importante recordar de nuevo que el *value* (*el dato*) nunca “sale” del [dispositivo] y nunca está en el [CORE NIRE] (*NIRE NO almacena datos*)

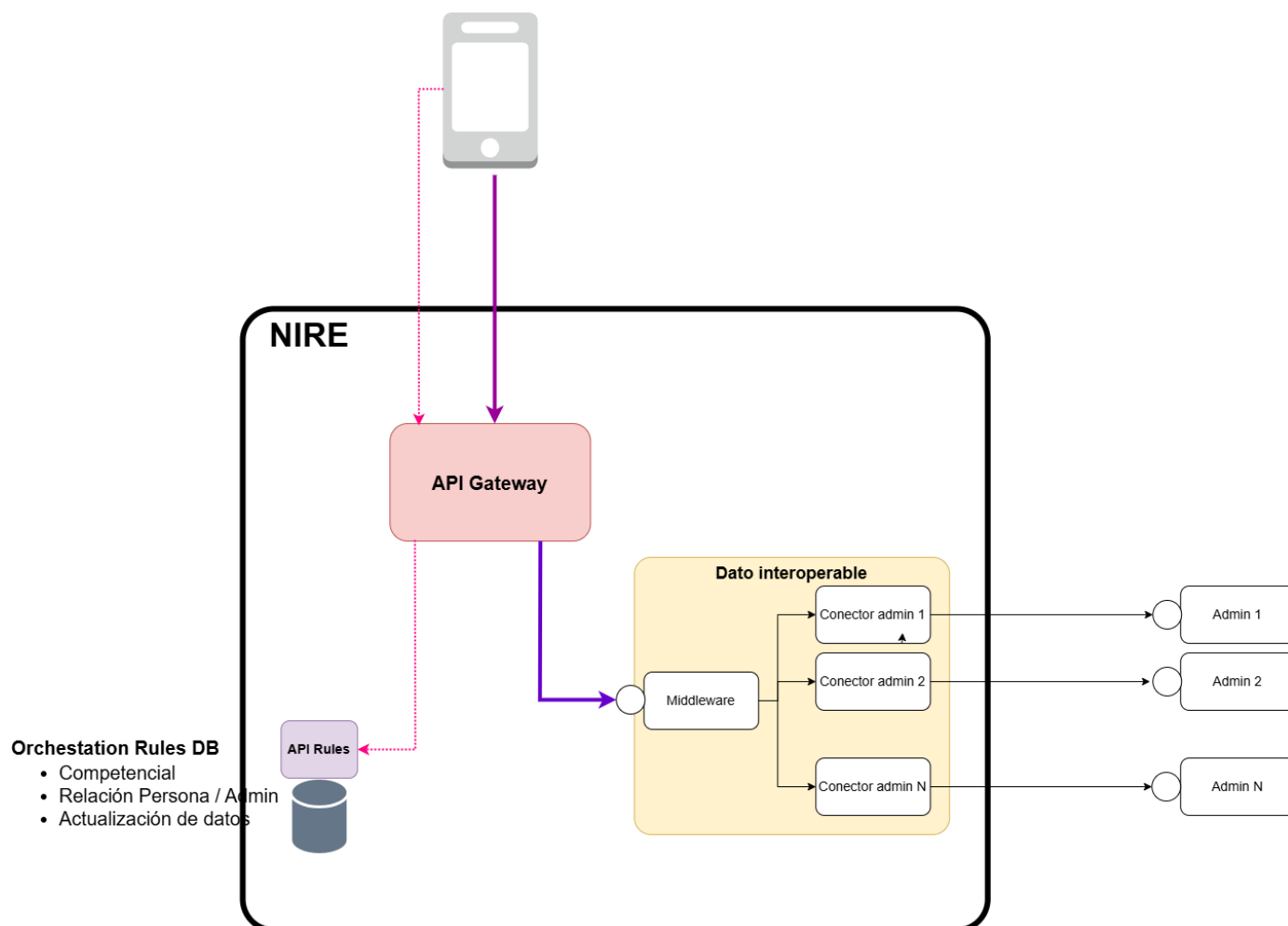
... con esta información, el [CORE NIRE] es capaz de **discriminar a qué [orígenes de datos] se deben invocar en un segundo paso (*retrieve*) desde el [dispositivo] para obtener los [datos] nuevos o actualizados** de forma que la respuesta a esta llamada de inicialización es *simplemente* una **lista de [datos interoperables] y [administraciones] que son [origen de datos] a las que hay que llamar en el siguiente paso con el objetivo de recuperar los [datos] en sí.**

2 Retrieve

Una vez que el [dispositivo] “sabe” qué [orígenes de datos] y [administraciones] tienen datos / cambios para la persona, **el [dispositivo] hace una petición independiente** para cada [origen de datos] para recuperar los [datos]

... y finalmente “pintarlos”

Enfocando un poco más en el detalle de la [arquitectura] del sistema:



Los componentes a destacar en el esquema anterior son:

3.2.1 API Gateway

Gestiona las [peticiones] que *llegan* desde los dispositivos de las personas usuarias y en concreto es responsable principalmente de:

- **Autenticar** al cliente y verificar la **autorización** para realizar la llamada (*ver más adelante en este documento*)
- **Controlar el [rate limit]** (*límite en el número de llamadas desde un mismo dispositivo en un rango de tiempo*)
- **Orquestar la llamada al [middleware]** de cada uno de los [orígenes de datos]
- **Cachear** datos
- **Registrar datos** de [audit] / [monitoring] / [observability] / [log]



Como solución [API Gateway] se utilizará un [producto] que se determinará junto con [EJIE] y la [Oficina Técnica NIK-NIRE] como [WSO2](#) o [Kong](#), dando prioridad a los productos de [código abierto] y que no requieran [licencia de uso] e impliquen un coste recurrente futuro.

3.2.2 Middleware + conectores

Cada uno de los **[datos interoperables]** de **[NIRE]** (*expedientes, notificaciones, multas, carnet de pesca, préstamos bibliotecarios, etc*) tendrá un **[middleware] propio** responsable de **orquestrar las peticiones para cada [origen de datos]**

En este punto hay que tener en cuenta que:

- A** El [middleware] “devuelve” los [datos] al [API Gateway] y este al [dispositivo] en un **formato estándar** definido ad-hoc para cada tipo de [dato]



En el ámbito del proyecto se definirá una “semántica” para cada tipo de dato (*un [modelo] y [formato] para cada [dato]*)

- B** Cada [administración] puede exponer los datos de una forma diferente (*ej: una expone un [servicio REST] y otra un [servicio SOAP] o bien una devuelve los datos en un formato diferente al “estándar”*)

... por lo tanto será necesario un **[conector] para cada [administración]** que se encarga de:

1. “**llamar**” al [origen de datos] en la [administración]
2. “**transformar**” los [datos] devueltos al **formato estándar** que espera y *entiende* la [app]

Hay dos tipos de [conectores]:

Conector estándar

La [administración] (*el [origen de datos]*)

1. **Devuelve los [datos] en el formato estándar utilizado por [NIRE]** (*el que devuelve [NIRE] al [cliente]*)
2. Ofrece los [datos] en un [servicio REST] que sigue un estándar [NIRE] (*ej: un servicio REST con una semántica de invocación fijada desde [NIRE]*)

... en este caso, **se puede utilizar el mismo [conector] para cualquier [administración]** ya que NO es necesario que el [conector] haga “nada especial” (*no hay que hacer transformaciones de datos y las llamadas son siempre iguales independientemente de la [administración]*)



Con el [conector estándar] se desarrollarán **[librerías JAVA]** que faciliten al máximo a una [administración] ofrecer un [servicio REST] para un [origen de datos] que se conecte desde [NIRE] con el [conector estándar]

Conector NO estándar

La [administración] NO sigue el estándar [NIRE], por ejemplo:

- *Se devuelve un formato XML y [NIRE] trabaja con JSON*
- *El servicio expuesto es SOAP y [NIRE] trabaja con REST*

... en este caso es necesario **desarrollar un [conector ad-hoc]** para la [administración]

- C** Cada [administración] puede devolver los datos a un *ritmo* diferente (*y alguna puede incluso no devolverlos en un tiempo razonable*)

El [middleware] debe encargarse de gestionar estas condiciones excepcionales junto con el [API Gateway] de forma que el sistema no se *resienta* en su globalidad

3.2.3 Retrieve Rules API & DB

Como se ha introducido anteriormente, las [reglas] que determinan los [orígenes de datos] a los que *consultar* (*retrieve*) inicialmente pueden ser:

a)	Competenciales	Para un [dato interoperable] hay solo una/varias [administraciones] competentes
b)	Relación persona - administración	Una persona NO tiene datos en todas las [administraciones]
c)	Actualización de datos	Solo hay que consultar a la [administración] si el dato se ha actualizado
d)	Última vez que se han recuperado los datos	No consultar los datos en un [origen de datos] si no ha pasado un tiempo X desde que se consultaron

La base del sistema de [reglas] es conceptualmente una **[base de datos]** y **[servicios]** que a muy alto nivel funcionará de la siguiente forma:

- a) **Discriminación competencial** El sistema dispondrá de un **[registro de orígenes de datos]** que relaciona el [dato interoperable] con la [administración] que dispone de [datos] (*ver más adelante*)
- A nivel “conceptual” (para entender el sistema) es algo similar a una [tabla] como:

Dato interoperable	Admin	competente
expedientes	EJGV	true
carnet-pesca	Diputación X	true
...	...	...

La discriminación [competencial] es muy sencilla a partir de este **[registro de orígenes de datos]**

- b) **Discriminación en base a la relación persona - administración** Conceptualmente (para entender el sistema) si existe una [tabla] como:

PersonID	Dato interoperable	Admin	última actualización
person-1	expedientes	EJGV	Mon 2 Dec 2024 (11:05)
person-2	carnet-pesca	Diputación X	Wed 1 Ago 2024 (14:13)
...	...	...	...

... se puede inferir que si NO hay datos en esta [tabla] para una persona en un *par* [origen de datos] / [administración] NO es necesario consultar

- c) **Discriminación en base a la actualización de datos** Cada uno de [datos] (*cada expediente, cada notificación, cada carnet, etc*) tiene un **[identificador único] (OID) asignado por [NIRE]**

- El **[dispositivo cliente]** almacena el [dataOid] asociado al propio [dato] en la [cache local]
- El **[CORE NIRE]** únicamente almacenará el OID (dataOid), el ID del [dato] en la administración origen y algún meta-dato que permita saber si hay cambios y hay que consultar al [origen de datos]

Conceptualmente (para entender el sistema) si se “amplia” la [tabla] utilizada en el [caso b] con dos nuevas columnas:

PersonID	Dato interoperable	Admin	OID dato	ID dato admin	última actualización (enviada por la admin)
person-1	expedientes	EJGV	Oid1	Exp1	Mon 2 Dec 2024 (11:05)
person-2	carnet-pesca	Diputación X	Oid2	Carnet1	Wed 1 Ago 2024 (14:13)
...	...	...	...	...	...

... se puede inferir si es necesario o NO hacer la consulta a la [administración]

d) Última vez que se han recuperado los datos

Esta estrategia *pasa* por NO consultar los datos en un [origen] de datos si no ha pasado un tiempo X desde la última vez que se consultaron

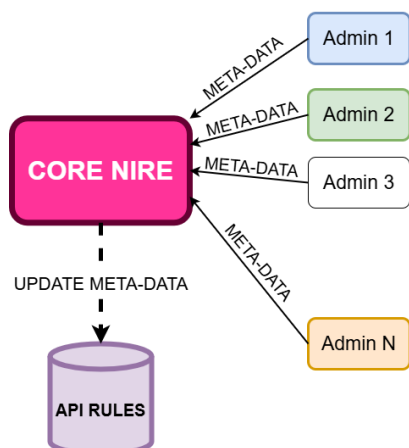
... probablemente este tiempo X dependa del [dato interoperable] (*no es lo mismo un expediente que un certificado*) y del [origen de datos] (*no es lo mismo una [administración] que otra*)

Conceptualmente de nuevo (para entender el sistema) si se “amplia” la [tabla] utilizada en el [caso c] con una nueva columna:

PersonID	Dato interoperable	Admin	OID dato	ID dato admin	última actualización (enviada por la admin)	Última consulta al [origen de datos]
person-1	expedientes	EJGV	Oid1	Exp1	Mon 2 Dec 2024 (11:05)	Mon 7 Ene 2025 (09:00)
person-2	carnet-pesca	Diputación X	Oid2	Carnet1	Wed 1 Ago 2024 (14:13)	Mon 7 Ene 2025 (09:00)
...	...	...	...	...	...	...

... se puede inferir si es necesario o NO hacer la consulta a la [administración]

Como se puede observar de lo descrito, para que el sistema de [retrieve rules] y [cache] en el [dispositivo cliente] funcione correctamente **es necesario que las [administraciones] “propietarias” de los [datos] actualicen periódicamente meta-información sobre los mismos en [NIRE]**



Es necesario que las [administraciones] “envíen” periódicamente [meta-información] sobre la actualización de los [datos] a [NIRE]

... en definitiva, responder a la pregunta:

¿Para una persona X, hay algún [dato] **nuevo** o un **cambio** sobre un [dato] ya existente en [NIRE] (*sobre un expediente, notificación, cita, etc*)?

... y con esto *actualizar* la [meta-información] de la [tabla] anterior:

PersonID	Dato interoperable	Admin	OID dato	ID dato admin	última actualización (enviada por la admin)
person-1	expedientes	EJGV	Oid1	Exp1	Mon 2 Dec 2024 (11:05)
person-2	carnet-pesca	Diputación X	Oid2	Carnet1	Wed 1 Ago 2024 (14:13)
...	...	...	...	...	...

Para que el [CORE NIRE] “reciba” esta [meta-información] son posibles varias **estrategias** que se describen a continuación utilizando el ejemplo del [dato interoperable] de [expedientes] asociados a [procedimientos administrativos]:

Admin-PUSH ONLINE

La [administración] “**proactivamente**” *envía* on-line (*casi al momento*) la [meta-información] de actualización del dato a [NIRE]

Cuando los sistemas [back-end] de la [administración] *detectan* un cambio en un [dato] asociado a una persona X, *simplemente* enviarán [meta-información] a [NIRE]:

PersonID	ID dato admin	acción
person-1	Exp1	UPDATE DATA

Esta estrategia:

- Está “gobernada” por la [administración]: la actualización en [NIRE] es tan rápida como lo es la [administración] en enviarla
- Se basa en micro-actualizaciones, frecuentemente de un solo [dato] (*ej: de un solo [expediente]*)
- Es más compleja de implementar para la [administración]

NIRE-PULL ONLINE

La [administración] “**reactivamente**” (cuando el [CORE NIRE] lo solicita) *envía* on-line a [NIRE] la [meta-información] de actualización del dato

[NIRE] periódicamente **consulta** a la [administración] sobre si hay algún [dato] nuevo o cambio en uno ya existente en [NIRE]

PersonID	ID dato admin	acción
person-1	Exp1	UPDATE DATA
Person-1	Exp2	CREATE DATA

Esta estrategia:

- Está “gobernada” por [NIRE]: la actualización depende de la frecuencia con la que [NIRE] consulte a la [administración]
 Esta frecuencia puede modularse en función de factores como la frecuencia con la que se “conecta” la persona a [NIRE], el volumen de datos del origen o su naturaleza
- Dado que las actualizaciones son menos frecuentes puede ser que se envíe información de varios [datos] asociados a una misma persona (*ej: más de un solo expediente*)
- Es más sencilla de implementar para la [administración]

NIRE-PULL BATCH

La [administración] “**reactivamente**” *envía* off-line (batch, cada cierto tiempo) la [meta-información] de actualización a [NIRE]

[NIRE] expone un punto (*ej: un servicio*) donde la [administración] puede enviar de forma [batch] los cambios producidos en un periodo de tiempo (*cada [administración] decide cuál*)

PersonID	ID dato admin	acción
person-1	Exp1	UPDATE DATA
Person-1	Exp2	CREATE DATA
Person-2	Exp4	UPDATE DATA

Con esta estrategia:

- Está “gobernada” por [NIRE]: la actualización depende de la frecuencia con la que [NIRE] consulte a la [administración]
 Esta frecuencia puede modularse en función de factores como el volumen de datos del origen o su naturaleza
- Dado que las actualizaciones son menos frecuentes puede ser que se envíe información de varios [datos] asociados a múltiples personas
- Es la más sencilla de implementar para la [administración]

Estos mecanismos de actualización de meta-data desde las [administraciones] a [NIRE] **son la parte más compleja del sistema** puesto que requieren de cierto trabajo en las [administraciones].

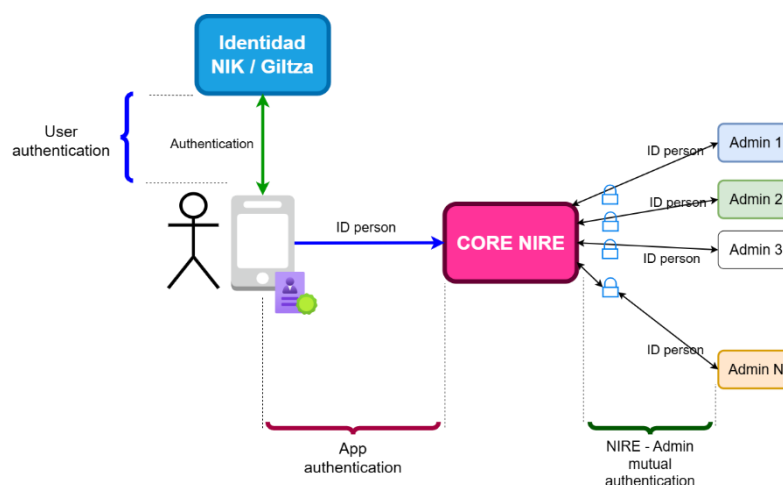
En cualquier caso, es mucho **más sencillo** enviar a [NIRE] únicamente “**cambios de estado**” en los [datos] que “todo” el [dato] y almacenarlo en un *enorme* [data lake] en [NIRE].

3.3 Identidad y autenticación

En este punto es importante diferenciar entre:

Concepto		Descripción	Qué sistemas pueden ser utilizados en [NIRE]
Identidad	Identity	La persona y sus atributos / meta-datos	BAK / BAKQ (<i>Izenpe</i>) DNI Certificado FNMT
Autenticación	Authentication (AuthN)	Verificar quién es la persona que quiere entrar a un sistema verificando la [identidad]	Giltza (<i>Izenpe</i>) Clave
Autorización	Authorization (AuthZ)	Verificar si la persona autenticada puede o no puede realizar una acción determinada en un sistema	--

A partir de aquí, la visión general de la *autenticación* en el sistema se muestra en el siguiente gráfico:



Hay que destacar tres áreas conceptuales en este gráfico:

User authentication	Las personas usuarias se autentican utilizando un sistema de [identidad] / [autenticación] como [Giltza] (o [NIK] <i>posiblemente en un futuro</i>) Con la autenticación obtenida, la persona es identificada en [NIRE] (<i>se tiene la certeza de quién está interactuando</i>) creándose una <i>sesión</i> perdurable en el [dispositivo cliente] (móvil o web) que permite utilizar (<i>autoriza</i>) a utilizar los servicios [NIRE]
App Authentication	La [app] (móvil / web) debe autenticarse en el [CORE NIRE] para <i>solicitar</i> [datos] (<i>que a su vez el [CORE NIRE] solicita a la [administración] correspondiente</i>) Esta autenticación [app] < - > [CORE NIRE] puede simplemente <i>basarse</i> en la [autenticación] de persona usuaria anterior
NIRE – Admin mutual authentication	El [CORE NIRE] y las [administraciones] intercambian [datos] invocando mutuamente [servicios] que exponen [NIRE] y las [administraciones]. Para asegurar que este intercambio de [datos] es seguro es necesaria una autenticación mutua: - Las [administraciones] deben tener certeza de que es [NIRE] que quién está <i>llamando</i> a los [servicios] [NIRE] debe tener certeza de que es una [administración] <i>legítima</i> quién está <i>llamando</i> a los [servicios]

Es muy importante entender que esta [autenticación] mutua [NIRE] ↔ [Admin] **NO se basa en la [autenticación] de la persona usuaria**

Para intercambiar [datos] simplemente [NIRE] y la [Administración] han de “reconocerse mutuamente”, **independientemente de la persona autenticada en el [dispositivo cliente]**.

Obviamente la [identidad] de la persona autenticada en el [dispositivo cliente] será un **parámetro de entrada a los [servicios]** expuestos por las [administraciones]

Ej: para que una administración devuelva los [expedientes] de una persona será necesario facilitar un [identificador de la persona] (*dni, nie...*)

En palabras más técnicas: **para interoperar, a nivel técnico, la [autenticación] de la persona en [NIRE] NO se extiende a la [administración] proveedora de los [datos]** (*no tiene por qué utilizarse el [token] de [autenticación de persona usuaria] en el [dispositivo cliente] para autenticar el [CORE NIRE] en un servicio de una [administración]*)

Otra cosa **diferente** es que **cuando la [persona usuaria] quiere tener más información sobre un [dato] que ve en [NIRE] será redirigida desde el [dispositivo cliente] a la [sede electrónica] de la [administración] correspondiente y en este caso SI serán necesario extender la [autenticación] del [dispositivo] a la [sede electrónica]**



La [autenticación] en todas las áreas detalladas:

- User authentication
- App authentication
- [CORE-NIRE] <-> [admin] mutual authentication
- Extensión de la [autenticación] en el [dispositivo cliente] a la [sede electrónica] de la [administración] correspondiente

es uno de los puntos **más críticos del sistema** y se estudiará y trabajará en detalle con todas las partes implicadas:

- Adjudicatario del [expediente de contratación]
- Oficina Técnica [NIK-NIRE]
- IZENPE
- EJIE (*todas las áreas afectadas*)

En el presente punto se exponen algunas soluciones en las que se ha empezado a trabajar **en las que hay que profundizar y seguir trabajando en la solución final**

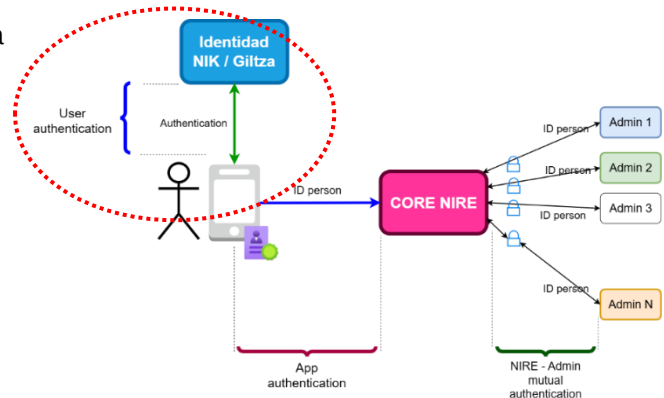
El objetivo de esta detallada descripción es doble:

- Que la empresa ofertante *entienda* la complejidad del sistema
- Proporcionar toda la información disponible para que la empresa ofertante tenga más claves para ajustar la oferta

A continuación, se detallan cada uno de estos aspectos:

3.3.1 User Authentication: Autenticación en la app / web [NIRE]

Este punto se centra en la [autenticación] de la persona usuaria en la aplicación web / móvil



Como se ha introducido, [NIRE] **delegará** la [identidad] en [IZENPE], [DNI] o cualquier [certificado] reconocido y la [autenticación] en un sistema como [Giltza], (en un futuro posiblemente localmente en [NIK]) o [clave]



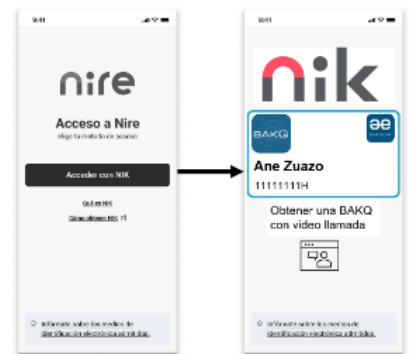
[NIK] es esencialmente un [wallet] en el que se pueden *custodiar* [credenciales] (de [identidad] y otras)

Actualmente [NIK] utiliza [Giltza] de [izenpe] para [autenticarse] y obtener una primera [credencial de identidad] basada en [BAQK] que puede utilizarse en otros sistemas para obtener más [credenciales] (*tarjeta sanitaria, credencial de familia numerosa, etc*)

[NIK] forma parte del alcance del [programa de proyectos] global y en este ámbito evolucionará y se adaptará a los objetivos del [programa]

En una primera *visión* a nivel de usabilidad la aproximación sería:

- 1 La persona en un [wallet] (NIK) obtiene una [credencial de identidad] (por ejemplo basada en [BAQK]); esta [credencial de identidad] será utilizada más adelante para [autenticarse] en [servicios digitales]
- 2 Cuando la persona entra en [NIRE] se le ofrece **únicamente** la opción de utilizar una [credencial de identidad] del [wallet] (NIK)
- 3 Se “abre” [NIK] y la persona usuaria selecciona una [credencial de identidad] con la que quiere “entrar” en [NIRE]
- 4 Una vez que la persona se ha [autenticado] y obtenido una [identidad] en [NIRE] **no debería tener que volver a utilizar [NIK]** y para entrar de nuevo a [NIRE] bastaría con utilizar un [PIN] o un [factor biométrico] local al [dispositivo]



Una vez que la app [NIRE] “tiene” una [identidad] puede utilizar los [servicios de interoperabilidad] para obtener los [datos] de los diferentes orígenes de datos.



La descripción de la interacción anterior *asume* que existen dos [app] diferentes (NIK y NIRE), algo que aún está pendiente de definir, de la misma forma que las [marcas] (NIK y NIRE)

Otra opción para [autenticarse] en [NIRE] es *simplemente* utilizar [Giltza] o [clave], algo que NO se descarta totalmente.



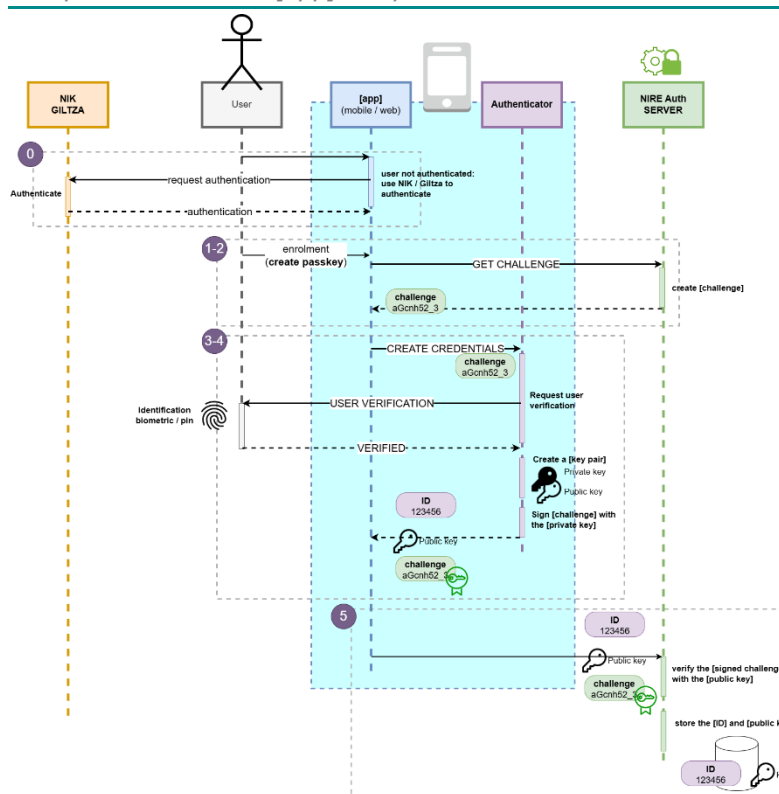
En todo caso, una vez [autenticada] la persona usuaria, la [app] (web / móvil) [NIRE] tiene la [identidad] de la persona que está interactuando con el sistema.

La persona usuaria NO debería volver a tener que autenticarse durante un tiempo considerable (ej: 1 mes o más) y para volver a acceder a la [app] (web / móvil) debería bastar con utilizar un factor local (biométrico, pin, etc)

La solución para NO tener que “pasar” por el proceso de autenticación en [NIK] / [Giltza] cada vez que se abre [NIRE] se definirá en la ejecución del proyecto trabajando con la [Oficina Técnica NIK-NIRE], [EJIE] e [IZENPE]

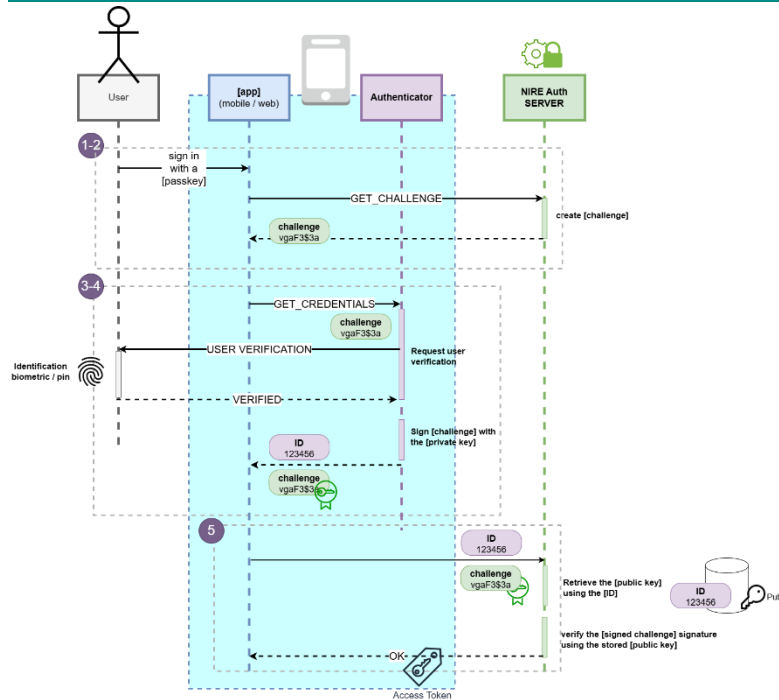
Una opción posible es utilizar [passkeys] (detalles técnicos [1] y [2]) que a muy alto nivel funciona así:

FASE I: creación del [passkey] durante el enrollment en la [app] (cuando se instala la [app] en el móvil o la primera vez que se entra en la [app] web)



- 0 La persona usuaria se autentica utilizando [NIK] o [Giltza] (o cualquier otro servicio de [autenticación]) -estar autenticado es requisito previo a crear un [passkey]-
- 1 La [app] en el [dispositivo] hace una petición [GET CHALLENGE] al [servidor NIRE] que devuelve un [challenge]
- 2 La [app] en el [dispositivo] llama a la función [CREATE_CREDENTIALS] del componente [authenticator] (que está también en el [dispositivo]) pasándole el [challenge] recibido del [servidor NIRE]
- 3 El componente [authenticator] requiere la identificación de la persona usuaria (biométrica / pin)
- 4 El componente [authenticator]:
 - a) Crea una [pareja de claves] (pública y privada)
 - b) Firma el [challenge] con la [clave privada]
 - c) Crea un [ID] asociado a la persona (credential ID)
 ... y devuelve a la [app] como respuesta a la llamada [CREATE_CREDENTIALS] del [paso 2]:
 - El [ID] asociado a la persona
 - La [clave pública]
 - El [challenge firmado] con al [clave privada]
- 5 La [app] envía todo lo anterior al [servidor NIRE] que:
 - a) Verifica con la [clave pública] recibida que el [challenge firmado] (con la [clave privada] en [4]) es válido con lo que “sabe” que la petición es “legítima”
 - b) Guarda el [ID] de la persona asociado con la [clave pública] recibida
 (Este [ID]+[clave pública] será utilizado posteriormente en la [autenticación] con un [passkey] -FASE II-)

FASE II: autenticación con [passkey]



- 1 La [app] en el [dispositivo] hace una petición [GET CHALLENGE] al [servidor NIRE] que devuelve un [challenge]
- 2 La [app] en el [dispositivo] llama a la función [GET_CREDENTIALS] del componente [authenticator] (que está también en el [dispositivo]) pasándole el [challenge] recibido del [servidor NIRE]
- 3 El componente [authenticator] requiere la identificación de la persona usuaria (*biométrica / pin*)
- 4 El componente [authenticator]:
 - a) Devuelve el [ID] asociado a la persona (*credential ID*)
 - b) Firma el [challenge] con la [clave privada] ... y devuelve a la [app] como respuesta a la llamada [GET_CREDENTIALS] del [paso 2]:
 - El [ID] asociado a la persona
 - El [challenge firmado] con al [clave privada]
- 5 La [app] envía todo lo anterior al [servidor NIRE] que:
 - a) Utilizando el [ID] asociado a la persona (*credential ID*) recupera la [clave pública] que almacenó al crear la [passkey] (ver antes)
 - b) Verifica con la [clave pública] recuperada que el [challenge firmado] (con la [clave privada] en [4]) es válido con lo que "sabe" que la petición es "legítima" y se está en posesión del [passkey] y por lo tanto en algún momento inicial fue **autenticado** (con [Giltza] / [NIK]) con lo que se puede *entrar* en la [app]
 - c) Otorga acceso al [usuario] permitiendo usar el servicio a partir de un [token de autenticación] (*jwt*) devuelto

Como se puede observar de la descripción anterior el proceso es:

1. Cuando la persona usuaria se instala la [app] o entra por primera vez en la web [NIRE] se autentica utilizando [Giltza] o [NIK] o cualquier otro sistema de [autenticación]
Justo después de obtener esta [autenticación], se crea una [passkey] en [NIRE] (en el [dispositivo cliente] -app/web- y en el [servidor NIRE])
2. ... en un momento posterior cuando la persona usuaria quiere volver a entrar en la [app] **NO tiene que utilizar [Giltza] o [NIK] y simplemente se utiliza la [passkey] para entrar en [NIRE]**

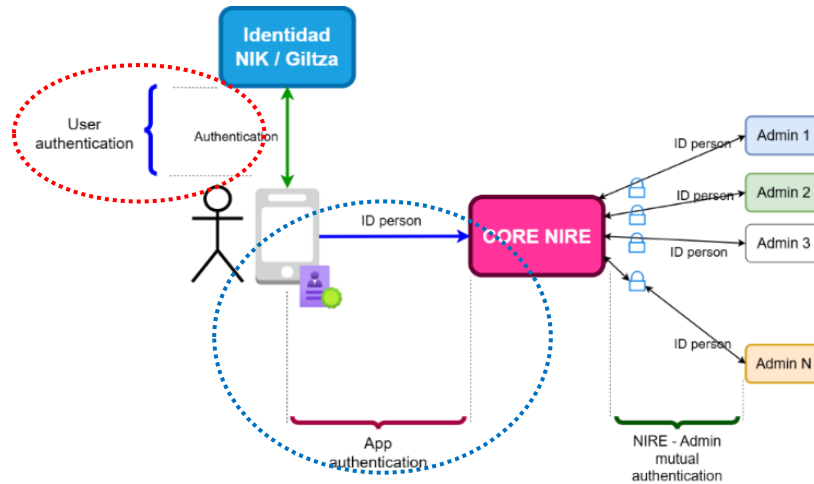
3.3.2 App authentication

Una vez [autenticada] la persona usuaria en el [dispositivo cliente] (app/web) -ver punto anterior-, la app/web [NIRE] tiene que “solicitar” [datos] al [CORE NIRE de interoperabilidad] para “pintar” la [UI].

Cuando el [CORE NIRE de interoperabilidad] recibe una [petición de datos] desde el [dispositivo cliente] debe tener **certeza de que se trata de un [dispositivo cliente] “registrado”**



CONCEPTUALMENTE (para separar “ámbitos” de [autenticación] y hacer más “entendible” el sistema), la [autenticación] del [dispositivo cliente] en el [CORE NIRE de interoperabilidad] (app authentication) **NO** es lo mismo que la [autenticación] de la [persona usuaria] en el [dispositivo cliente] (user authentication)



El [CORE NIRE de interoperabilidad] cuando recibe una [petición de datos] tiene que:

1. Verificar que la [petición de datos] *procede* de un [dispositivo cliente] “registrado”
2. Utilizar un [identificador de persona] (ej: *DNI, NIE...*) que “llega” en la [petición de datos] como parámetro para *recuperar* los [datos]

Este punto se *ocupa* del [paso 1]

Para hacer esta *verificación* de que la [petición de datos] es legítima (*procede de un [dispositivo cliente] “registrado”*) se podrían proponer dos soluciones:

- [1] – Utilizar una pareja [clave pública] – [clave privada] generada en el momento de instalación de la [app] y *enrollment (pairing)* en [NIRE]

Es una solución *sencilla* que se utiliza bastante y que funciona así:

1. Cuando se instala la [app] y se hace el *enrollment (pairing)* en [NIRE] se genera una pareja [clave pública] – [clave privada]
 - a. La [clave privada] se devuelve al [dispositivo cliente]
 - b. La [clave pública] se guarda en el [CORE NIRE] junto con un [ID dispositivo]
2. Cuando la [app] hace una [petición de datos] al [CORE NIRE] **firma un [token] con la [clave privada]** que incluye en la [petición de datos] junto con el [ID dispositivo]
3. El [CORE NIRE] al recibir la [petición de datos] *simplemente* **utiliza la [clave pública] que se guardó en [1] para verificar la [firma]**

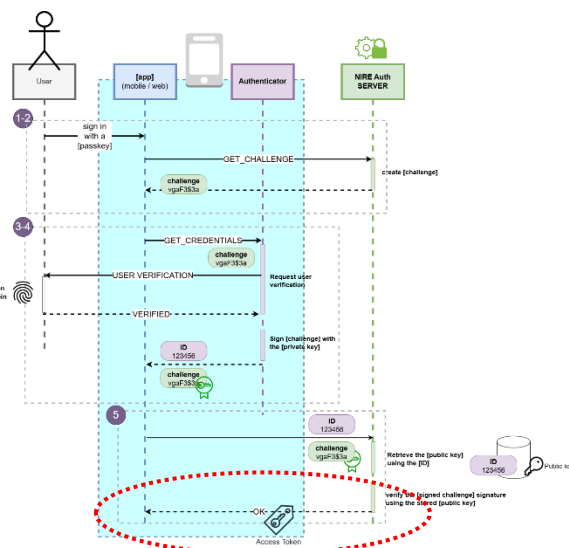
[2] – “Re-utilizar” el sistema [passkeys] que se ha utilizado para la [autenticación de usuario] en el [dispositivo cliente]

En el punto anterior se ha *detrallado* cómo el [CORE NIRE] almacena un [ID] asociado a la persona junto con una [clave pública] que se creó al generar el [passkey]

Se puede utilizar el mismo sistema descrito antes para verificar las [peticiones de datos] incluyendo el [ID] y el [token de acceso] (jwt) generado en el punto [5(c)] del [diagrama de autenticación con [passkeys]] anterior.

Es decir, con este sistema basado en [passkeys], la persona usuaria:

1. Accede a la [app] (web/móvil) -se autenticando utilizando un [passkey] (con verificación biométrica / PIN, SIN requerir una [autenticación] externa en [Giltza]/[NIK])
2. El [token de autenticación] generado en el paso anterior (punto 5 c del flujo de autenticación con [passkeys]) puede ser utilizado en llamadas posteriores de [petición de datos] al [CORE de NIRE] con lo que éste tiene la *certeza* del origen legítimo de la llamada



3.3.3 Autenticación mutua [NIRE] ↔ [Admin]

Para que el [CORE NIRE] pueda “solicitar” a una [administración] datos de una persona necesita:

- 1 La [identidad] de la persona: un [identificador de la persona] (ej: DNI / NIE) → La [identidad] la “tiene” la [app] (móvil / web) y se la “pasa” al [CORE NIRE] en la [solicitud de datos]
- 2 El [consentimiento] de la persona que debe haber *aceptado* explícitamente la consulta de los datos en la [administración] (que por otra parte son SUS datos que el [CORE NIRE] ni ve ni almacena) → (ver más adelante en este documento)
- 3 **Autenticarse** en el servicio de la [administración] que proporciona los [datos] que debe **tener certeza de que es [NIRE] quién está solicitando los [datos]** → Es lo que se describe en este punto



Para conseguir el objetivo de [NIRE] de obtener el mayor número de [datos] posible en el mayor número de [administraciones], [NIRE] debe **adaptarse al contexto existente en estas [administraciones] y si es posible NO imponer una aproximación técnica.**

En el caso de la [autenticación mutua NIRE <-> Admin] **se ofrecerán diferentes opciones técnicas** y las [administraciones] *elegirán* la más viable en función de su contexto.

Hay dos escenarios de [autenticación mutua NIRE <-> Admin]:

- | | | |
|---|---|--|
| 1 [NIRE] solicita [datos] a una [administración] | → | La [administración] tiene que tener certeza de que es [NIRE] quién solicita los datos para una persona |
| <hr/> | | |
| 2 Una [administración] envía meta-datos a [NIRE] sobre la actualización de los [datos] (<i>ver antes en este documento</i>) | → | [NIRE] tiene que tener certeza de que es una [administración] <i>legítima</i> la que actualiza información en [NIRE] |

Las opciones técnicas inicialmente previstas son:

3.3.3.1 Clave compartida

[NIRE] y la [administración] **comparten una [clave]** que se utiliza para *firmar* un [token] que se utiliza en:

- Las peticiones de datos [CORE NIRE] -> [admin]
- El envío de meta-data sobre la actualización de los datos desde la [admin] -> [CORE NIRE]

NO es la mejor opción y debería evitarse siempre que sea posible, pero es la opción más simple y podría utilizarse en caso *extremo* si técnicamente NO es viable utilizar otra alternativa.

3.3.3.2 Par [clave pública] – [clave privada]

En este caso hay que diferenciar los dos casos de interacción:

- | | |
|--|---|
| <ul style="list-style-type: none"> ▪ Las peticiones de datos [CORE NIRE] -> [admin] | <p>[NIRE] genera un par [clave pública] – [clave privada]</p> <ul style="list-style-type: none"> ▪ La [clave privada] se <i>custodia</i> en el [CORE NIRE] (<i>ninguna [administración] tiene acceso a esta [clave privada]</i>) ▪ La [clave pública] es accesible por TODAS las [administraciones] <p>Con este par de claves:</p> <ul style="list-style-type: none"> ▪ El [CORE NIRE] <i>firma</i> un [token] con la [clave privada] y lo incluye en la [petición] de datos ▪ La [administración] <i>verifica la firma</i> del [token] con la [clave pública] del [CORE NIRE] |
| <hr/> | |
| <ul style="list-style-type: none"> ▪ El envío de meta-data sobre la actualización de los datos desde la [admin] -> [CORE NIRE] | <p>Se genera un par [clave pública] – [clave privada] para cada una de las [administraciones]:</p> <ul style="list-style-type: none"> ▪ La [clave privada] se <i>custodia</i> en cada [administración] (<i>el [CORE NIRE] NO tiene acceso a esta [clave privada]</i>) ▪ La [clave pública] es accesible por el [CORE NIRE] <p>Con este par de claves:</p> <ul style="list-style-type: none"> ▪ La [administración] <i>firma</i> un [token] con la [clave privada] y lo incluye en la llamada al [CORE NIRE] para enviar meta-datos de actualización ▪ El [CORE NIRE] <i>verifica la firma</i> del [token] con la [clave pública] de la [administración] |

Esta solución técnica es mejor que la anterior (*clave compartida*) pero tiene la complejidad de la gestión de las claves.

3.3.3.3 Certificados X509

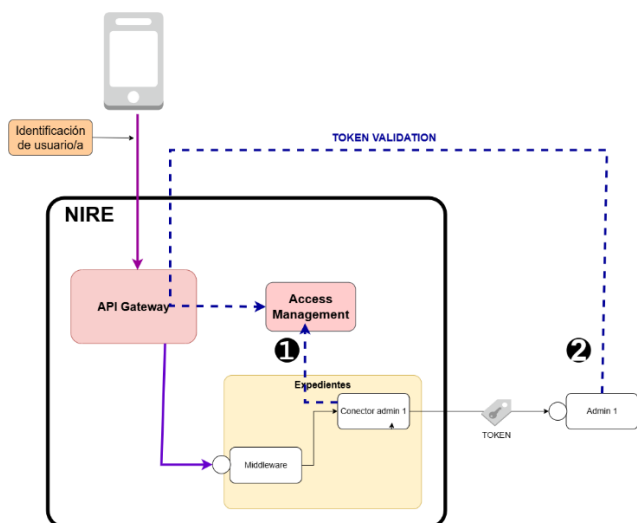
Es una solución similar a la anterior pero basada en el intercambio de [certificados X509] en lugar de [claves] así que también tiene el inconveniente de la gestión e intercambio de los [certificados].

Se utiliza fundamentalmente cuando se utilizan [servicios SOAP].

3.3.3.4 Solución Zero-trust basada en un [Access Management System].

En este caso se evita la gestión de [claves] o [certificados] (*distribuir [claves] y [certificados] en [CORE NIRE] y las [administraciones]*) mediante el uso de un [Access Management System] (ej: [keycloak](#))

A muy alto nivel, el funcionamiento es el siguiente:



[1] - En cualquiera de los dos casos:

- Las peticiones de datos [CORE NIRE] -> [admin]
- El envío de meta-data sobre la actualización de los datos desde la [admin] -> [CORE NIRE]

la entidad "llamante" **solicita** al sistema [Access Management] (ej: [keycloak](#)) un [token]

[2] - Al recibir la llamada, la entidad "invocada" **verifica** el [token] recibido *contra* el sistema [Access Management]

Esta aproximación evita la distribución de [claves] o [certificados X509] así que sería la solución *preferida*

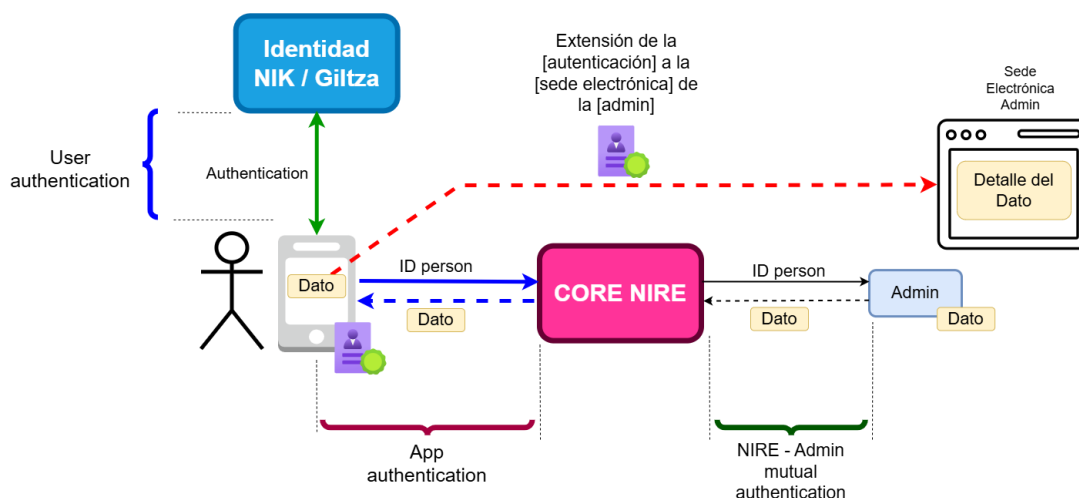
3.3.4 Extensión de la autenticación desde el [dispositivo cliente] a la [sede electrónica] de la [administración]

[NIRE] es un punto común que tiene la vocación de **mostrar** [datos] de diferentes [administraciones] sin sustituir a las [sedes electrónicas] de las [administraciones].

... esto implica que cuando se hay que "hacer algo" con el [dato], la **persona usuaria será redirigida a la [sede electrónica] de la [administración] correspondiente**.

Ej: En [NIRE] se pueden ver las [notificaciones] de cualquier [administración], pero el detalle ha de verse obligatoriamente en la [sede electrónica] de la [administración] porque ahí se registra el momento de recepción que tiene efectos en la tramitación del [expediente]

... obviamente, **si la persona está autenticada en [NIRE], NO debería volver a autenticarse en la [sede electrónica] de la [administración]**: de alguna forma hay que *extender* la [autenticación] desde [NIRE] a la [sede electrónica] de la [administración]



En el entorno del [navegador web], de alguna forma esto ya ocurre ya que cuando la persona se [autentica] utilizando [Giltza] (*Izenpe*) en la [sede electrónica] de una [administración] y navega a la [sede electrónica] de otra [administración] diferente, la [autenticación] se conserva: [giltza] proporciona un **single-sign-on (SSO)**

Hay que conseguir un single-sign on cuando la [autenticación] se obtiene en primer lugar en una [app móvil] y de ahí se *salta* a un [navegador web] (*son “contenedores” diferentes: se “salta” de [app] a [web browser]*)



Las [administraciones] por lo tanto tendrán que implementar en sus [sedes electrónicas] los mecanismos técnicos para hacer este single-sign-on

A continuación se *propone* una posible solución *estándar* a este problema basada en el protocolo **“Token Exchange (RFC 8693 – OAuth 2.0 Token Exchange)”**



Este protocolo permite que el [CORE NIRE] envíe a [Giltza] (IZENPE) un [token OAUTH] emitido por el propio [NIRE] y que [Giltza] **devuelva a cambio otro [token OAUTH] emitido por [Giltza]** y que en principio podría ser utilizado para entrar en cualquier [sede electrónica] que *soporte* [Giltza]

En esencia el protocolo [OAuth 2.0 Token Exchange] permite **intercambiar** (*exchange*) un [token OAUTH] emitido por un [proveedor] (*en este caso [NIRE]*) por otro [token OAUTH] emitido por otro [proveedor] (*en este caso [Giltza]*) y utilizar este último [token OAUTH] para *entrar* en la [sede electrónica] destino

Las *pre-condiciones* para poder utilizar este sistema son:

- [Giltza] debe *soportar* el [protocolo token Exchange] (RFC 8693 – OAuth 2.0 Token Exchange)
- [NIRE] ha de *federarse* en [Giltza]

Finalmente otro aspecto NO directamente *ligado* a el *traslado* de [autenticación] desde la [app] al [navegador web] para poder “ir” a la [web] de la [sede electrónica], pero que *está* directamente relacionado:



Cada [dato] tendrá que exponer una URL propia ya que a la persona usuaria se la **redirige directamente al [detalle del dato] en la [sede electrónica]** (*NO “navega” por la [sede electrónica] hasta el [dato]*)

... es decir, por ejemplo, suponiendo que la persona usuaria quiere ver el [detalle] de una [notificación] que ve en su [app NIRE], al “pinchar” en [detalle] será redirigido a una URL en la [sede electrónica] de una [administración].

... esta URL debe dirigir **directamente** a la [notificación] y sería algo como:

`https://sede.admin.eus/notificaciones/{ID notificación en la admin}`

En otras palabras:



Las [administraciones] además de los [datos] para “pintar” en [NIRE] tienen que enviar una URL directa al [detalle del dato]

3.4.1 Monitorización / Observabilidad / Traza

Este punto se centra en dos aspectos:

1 Monitorización de los componentes del sistema	Obtener información sobre el estado de los sistemas de la infraestructura : uso de CPU, memoria, comunicaciones, si los servicios están activos o no, etc
2 Observabilidad: estado del sistema en base al “desempeño” y las interacciones entre componentes	Se utilizarán datos asociados al “desempeño” del sistema como [número de peticiones de interoperabilidad] (<i>si en algún momento este número es bajo respecto a la media se podría inferir que hay algún tipo de problema</i>) ...frente a la aproximación “clásica” de la [monitorización] que se centra en componentes individuales y datos como CPU, memoria estado de procesos, etc, la [observabilidad] pretende analizar el sistema completo y las interacciones entre componentes.
3 Traza: depurar [incidencias] en la interoperabilidad ente [NIRE] y una [administración] concreta en un [origen de datos] concreto (<i>ej: expedientes</i>)	En ocasiones, se pueden producir [incidencias] puntuales que han de ser “depurados” en detalle por personas técnicas asociadas a [NIRE] para, por ejemplo, “trazar” una petición por todos los componentes por los que pasa y determinar el origen del error

Para lograrlo, hay que trabajar en tres áreas:

[A] Recolección	Trazas	Componentes del sistema por los que cada [petición] va “pasando”
	Métricas	Mediciones en tiempo de ejecución como: - Duración de una llamada de interoperabilidad - Número medio de peticiones / minuto - CPU - Memoria - Etc
	Logs	Texto (estructurado preferentemente) que proporciona información sobre lo que está pasando en el sistema
[B] Almacenamiento	Sistema donde almacenar de forma persistente los datos recolectados en [1]	
[C] Visualización y acceso a los datos	Cuadros de mando de los datos: ■ Para el [centro de control] de [EJIE]: monitorización ■ Para las personas que gestionan el sistema y resuelven incidencias	



En la [monitorización] / [observabilidad] **menos es más** y por lo tanto se priorizará:

- La **simplicidad** del sistema de monitorización / observabilidad
- Capturar unas **pocas [trazas] / [métricas] / [logs] pero muy depuradas**
- Crear **[cuadros de mando] simples** con las [visualizaciones] indispensables que permitan saber si el sistema está funcionando correctamente de la forma más simple posible

Hay que hacer **énfasis** en dar solución a los siguientes [casos de uso] / necesidades:

Caso de uso [1]: depurar petición de interoperabilidad

Personas usuarias	Técnicos/as de [interoperabilidad NIK-NIRE]
Problema	Una determinada [petición] de [interoperabilidad] NO funciona correctamente
Necesidad	Tracear <i>(de la forma más sencilla posible)</i> el “camino” de una [petición de interoperabilidad] por todos los puntos por donde pasa: 1. [app] <i>(móvil o web)</i> 2. API Gateway 3. Middleware 4. Conector 5. Origen de datos En cada paso intermedio se debe visualizar: ▪ Identificador de la [petición] ▪ Parámetros de entrada ▪ Respuesta ▪ Logs asociados a la [petición] <i>(opcionalmente)</i> Es muy importante que la [UI] para hacer estas operaciones de “rastreo” sean lo más sencillas posible evitando que la/el técnico/a tengan que tener conocimientos técnicos especializados del sistema

Caso de uso [2]: paneles de centro de control

Personas usuarias	Personal de operación de [EJIE] que monitoriza los sistemas Técnicos/as de [interoperabilidad NIK-NIRE]
Problema	Es necesario tener un [panel de control] del sistema [NIK-NIRE] en el [centro de mando] de [EJIE]
Necesidad	En el [centro de mando] de [EJIE] se deberían integrar paneles simples que permitan: ▪ Ver el estado de los componentes principales del sistema: – API-Gateway – N-Middleware <i>(uno por [origen de datos])</i> – Sistema de reglas – ... Este estado de los componentes se <i>obtendrá</i> a partir de [métricas] de cada uno como CPU, memoria, estado de los servicios, comunicaciones, etc ▪ Ver algunos datos básicos de rendimiento del sistema: – Número de [peticiones] de [interoperabilidad] / tiempo <i>(a nivel global y por [origen de datos])</i> – Tiempo medio de procesamiento de peticiones de [interoperabilidad] <i>(a nivel global y por [origen de datos])</i>

Esta parte se trabajará con la [Oficina Técnica NIK-NIRE] y las personas responsables de la [monitorización] / [observabilidad] en [EJIE] en identificará:

- Las herramientas a utilizar en cada uno de los puntos anteriores, *priorizando si es posible herramientas abiertas como [Open Telemetry] para la [recolección], [Prometheus] para el [almacenamiento] y [Grafana] para la [visualización]* (aunque durante el trabajo con la [Oficina Técnica NIK-NIRE] y EJIE puedan trabajarse otras alternativas: [Elastic [ELTK](#)] u otras basadas en productos [SaaS])
- Las [trazas], [métricas] y [logs] a capturar
- La integración con los sistemas de monitorización / eventos de [EJIE]
- La definición de [procedimientos] y [protocolos]
- Etc

3.4.2 **Audit**

Todos los **usos** de la [interoperabilidad de datos NIRE] deben guardar información de [auditoría] (*audit*) para conocer:

- **Quién** ha utilizado el [servicio de interoperabilidad] (*en principio siempre es la [persona] “detrás” de la [app]*)
- **Qué** [datos] se han consultado
- **Cuándo**
- Si en el momento de la consulta existe un [**consentimiento**] válido o no
- ... y cualquier otra información que se considere relevante de cara a la auditoría del intercambio de datos.



Los datos de [audit] deben estar **disponibles** para su consulta:

- Por parte de personal técnico autorizado de cualquier [administración] desde la [UI] de la [aplicación de gestión de NIRE] (*ver más adelante*)
- Como [servicio web] (REST preferentemente) por parte de cualquier sistema autorizado de cualquier [administración]

Se debe asegurar la **integridad** de estos datos de [audit] y se debe impedir:

- Su consulta por parte de personas no autorizadas
- Su modificación en cualquier circunstancia

A nivel técnico, en principio los datos de [audit] deben tener un **sistema ad-hoc** donde se almacenen de forma segura e inmutable y se habilite su consulta de forma sencilla con garantías de estar autenticado y autorizado en el sistema.

... en otras palabras en principio **NO se considera que la misma solución para la [monitorización] / [observabilidad] sea adecuada para los datos de [auditoria]** ya que su naturaleza y finalidad es muy diferente.

(*en cualquier caso, durante el proyecto se puede reconsiderar esta aproximación técnica con la ayuda de la [Oficina Técnica NIK-NIRE]*)

3.4.3 Datos Analíticos para el Observatorio de Administración Digital

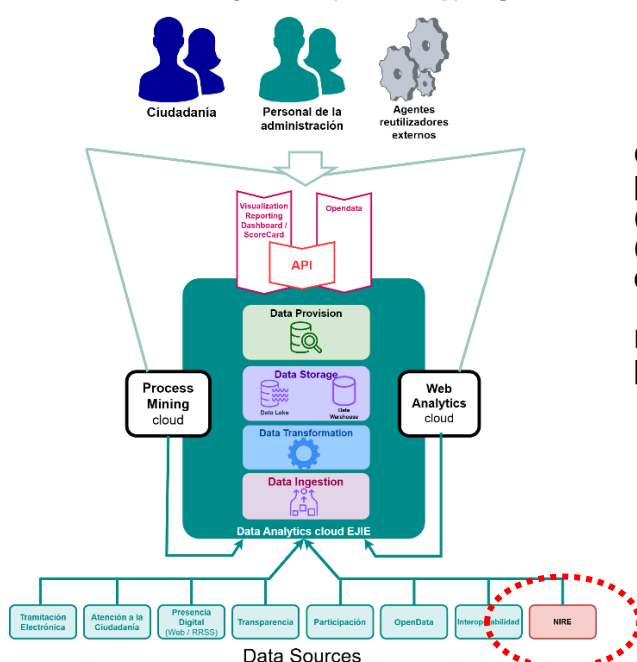
El [Observatorio de la Administración Digital] es un sistema que tiene dos grandes objetivos:

- Tener **información de [cuadro de mando]** como soporte para la **toma de decisiones** informadas en base a datos (*indicadores*)
- **Difundir datos e información sobre el uso** de los servicios de la [Administración Digital]

para lograrlo, se “recolectan” datos desde diversos componentes de la [Administración Digital] (*presencia digital, tramitación electrónica, atención a la ciudadanía, etc*) y con ellos se crean [cuadros de mando] a diferentes niveles:

Dirección	Destinado a los niveles de dirección de la [Administración Digital]
Operativo horizontal	Destinado a los diferentes [servicios] responsables a nivel horizontal (<i>global</i>) de la operativa de las áreas de la [Administración Digital]
Operativo vertical (<i>departamental</i>)	Destinado a la dirección operativa en cada departamento: debería mostrar una visión del desempeño del departamento en las diferentes áreas de la [Administración Digital]
Iniciativa	Destinado a tener un [cuadro de mando] de una iniciativa departamental concreta, típicamente en el área de [tramitación electrónica]
Publico	La visión del <i>desempeño</i> de la [Administración Digital] que se publica de forma abierta en internet

[NIK]/[NIRE] es un área más que tiene que tener “**presencia**”/representación en el [Observatorio de Administración Digital] y para ello hay que trabajar con la [Oficina Técnica NIK-NIRE] y con el proyecto [Observatorio de Administración Digital] en **hacer las integraciones** necesarias para “enviar” los **datos de analíticos en tiempo real** (*streaming*) al [Observatorio de Administración Digital]



Como se ve en la figura (*desde abajo hacia arriba*), [NIRE] es un [origen de datos] más que (1) se **ingestan**, (2) **transforman** (*limpian, normalizan, etc*) y finalmente (3) se **almacenan** en el [data-lake] / [data-warehouse] de la [plataforma analítica]

La capa de [data provision] permite **acceder** a los [datos analíticos] y crear [cuadros de mando]

El proyecto [Observatorio de Administración Digital] se estructura en tres [lotes]:

LOTE 1 Oficina Técnica	■ Gobernanza del Proyecto ■ Coordinación Técnica y Funcional ■ Gestión del Cambio
LOTE 2 Almacenamiento de datos	■ Creación del [data-lake] / [data-warehouse] con datos de los diferentes [orígenes]
LOTE 3 Cuadro de mando	■ Visualización de los [datos] en [cuadros de mando] a diferentes niveles

El [lote 1] (*en coordinación con la [Oficina técnica NIK-NIRE] y [EJIE]*) guiará al presente proyecto en este [paquete de trabajo] de integración con el [almacenamiento] responsabilidad del [lote 2]

3.5 Consentimientos

Los [consentimientos] son una parte “clave” en [NIRE]:



Todas las invocaciones a servicios (*todas las llamadas de interoperabilidad que recibirán las [Administraciones] origen de datos*) incluirán una **“base” que habilita a la consulta de los datos** que puede ser:

- Un **[consentimiento informado]** expreso **“otorgado”** por parte de la persona interesada



El [consentimiento informado] se refiere a

- Informar en un lenguaje sencillo a la persona interesada sobre **qué datos se recopilan, tratan o intercambian, por quién y para qué motivo.**
- Obtener la **autorización** (*consentimiento*) por parte de la persona interesada

La regulación europea [EU - 2016/679] establece que el consentimiento debe:

- Ser otorgado con libertad
- Ser informado
- Ser explícito
- Basarse en una prueba no ambigua de la autorización de la persona interesada
- Ser demostrable: tiene que poder ser accedido fácilmente
- Ser revocable

- Una **[habilitación normativa] a la [Administración]:** *en algunos casos, las [Administraciones] están “habilitadas” normativamente a obtener determinados [datos] sin necesidad de [consentimiento] expreso por parte de la persona interesada*

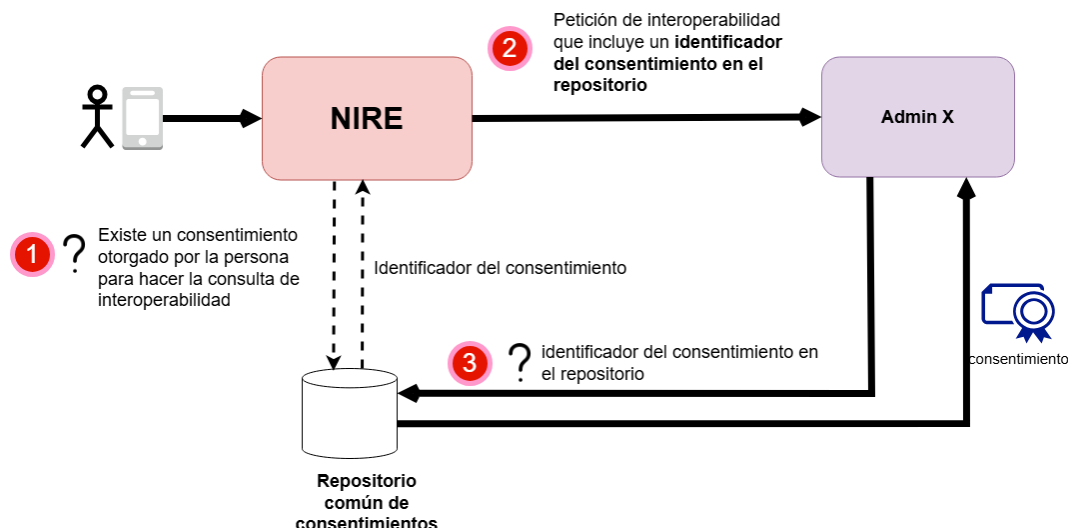
Los **principios** de uso del [consentimiento] / [habilitación normativa] en el ámbito de los [servicios de interoperabilidad NIK-NIRE] son:

- 1 Es mandatorio *recabar* el [consentimiento informado] de la persona**
 - Si NO existe [consentimiento] NO se puede hacer la [petición de interoperabilidad NIRE <-> Administración]: **si no hay base habilitante NO se hace la petición**
 - Si existe una [habilitación normativa] de aplicación general no es necesario el [consentimiento informado] (*aunque SI es deseable “informar” a la persona de la existencia de esta [habilitación normativa]*)
- 2 Los [consentimientos] y las [habilitaciones normativas] y se almacenarán en un [repositorio] común que contendrá:**
 - El **[consentimiento]** (o *[habilitación normativa]*) junto con las **[evidencias]** de cómo se obtuvo y de que es expreso e informado.
 - **Datos que uso:** para qué se utiliza y cuando > se debe registrar el uso por parte de sistemas que utilizan un [consentimiento] concreto (*por ejemplo [NIRE]*)

La información del repositorio puede ser consultada por:

 - La persona usuaria que puede ver los [consentimientos] otorgados y en su caso revocarlos (*si es que el [consentimiento] es revocable ya que no todos podrían ser revocables*)
 - Las [Administraciones] adheridas a [NIRE]
- 3 Todas las peticiones a [servicios de interoperabilidad NIRE] incluirán información sobre la *base habilitante* (*consentimiento / habilitación normativa*) que permitirá a la [Administración] receptora de la petición **comprobar** su existencia y validez en el [repositorio] común.**

A muy alto nivel el sistema funciona de la siguiente forma:



- 1 Ante una petición por parte de un *cliente* [NIRE] en primer lugar se asegurará de que en el [repositorio común] **existe un [consentimiento]** otorgado por la [persona] usuaria ya que **habilita** a la ejecución de la [petición de interoperabilidad]

La consulta al [repositorio común] contendrá:

Quién (<i>subject</i>)	- La persona que ha otorgado el [consentimiento]
Para quién (<i>data owner</i>)	- La [Administración] o entidad de la [Administración] para la que se requiere el [consentimiento]
Para qué (<i>purpose = propósito de uso</i>)	- El [dato] de la [Administración] en el que se va a utilizar el [consentimiento] (<i>ej: consultar el dato X</i>)

y la respuesta simplemente será un **[identificador del consentimiento]** (*en caso de existir el consentimiento solicitado*)

- 2 Si el [consentimiento] existe, [NIRE] en la [petición de interoperabilidad] que *envía* a la [administración] origen de datos **adjunta el [identificador del consentimiento]** anterior

- 3 La [Administración] antes de ejecutar la [petición de interoperabilidad] recibida puede **validar el [consentimiento]** si lo estima conveniente (*no es obligatorio*)

Esta [validación de consentimiento] es una *petición* que hace la [Administración] al [repositorio común] de [NIRE] en base al [identificador del consentimiento] y que tendrá como respuesta un *documento* firmado por [NIRE] con los detalles:

Quién (<i>subject</i>)	- La persona que ha otorgado el [consentimiento]
Para quién (<i>data owner</i>)	- La [Administración] o entidad de la [Administración] para la que es válido el [consentimiento]
Para qué (<i>purpose = propósito de uso</i>)	- El [dato] de la [Administración] en el que se va a utilizar el [consentimiento] (<i>ej: consultar el dato X</i>)
Cuándo	- La fecha en la que se emitió el [consentimiento]
Durante cuánto tiempo	- La fecha de validez del [consentimiento] (<i>hasta qué fecha se puede utilizar</i>)
Evidencias	- Cómo se ha recabado el consentimiento - La información base que se ha utilizado - <i>Huellas</i> que evidencien que el [consentimiento] es expreso (<i>ej: firma / log / etc</i>)

Según este modelo:

- [NIRE] se asegura de que **existe** un [consentimiento] válido antes de hacer la invocación al [servicio de interoperabilidad] (*si no existe el [consentimiento] no se hace la invocación*)
- La [Administración] dispone de datos para poder **consultar** y **validar** el [consentimiento] en cualquier momento
 - ① ... pero NO tiene obligatoriamente que hacer esta validación el [consentimiento] en el [repositorio común] ya que puede *confiar* en que lo ha hecho [NIRE] antes
 - ... pero siempre tiene a su disposición datos que le permiten acceder al [consentimiento] en caso de conflicto o duda

El [repositorio común de consentimientos] es por lo tanto un componente que:

- **Almacena** los [consentimientos] en formato *computable* (datos estructurados) junto con las [evidencias] de ser informado y expreso
- **Expone [servicios web]** (REST) para que:
 - Sistemas externos (*ej: una [administración]*) puedan consultar un [consentimiento] recibido en una [petición de interoperabilidad] y determinar si es legítima
 - Se puedan crear [interfaces de usuario] para:

Ciudadanía

En la [app] NIK-NIRE la persona usuaria debería poder **consultar** los [consentimientos] que ha otorgado y:

- Ver datos de cuándo se creó el [consentimiento] y para qué fin
- Ver quién, cuando y para qué se ha utilizado el [consentimiento]
(*ej: cuando [NIRE] utiliza un [consentimiento] para obtener datos de una [administración]*)
- Revocar el [consentimiento]

! No todos los [consentimientos] pueden ser revocados

Por ejemplo, si un [consentimiento] se ha dado en el ámbito de una [solicitud] de un [servicio] (*ej: ayuda*) este no debería poder ser revocado puesto que tendría consecuencias de compleja solución en la tramitación subsecuente

Personal funcional / técnico de la administración

Existirán [UI]s auxiliares (*ver más adelante*) donde personas autorizadas de la [administración] podrán consultar [consentimientos]



En el caso de [NIRE] es la propia persona usuaria la que *-a través de [NIRE]-* **consulta SUS datos** en diferentes [administraciones] ([NIRE] no “ve” ni “almacena” ningún dato) con lo que la necesidad del [consentimiento] para esta consulta podría NO ser necesario ... en cualquier caso, es un aspecto a estudiar desde el punto de vista [normativo]



Algunas referencias sobre [consentimientos]

- [Republic of Etonia Information System Authority](#)
- [The Role and Importance of Consent Management in Public Organizations in the Digital Age: Case on Estonia](#)
- [Nets.eu consent management system](#)

3.6 Datos que se interoperan

Como se ha señalado en diferentes puntos de este documento, el objeto de [NIRE] son los **[datos] de una persona** (*física o jurídica*) en cualquier [Administración Vasca] para lo que la base es un [sistema de interoperabilidad] objeto del presente [expediente de contratación]

En este punto se detallan a nivel general los [datos] que de forma progresiva se irán incorporando en [NIRE] (*en el [sistema de interoperabilidad] y por lo tanto en la [app]*)



La enumeración / descripción NO es exhaustiva ni completa: es únicamente una visión general de los posibles [datos] objeto de la [interoperabilidad NIRE]

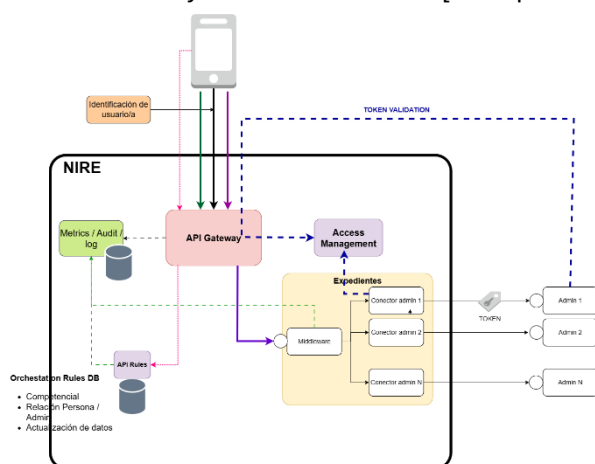
... actualmente se está trabajando desde la [Oficina Técnica NIK-NIRE] en identificar y detallar los [datos] así como [calendarizar] con las [Administraciones] su integración en [NIRE] (*road-map*)

En general (*en una primera aproximación de muy alto nivel*), la **integración** de un [dato interoperable] en la [NIRE] implica **trabajar en**:

A Análisis

B Semántica: modelo y formato de intercambio

C Construcción y securización de la [interoperabilidad NIRE <-> Admin]



Tomando como referencia el *esquema general* de la arquitectura descrita, hay que trabajar en:

- **Middleware**
- Integración en el **API-Gateway**
- **Securización** de la “conexión” [conector] <-> [administración]
- **Conectores** con las diferentes [administraciones] que proporcionan datos

D Documentación: documentación de la [semántica] en el [\[sitio web del desarrollador\]](#)

Se debe poner **especial atención** a la documentación de la [semántica] (*modelo y formato*) puesto que esta es la base para:

- Desde [NIRE] crear un nuevo [conector] en el [middleware] para nuevas [administraciones] que se van incorporando a [NIRE] (*si no se adaptan al [conector estándar]*)
- Desde una [administración] exponer un [servicio] estándar “llamable” desde [NIRE] por el [conector estándar]

E Despliegue y gestión del cambio (*ej: soporte a la integración de administraciones*)

Las [administraciones] en el proceso de integración a [NIRE] para un [dato interoperable] concreto necesitan un soporte por parte de [NIRE].

Como ya se ha introducido varias veces, para facilitar el “entendimiento”, [NIRE] se ha dividido en áreas:

1	NIRE Datuak	Datos que las [administraciones] tienen de las personas: contacto / bancarios, representaciones, certificados, carnets, etc
2	NIRE Karpeta	Datos asociados a [expedientes] : expedientes, notificaciones, registro, pagos, etc
3	Calendario	Datos que tienen que ver con eventos que tienen lugar en un punto en el tiempo : citas, hitos asociados a expedientes, devolución de préstamos bibliotecarios, reserva de instalaciones deportivas, etc
4	Servicios	Préstamos bibliotecarios, reservas en instalaciones deportivas, etc

Esta división en *grupos* se justifica ya que, a nivel general, las personas se *relacionan* con la [administración] a través de los [servicios] que estas ofrecen. Estos [servicios] pueden ser:

Basados en [procedimiento administrativo] (*ayudas, registros, autorizaciones, etc*)

Es la forma “normalizada” de ofrecer el [servicio] es base a [trámites] que “mueven” [expedientes]

NO basados en [procedimiento administrativo] (*préstamos bibliotecarios, instalaciones deportivas, etc*)

Es una forma *menos* “normalizada” donde no existen trámites o un [expediente] “formal”

En el caso más general de [servicios] basados en [procedimiento administrativo]:

- **Durante la *instrucción*** hay [datos] sobre el [expediente]: el estado, eventos, notificaciones, etc
- **Una vez finaliza la *instrucción*** en muchos casos **se “generan” otros [datos]**, por ejemplo, si se ha solicitado la [inscripción en un registro] (*ej: parejas de hecho*), al finalizar la *instrucción*, la persona puede tener un [certificado de inscripción en el registro]

Se podría decir que hay:

[1]	Datos “vivos” sobre la [tramitación] del [expediente] (<i>ej: estado del expediente, notificaciones, pagos,...</i>)	>	Se ven en [NIRE Karpeta]
[2]	Datos “producto” de la provisión de un [servicio] y que ya no cambian (<i>ej: un certificado, un título, una acreditación,...</i>)	>	Se ven en [NIRE Datuak]
[3]	Servicios no “administrativos” generalmente no basados en [expedientes] (<i>ej: préstamos bibliotecarios, instalaciones deportivas, etc</i>)	>	Se ven en [Servicios]

y finalmente hay un grupo de [datos] asociados al **calendario** (citas, eventos, etc)

A continuación, se hace una pequeña descripción de cada uno de estos [datos interoperables] (*que como se ha señalado NO es exhaustiva ni completa*)

3.6.1 NIRE Datuak

3.6.1.1 Datos básicos: contacto y bancarios

Las personas **tienen [datos de básicos]** de identidad y contacto (*nombre/apellidos, teléfono, email, etc*) y bancarios (*cuenta*) **en decenas de [bases de datos] de diferentes [Administraciones Públicas]** y este hecho plantea la necesidad de dar respuesta a dos grandes preguntas:

- **Cómo sé** en qué [bases de datos] estoy incluido/a (*y si es posible qué [datos básicos] existen en cada una*)
- **Cómo puedo actualizar** algunos de los [datos básicos] que sistemáticamente se repiten en cada una de las [bases de datos]

Esta dispersión de datos plantea muchos problemas:

- **La información NO está actualizada** en todos los [sistemas de información] lo que en muchas ocasiones fuerza a solicitar la actualización o confirmación de los [datos básicos] una y otra vez en los front-end de la [administración] por la simple necesidad de tener la seguridad de disponer de los datos más recientes.
- Un cambio en cualquier [dato básico] (*por ejemplo, el domicilio, el teléfono o la cuenta bancaria*) implica que la persona usuaria se ve forzada a **informar unitariamente a cada uno de los [sistemas de información]** (*algo complejo ya que en muchas ocasiones la persona desconoce qué [sistemas de información] almacenan sus [datos básicos]*)
- Cuando la [administración] tiene que **contactar** con una persona no se tiene la seguridad de cuáles son los [datos de contacto] más fiables.

Se plantea entonces la cuestión de **dónde deben residir estos [datos básicos]** y se plantean tres grandes opciones:

1 En el [wallet] de la persona usuaria

Es la aproximación que *propone* la tecnología SSI (*self-sovereign identity*) donde todos los datos están bajo el control de la persona usuaria que es quien decide con quien los comparte.

Esta aproximación canónica, tiene algunos grandes inconvenientes:

- Cualquier pequeño cambio en un [dato básico] (*ej: el número de teléfono de contacto*) requiere de renovar la [credencial] del [wallet], algo engorroso (*recordar que la [credencial] reside en el [wallet] que típicamente es una [app móvil]*)
- Las [Administraciones Públicas] no disponen de estos [datos básicos] (*se los tienen que solicitar a la persona usuaria*) lo que también es un problema que además impide otros usos como un sistema horizontal de contacto con las personas.

... en general, las [credenciales] en el [wallet] deberían contener pocos datos y que además sean lo más **inmutables** posible (*datos que no puedan cambiar como la fecha de nacimiento*)

2 **Centralizadamente** en un repositorio común a todas las [Administraciones Públicas]

Es una buena opción puesto que:

- La actualización de los datos es muy sencilla ya que se hace en un único sitio
- Permite a cualquiera de las [Administraciones Públicas] consultar y actualizar estos datos

... sin embargo, **en la realidad existen multitud de repositorios** en las diferentes [Administraciones Públicas] donde hay [datos de básico] (*contacto/bancarios*) y **no van a dejar de estar ahí** para pasar a un repositorio común por muchos servicios de consulta y actualización que este ofrezca.

... también hay que tener en cuenta los condicionantes legales que tiene un repositorio común de datos y los intercambios de datos entre diferentes [Administraciones]

- 3 De forma **distribuida** en múltiples repositorios en cada una de las [Administraciones Públicas]
- Es la opción más ajustada a la realidad (*lo que realmente "pasa"*) ... pero tiene el inconveniente de que cualquier cambio en un [dato básico] (ej: número de teléfono o banco) requiere **distribuir** / difundir este cambio a todos los repositorios de las diferentes [Administraciones Públicas] donde pueda estar

- 4 **Almacenes (PODs) descentralizados** bajo el control de las personas
- La especificación [**SOLID**] que permite a las personas almacenar sus datos de forma segura en **almacenes descentralizados** llamados [POD]s que están bajo su control exclusivo (*y no bajo el control de la [Administración]*)

Los datos están totalmente bajo el control de las personas que deciden:

- **Quién** tiene acceso a qué dato.
- **Dónde** se alberga / alojan los datos: una persona puede elegir entre *albergar* su [POD] personal en un [**POD provider**] o bien montar un *albergue* propio

Esta especificación tiene gran potencial, pero en estos momentos está en un estado muy inicial y aún no tiene gran difusión

Sin menoscabo de que los [datos básicos] puedan estar en el [wallet] de las personas, la solución óptima es quizá un **híbrido** entre la segunda (un repositorio central común) y la tercera (los datos básicos están distribuidos en múltiples repositorios en cada [Administración Pública])

... por lo tanto, sería deseable disponer de un [**punto común**] desde donde una **persona usuaria** pueda **consultar** los [datos básicos] de diferentes [Administraciones] y **actualizarlos** desde un único punto si lo considera necesario

[NIRE] actúa como una **federación de repositorios** que tienen [datos básicos] de las personas y en la que [NIRE] es un [**punto común**] (*hub*) desde donde:

1. **Consultar** qué [datos] tiene cada repositorio
2. **Actualizar** estos [datos] en una sola operación y difundir los nuevos [datos] a todos los repositorios federados

[NIRE] no determina lo que debe hacer un [repositorio] concreto con las actualizaciones comunicadas puesto que cada sistema federado puede decidir la estrategia ante un cambio:

- Consolidar el cambio directamente
- Añadir el cambio a los datos existentes en el repositorio (*ej: una nueva versión o un nuevo registro*)
- Dejar los cambios pendientes de una revisión (*para hacer una consolidación manual posterior*)
- ... o descartar los cambios solicitados



Los [datos básicos] (*contacto / bancarios*) son en principio los únicos datos que en una primera fase del proyecto [NIK-NIRE] van a tener posibilidad de **actualizarse** (*o al menos "solicitar" su actualización*)

Hay que recordar que, en esta primera fase, [NIRE] es fundamentalmente un sistema de **consulta** de los [datos] en diferentes administraciones (*solo lectura*)

Disponer de esta [punto común] / hub con [datos básicos] abre diferentes **escenarios de uso** hasta ahora imposibles o complejos:

Cambio centralizado de [datos básicos] (domicilio, teléfono, cuenta corriente, etc) Una persona puede cambiar sus [datos básicos] desde un lugar central y esta información *difundirse* a otras [bases de datos] (*siempre que exista una [autorización] o [consentimiento]*)

Control del dato por las propias personas y transparencia En la actualidad es muy complicado para una persona saber qué [sistemas de información] mantienen [datos básicos]
Las personas podrían *consultar* qué repositorios tienen datos sobre ellas

En este sentido hay que aclarar **qué NO es objetivo** de esta interoperabilidad de [datos básicos] de la persona:



En muchas [Administraciones Públicas] en el marco de estrategias de **[Gobernanza del Dato]** se está trabajando en crear **[datos maestros]** (ej: *datos maestros de [terceros] de la Administración*) que se convierten en **referencia** en otras [bases de datos] en sustitución de los propios (MDM = Master Data Management)

La aproximación a muy alto nivel, por ejemplo, para crear un *maestro* de [terceros] es:

1. Se parte de los datos de N [orígenes de datos] y se intenta consolidar un [maestro] único (*común*) en un proceso que implica acciones como eliminar duplicados, mejorar la calidad del dato, etc
2. Se cambian los N [orígenes de datos] para que *referencien* los [datos maestros]

Adicionalmente a lo anterior:

- Se crean [API]s para facilitar el acceso a los datos
- Se difunden [eventos] para asegurar que cualquier sistema este al corriente de cualquier cambio en los [datos maestros]

Las iniciativas [MDM] (*Master Data Management*) *sirven* a la [Administración] para mejorar la eficiencia en sus procesos (*e indirectamente dar un mejor servicio a la ciudadanía*).

[NIRE] sirve a la [ciudadanía] para facilitarle el control de sus datos y en un futuro podría convertirse en un maestro de referencia para las iniciativas que así lo consideren, pero en un inicio **[NIRE] no es estrictamente una iniciativa [MDM]** (*aunque en un futuro podría llegar a serlo*)



En coherencia con los *principios* de [NIRE], **NO se sustituye ni se pretende sustituir ninguna [DB de terceros / interesados] de ninguna [administración]**

... únicamente se pretende dar a las personas un punto de consulta y si es posible de actualización de ciertos datos básicos.

Otros puntos a tener en cuenta respecto a los [datos básicos] son:

[1] - Repositorio común de datos básicos

Uno de los *principios* de [NIRE] es que **NO se almacenan datos en [NIRE]** ... sin embargo, cabría la posibilidad (*pendiente de análisis y toma de decisión*) de crear un [repositorio común] de [datos básicos] (*contacto / bancarios*) que puedan ser utilizados por las [administraciones] en diferentes escenarios:

Atención a la ciudadanía	En los diferentes [canales] de [atención ciudadana] (<i>presencial, telefónico, video, etc</i>), las personas se pueden identificar con [NIK] y esto servir como base para “localizar” sus [datos básicos] en el [repositorio común]
Comunicación con la ciudadanía	El [repositorio común] de [datos básicos] puede ser la base de un sistema también común para “enviar” información a las personas (<i>avisos, comunicaciones, boletines, etc</i>) por diferentes canales (email, SMS, push -ver antes-, etc) puesto que al ser unos datos “curados” por la propia persona usuaria deberían ser “mejores”  Un ejemplo de este sistema de comunicación común a diferentes administraciones es GovUK Notify
Ayuda a la tramitación	En los [formularios de solicitud] de los sistemas de [tramitación electrónica] se puede “facilitar” el auto-completado de estos [datos básicos] a partir de la información de identificación (NIK) recuperando datos de [NIRE Datuak]
Etc	

En cualquier caso, si finalmente se *crea* un [repositorio común] de [datos básicos], **NO se plantea ningún tipo de carga masiva en el [punto común] / [hub]** desde ningún repositorio: el [repositorio común] de [datos básicos] “partiría” vacío (*sin datos de ninguna persona*) y se iría “cargando” conforme las personas se den de alta en [NIRE] y **consientan** su inclusión en este [repositorio común]

Otros *retos* que plantearía la creación de este [repositorio común] de [datos básicos] son:

Consentimiento Las personas deberían **consentir** de forma expresa e informada:

- La inclusión de sus [datos básicos] en este [repositorio común]
- El acceso (uso) de estos [datos básicos] por parte de cada [administración]

 Este punto plantea *retos* a nivel normativo ya que en principio NO se puede pedir a una persona que de un [consentimiento general] a una [Administración] para que pueda utilizar los [datos] sino que debería ser en función del propósito (ej: un [servicio] concreto, la [Atención Ciudadana], etc

Protección de datos [NIRE] no almacena datos especialmente relevantes en cuanto a la [protección de datos] (*aunque es un aspecto que se tiene permanentemente en cuenta en todas las áreas del proyecto*)

... sin embargo, si se crea este [repositorio común] de [datos básicos] habrá que trabajar ad-hoc en esta área

En definitiva: la creación de un [repositorio común] de [datos básicos] es un punto **complejo** con muchas implicaciones que se está analizando con la [Oficina Técnica NIK-NIRE] para tomar una decisión go / no-go en cuanto a su implementación

[2] - Identificador de Atención Ciudadana

La [identidad] (*en un sentido general y no técnico*) en el “mundo físico” tiene varias “representaciones”: DNI, NIE, Pasaporte, NIF (*en el caso de empresas*)

Los [sistemas informáticos] en general utilizan estos [identificadores] para “indexar” a las personas (*físicas o jurídicas*) en sus [bases de datos].

La utilización de uno de estos [identificadores] presenta dos problemas significativos:

[A] - Las personas cambian de [identificador]

Hay casos en los que una persona cambia de [identificador] como el caso de personas extranjera residentes que disponen de un [NIE] (*Número de Identidad de Extranjero*) y posteriormente se nacionalizan y pasan a tener un [DNI] (*Documento Nacional de Identidad*)

... obviamente la [identidad] es la misma (*es la misma persona*), pero las [administraciones] tienen que “reflejar” de alguna manera este hecho en sus [bases de datos] para que las personas puedan acceder a los datos que estaban anteriormente “indexados” con un [NIE] que ya NO tienen (*ahora disponen de un [DNI]*)

Las soluciones a este *problema* suelen ser:

- Utilizar un [identificador] “**propio**” independiente del [NIE] o [DNI] y “asociarle” los diferentes [identificadores] que tiene la persona (*primero el [NIE] y luego el [DNI]*)

```
Id propio de la admin
+-- NIE (f. inicio - f. fin)
+-- DNI (f. inicio - ...)
```

- Hacer procesos de **re-indexación** de las [bases de datos]: cambiar el [NIE] por el [DNI]
 - ① Estos procesos de re-indexación pueden *automatizarse* con ayuda de los [servicios NISAE] que permiten obtener el [DNI] asociado a un [NIE]

... en general estos procesos de consolidación / re-indexación se *desencadenan* a partir de un [servicio] de **[comunicación de cambio de identidad]** a la [administración correspondiente]



En el caso de los [certificados digitales] cuando alguien cambia de [NIE] a [DNI] tiene que solicitar a la [entidad de certificación] emisora (*ej: Izenpe*) la revocación del [certificado] asociado al [NIE] y la emisión de uno nuevo asociado al [DNI]

[B] - El [identificador] por sí solo NO proporciona datos completos sobre la [identidad]

Un [identificador] como el [DNI] no proporciona “información” sobre si una persona es autónoma o bien si pertenece o no a una [empresa]



- Para saber si una persona es trabajadora autónoma se podría consultar al [RETA - Régimen Especial de Trabajadores Autónomos]
- Para saber si una persona tiene algún vínculo con una [empresa] algunas opciones son:
 - Utilizar un [certificado profesional] o un [certificado de representante] que incorporan información sobre la empresa
 - Consultar un [registro de representaciones]

De lo anterior:



En [NIRE] en general (y en [NIRE Datuak] en particular) sería interesante utilizar la aproximación de “crear” un **[identificador] propio** (que se puede llamar **[Identificador de Atención Ciudadana]**) y que se utiliza para “consolidar” / “asociar” el histórico de [identificadores] “físicos” de una persona (como se hace en algunas administraciones)

```
Id de atención ciudadana
+-- Pasaporte (f. inicio - f. fin)
+-- NIE (f. inicio - f. fin)
+-- DNI (f. inicio - ...)
```

Sobre esta base, [NIRE] puede proporcionar **servicios** a las [administraciones]:

[1] - Consulta

Consulta de [identificadores]
“físicos” asociados a un
[identificador de atención
ciudadana]

Dado un [id de atención ciudadana] se devuelven los [id]
“físicos” asociados

```
Id de atención ciudadana
+-- Pasaporte (f. inicio - f. fin)
+-- NIE (f. inicio - f. fin)
+-- DNI (f. inicio - ...)
```

Consulta de [identificadores]
“físicos” asociados a otro
[identificador] “físico”

Dado por ejemplo un [DNI] se devuelven el [pasaporte] y
[NIE] anteriores

```
Id de atención ciudadana
+-- Pasaporte (f. inicio - f. fin)
+-- NIE (f. inicio - f. fin)
+-- DNI (f. inicio - ...)
```

[2] - Depuración de [identificadores]

Se puede **automatizar** la comprobación de si existe un [DNI] asociado a un [NIE] que no estaba previamente asociado a ninguno utilizando los [servicios NISAE] (ej: [consulta de identidad de extranjeros](#)): Si se encuentra una asociación se puede guardar en [NIRE Datuak]

Antes de la consulta	Después de la consulta
<pre>Id de atención ciudadana +-- NIE (f. inicio - ...)</pre>	<pre>Id de atención ciudadana +-- NIE (f. inicio - f. fin) +-- DNI (f. inicio - ...)</pre>

[3] - Actualización de datos básicos en repositorios de diferentes administraciones desde un punto único (NIRE Datuak)

Desde [NIRE] se puede **iniciar** (*hacer una “especie de” [solicitud]*) el cambio de [datos básicos] en [repositorios] de [administraciones] *federadas* en [NIRE]

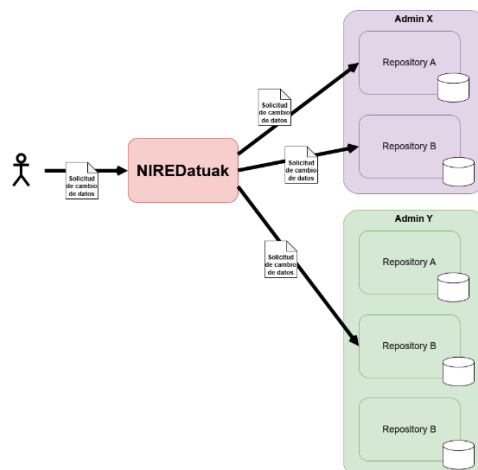
La [persona usuaria] puede en la [UI]:

1. **Consultar** los [datos básicos] (*identidad / contacto / bancarios*) que *figuran* en los [repositorios] de las [administraciones]
2. Decidir que quiere **actualizar algún [dato básico]** (*por ejemplo el contacto o la cuenta corriente*) en uno o en varios de estos [repositorios]

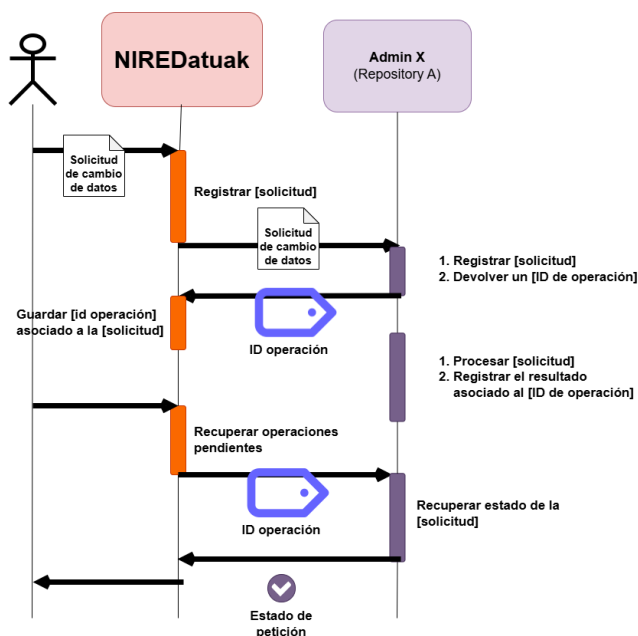
Esta [solicitud de cambio de datos básicos] llega al [CORE de interoperabilidad] de [NIRE] que a su vez se la hace llegar a los [repositorios] seleccionados para actualización por la persona usuaria

Cada [repositorio] de la [administración] puede actuar como considere oportuno:

- Consolidar el cambio directamente
- Registrar la [solicitud de cambio] para ser consolidada tras una revisión manual
- Rechazar la [solicitud de cambio]

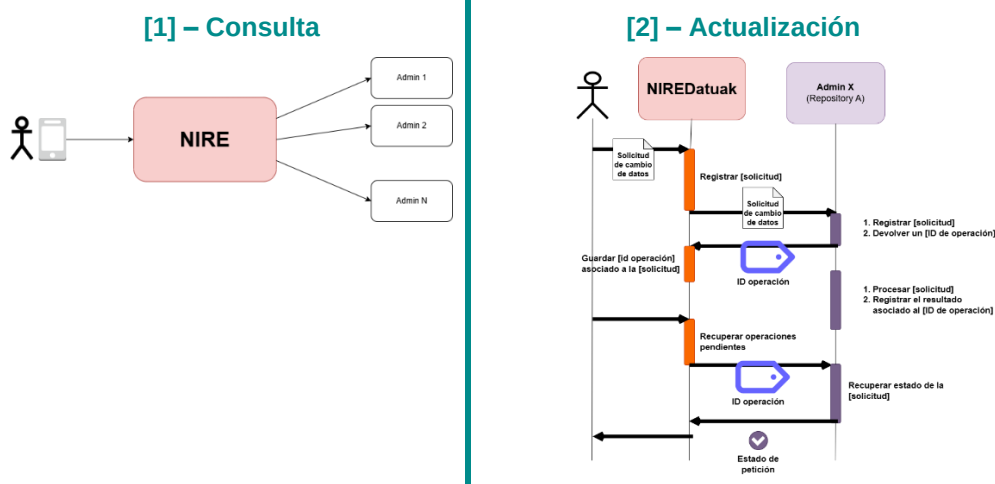


Obviamente para que esta federación funcione los diferentes [repositorios de datos básicos] en las [administraciones] tienen que **implementar un protocolo en base a [servicios web] (REST)** que a muy alto nivel funcionaría de forma similar a la descrita a continuación:



1	La persona usuaria hace una [solicitud de cambio] en la [UI]
2	[NIRE] registra la [solicitud de cambio] y la envía al [repositorio de datos básicos] en la [administración]
3	La [administración] registra la [solicitud de cambio] y devuelve un [id de operación]
4	Asíncronamente la [administración] procesa la [solicitud de cambio] y registra el resultado asociado al [id de operación]
5	... pasado el tiempo, la persona usuaria vuelve a entrar en la [UI] y se “detecta” que hay una [solicitud de cambio] <i>en curso</i> de forma que [NIRE] recupera el [id de operación] y envía una consulta al [repositorio de datos] en la [administración]
6	La [administración] a partir del [id de operación] recupera el resultado de la operación asociada a la [solicitud] y lo devuelve a [NIRE] para que <i>informe</i> a la [persona usuaria]

A la hora de trabajar en la [interoperabilidad de datos básicos] hay que trabajar en dos áreas:



Al igual que en el resto de [datos interoperables] de [NIRE] habrá que:

- **Analizar** el [dato] y los orígenes en las [administraciones]
- Trabajar la **semántica**: modelo, formato, etc
- **Construir** el [middleware] común y [conectores] con cada uno de los [repositorios]
- **Documentar**

Las [administraciones] tendrán que construir [servicios] para:

- Devolver los [datos básicos] de una persona ante una *petición* desde [NIRE]
- Recibir [peticiones de cambio] y consultar el estado de ejecución de una [petición de cambio]

3.6.1.2 Representaciones y Autorizaciones

La mayor parte de las [administraciones] disponen de un **[Registro de Representaciones y Autorizaciones]** que en el caso más amplio puede tener los siguientes *tipos* de registros:

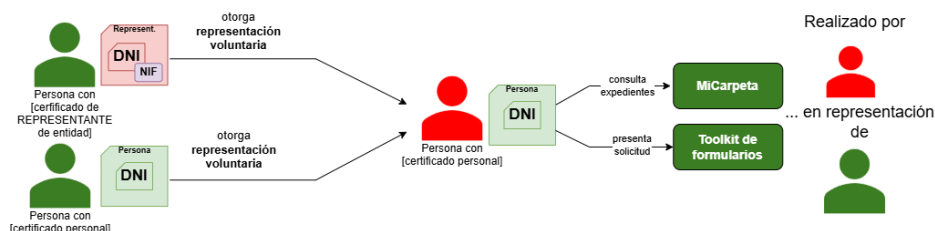
[1] - Representación Voluntaria El trámite figura como “realizado por” el [representante] “en nombre de” el [representado]

[2] - Autorización El trámite figura como “realizado por” el [autorizante] (*el [autorizado] es simplemente la figura que “ejecuta” PERO a todos los efectos es “como si” el trámite lo hubiera hecho [autorizante]*)

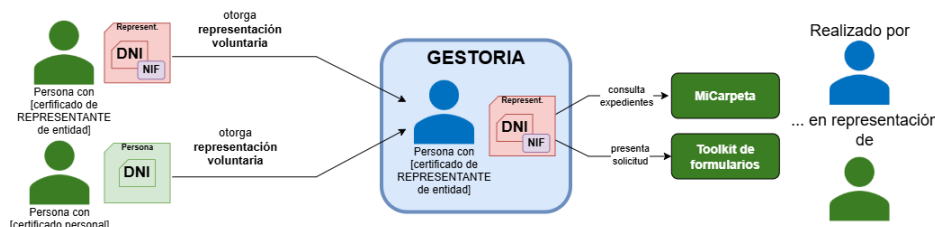
En detalle:

[1] – Representaciones Voluntarias

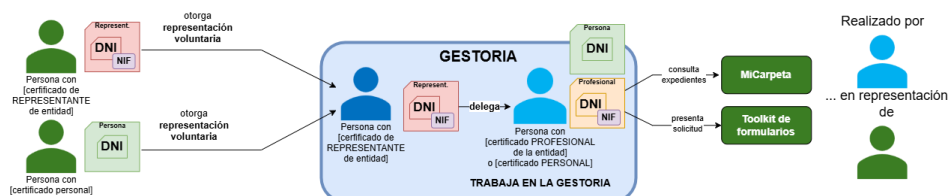
Una [persona] o una [entidad] **otorga una REPRESENTACION VOLUNTARIA** a una [persona] para que **actúe en su nombre** en un [tema] o [servicio](s)



Una [persona] o una [entidad] **otorga una REPRESENTACION VOLUNTARIA** a una [entidad] (*ej una [gestoria]*) para que **actúe en su nombre** en un [tema] o [servicio](s)

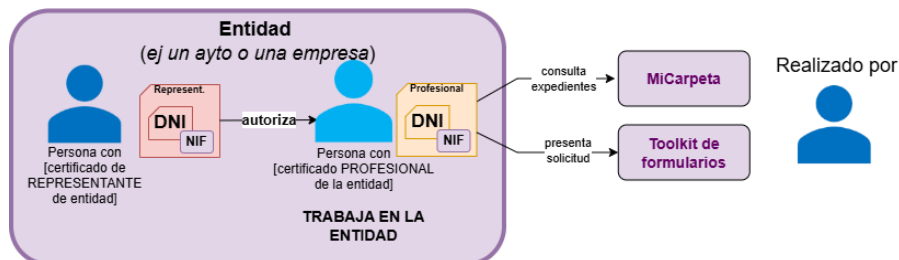


Una [persona] o una [entidad] **otorga una REPRESENTACION VOLUNTARIA** a una [entidad] (*ej una [gestoria]*) que **“delega”** en una persona trabajadora de la [entidad]

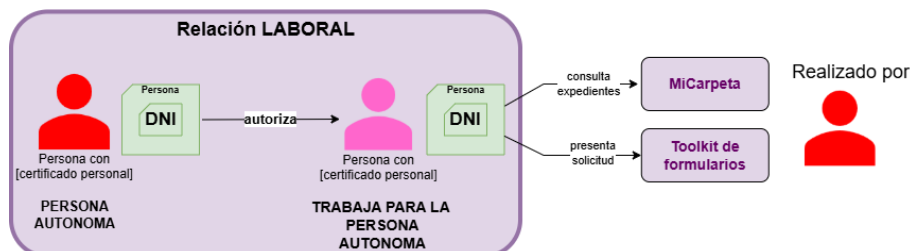


[2] – Autorizaciones

Una [entidad] (*ej: una administración o una empresa*) **AUTORIZA** a una persona que **trabaja en esta [entidad]** a que haga trámites para la [entidad]



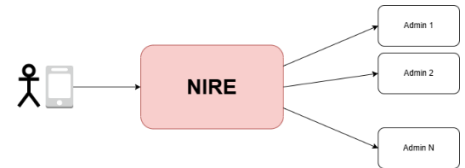
Una [persona] (*autónomo/a*) **AUTORIZA** a otra [persona] a que haga trámites para él



El objetivo en este punto de [NIRE Datuak] es que en [NIRE] se puedan **consultar** todas las [representaciones] y [autorizaciones] que ha “otorgado” una persona en las diferentes [administraciones] federadas en [NIRE]

Al igual que en el resto de [datos interoperables] de [NIRE] habrá que:

- **Analizar** el [dato]
- Trabajar la **semántica**: modelo, formato, etc
- **Construir** el [middleware] común y [conectores] con cada uno de los [Registros de Representaciones / Autorizaciones] de cada [Administración]
- **Documentar**



Las [administraciones] tendrán que construir [servicios] para devolver las [representaciones / autorizaciones] de una persona

3.6.1.3 Certificados / carnets / títulos / etc

En general son datos que son “producto final” de la *provisión* de un [servicio] (*habitualmente provisto a través de un [procedimiento administrativo]*)

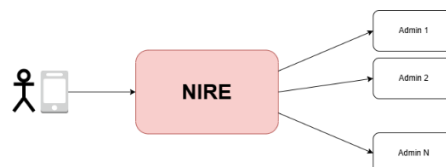
[1]	Datos “vivos” sobre la [tramitación] del [expediente] (ej: estado del expediente, notificaciones, pagos,...)	>	Se ven en [NIRE Karpeta]
[2]	Datos “producto” de la provisión de un [servicio] y que ya no cambian (ej: un certificado, un título, una acreditación,...)	>	Se ven en [NIRE Datuak]
[3]	Servicios no “administrativos” generalmente no basados en [expedientes] (ej: préstamos bibliotecarios, instalaciones deportivas, etc)	>	Se ven en [Servicios]

Algunos ejemplos de este tipo de [datos]:

- Certificados de profesionalidad / formación
- Certificado de discapacidad y dependencia
- Certificado de inscripción en el registro de Parejas de hecho
- Certificado de familia numerosa
- Voluntades anticipadas
- Acreditaciones de euskera
- Inscripción en Etxebide
- Certificados de Eficiencia Energética
- Inscripción como demandante de empleo
- Certificado de inscripción en el Registro de Animales (REA)
- ...

Al igual que en el resto de [datos interoperables] de [NIRE] habrá que:

- **Analizar** el [dato] y el origen en cada [administración]
- Trabajar la **semántica**: modelo, formato, etc
- **Construir** el [middleware] común y [conectores] con cada uno de los [orígenes de datos] en cada [Administración]
- **Documentar**



Las [administraciones] tendrán que construir [servicios] para devolver el [dato] desde el [repositorio] donde resida

3.6.2 NIRE Karpeta

Si en el punto anterior se ha hablado de los [datos] asociados a [NIRE Datuak] este punto se centra en [datos] asociados a [expedientes] (*datos “vivos”*): **[NIRE Karpeta]**

[1]	Datos “vivos” sobre la [tramitación] del [expediente] (ej: estado del expediente, notificaciones, pagos,...)	>	Se ven en [NIRE Karpeta]
[2]	Datos “producto” de la provisión de un [servicio] y que ya no cambian (ej: un certificado, un título, una acreditación,...)	>	Se ven en [NIRE Datuak]
[3]	Servicios no “administrativos” generalmente no basados en [expedientes] (ej: préstamos bibliotecarios, instalaciones deportivas, etc)	>	Se ven en [Servicios]

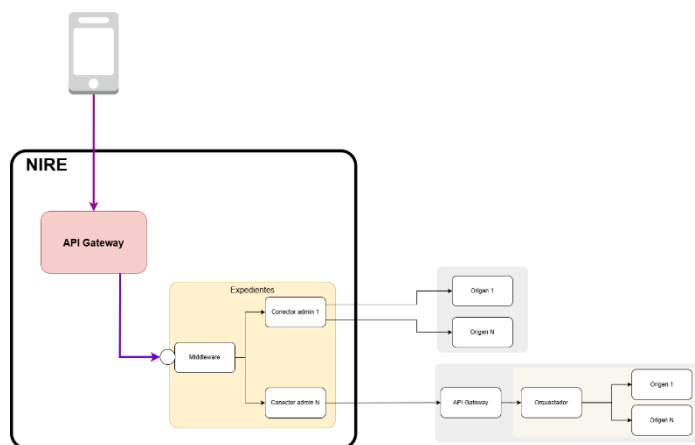
3.6.2.1 Datos asociados a expedientes

Las [administraciones] típicamente tienen múltiples aplicaciones que gestionan [expedientes], sin embargo, todas ellas en los últimos años han hecho un esfuerzo importante en crear [carpetas ciudadanas] en las [sedes electrónicas] donde proporcionan una *visión unificada* de los [expedientes] en los diferentes [gestores de expedientes] (*en caso de existir varios*)

Partiendo de la base de estas [carpetas] de las [sedes electrónicas], proporcionar los datos de [expedientes] para [NIRE] no debería implicar una gran complejidad técnica pero obviamente hay que analizar el caso de cada una de las [administraciones], en particular aquellas que puedan tener **múltiples [gestores de expedientes]** y no tienen actualmente una “vista unificada” de los [expedientes] en la [carpeta] (*se muestran en “secciones” independientes*)

... es decir, hay casos en los que pueden ser necesarias varias “llamadas” a la [administración] para tener todos los posibles [expedientes] en una **respuesta única** para la [app] con todos los [expedientes] “agregados”.

Este problema de “agregación” se resolver de dos formas que se muestran en la figura:



[1] – Hacer una “agregación” en el [conector] en el [middleware] de [NIRE]

El [conector] en el “lado” de [NIRE] hace múltiples “llamadas” a cada uno de los [orígenes de datos] en la [administración] y devuelve a la [app] una respuesta única

[2] – Hacer una “agregación” en “lado” de la [administración]

En el “lado” de la [administración] se hacen múltiples “llamadas” a cada uno de los [orígenes de datos] y se devuelve al [conector] en [NIRE] una respuesta única

(*en este caso se puede reutilizar el patrón [api-gateway] – [conector] de [NIRE] en el lado de la [administración]*)

Cualquiera de los dos casos anteriores en los que es necesaria una agregación de datos de diferentes orígenes es el caso más complicado de integración que se va a encontrar en el proyecto.



Otra opción posible -menos “elegante” desde el punto de vista de la persona usuaria final- es “pintar” los diferentes orígenes de [expedientes] de forma independiente en la [app]: cada origen de [expedientes] tendría su propio [conector] *simple* en [NIRE]

... esto implica que en la [app] una misma [administración] tendría múltiples “secciones” para [expedientes].

3.6.2.2 Otros datos de asociados a la tramitación de [expedientes]

Los [expedientes] se *apoyan* en otros sistemas donde también existen [datos] que son susceptibles de ser “mostrados” en [NIRE]:

Registro

El [registro] es una fuente importante de [datos] en algunas [administraciones]

Notificaciones / avisos

Cuando la [administración] tiene que informar / comunicar a las personas sobre algún hecho relevante de la tramitación del [expediente] y esta comunicación tiene que ser *fehaciente* (*por ejemplo se requiere a la persona subsanar una documentación presentada o se le informa -notifica- que se le ha abierto un expediente sancionador*) se utiliza una [notificación] que todas las [administraciones] hacen a través del [PUC] (*punto único de comunicación*)

Esto *simplifica* mucho la obtención de estos datos para [NIRE] puesto que NO es necesario obtener estos datos de cada una de las [administraciones] sino que basta con **consultar en el [PUC]**

3.6.2.3 Datos asociados a pagos

En el caso de los datos asociados a [pagos] se presentan dos casos:

[A] – Pagos NO domiciliados Es el caso de las [multas], las inscripciones a [OPE]s, tasas puntuales, etc
La [administración] genera una [liquidación] (*carta de pago con código de barras*) cuando se crea la “obligación de pago” para la persona.

En este caso se plantean dos opciones:

1 Crear un [conector] en [NIRE] para [pagos no domiciliados] para cada [administración] (*como el resto de [datos interoperables] que se están describiendo en el documento, las [administraciones] enviarían los [pagos no domiciliados] -las [liquidaciones]- ante una petición de la [app] a través de [NIRE]*)

2 Hacer que [MiPago] sea un *repositorio* de los [pagos no domiciliados] de todas las [administraciones], es decir, **cuando se genera la “obligación de pago”** (*por ejemplo, cuando se genera la [multa] en la administración y se notifica a la persona interesada*), la [administración] enviaría los datos del pago (*la [liquidación]*) a [MiPago]

De esta forma, todas las [liquidaciones] de todas las [administraciones] estarían en [MiPago] lo que permitiría a [MiPago] ofrecer servicios adicionales al [pago] como automatizar la conciliación diaria de [liquidaciones] pagadas por cualquier [medio de pago] a partir de los datos recibido en [batch] desde las [Entidades Financieras] (*las [administraciones] no tendrían que hacer esta conciliación diaria [batch] con cada [Entidad Financiera] ya que lo haría [MiPago]*)

ⁱ Estas funcionalidades adicionales de [MiPago] son un ejemplo de las funcionalidades que se podrían obtener si las [administraciones] *inician* todas las [liquidaciones] en [MiPago] en el momento de su generación (y no en el del pago como ahora)

... pero NO forman parte del presente proyecto.

En este caso, [NIRE] no tendría que “preguntar” a cada [Administración] por las [liquidaciones] sino que bastaría con consultar en [MiPago]

La opción más viable a corto plazo es la [1] -*consultar a las diferentes [administraciones] a través de [NIRE]-*, pero son opciones NO excluyentes y que pueden “convivir”.

La [administración] debería enviar:

- Liquidaciones pendientes de pago
- Liquidaciones ya pagadas
- Liquidaciones NO pagadas

[B] – Pagos Domiciliados

Es el caso de las tasas / impuestos que se liquidan periódicamente como las de [basuras], [agua], [IBI], etc donde las personas han facilitado a la [administración] una [cuenta corriente] donde quiere que “se les cargue” (“se les pase”) los recibos que se van generando en el tiempo.

En este caso la [administración] debería enviar a [NIRE] a petición de la [app]:

- Próximas liquidaciones que se van a pasar al cobro (*que se van a cargar en la cuenta*)
- Liquidaciones que ya se han cobrado
- Liquidaciones que se han intentado cobrar y no se ha podido (*devueltas*)

3.6.3 Calendario

En este *grupo* de datos se incluyen:

Citas con servicios de la [administración]

- Citas de [osakidetza]
- Citas con servicios de orientación en [Lanbide]
- Citas con servicios de atención a la ciudadanía
- ...

Eventos relevantes

- Certificados / carnets / autorizaciones de caducan
- Fecha de un examen de una [OPE]
- Fecha de devolución de un [préstamo bibliotecario]
- Reservas de [instalaciones deportivas]
- ...

Fechas relevantes en la tramitación de un [expedientes]

- Fecha límite de pago de una [liquidación] (*ej: una multa*)
- Fecha en la que se va a “pasar al cobro” un [pago domiciliado] (*ej: tasa de basuras*)
- Fecha limite para presentar una documentación de subsanación en la tramitación de un [expediente]
- ...



Algunos de estos [datos] de [calendario] posiblemente hay que *consultarlos* ad-hoc a la [administración] correspondiente (*ej: citas osakidetza / lanbide*), sin embargo, otros **se derivan** de [datos] que se consultan desde [NIRE] para otras áreas.

Ej: NO es necesario que las [administraciones] *construyan* un [servicio] ad-hoc que *devuelva* las fechas asociadas a [pagos] (*domiciliados o no domiciliados*) puesto que estos datos ya se *devuelven* a [NIRE] en la consulta de [pagos].

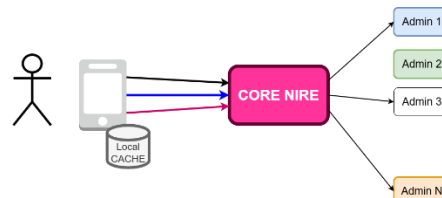
... es decir, [NIRE] ya está *de facto* obteniendo las *fechas* para mostrar en el [calendario] cuando consulta datos de [pagos], [expedientes], etc

... únicamente hay que “pintar” estas *fechas* en el [calendario] a partir de los datos obtenidos de las [administraciones]



A nivel técnico, en principio parece que el *lugar* más adecuado para tener esta lógica de *obtener* las fechas relevantes para mostrar en el [calendario] es la [aplicación] móvil / web

Hay que recordar que la [app] móvil / web hace *peticiones* “independientes” para cada [dato] (*pagos, expedientes, etc*) por lo que en la [app] móvil / web se deberá incluir la lógica para “extraer” las fechas relevantes a “pintar” en el [calendario]



3.6.4 Servicios

En los dos puntos anteriores han tratado los [datos] asociados a [NIRE Datuak] y [NIREKarpeta]: en este punto se tratan los [datos] a servicios “no administrativos” (*no basados en [procedimiento administrativo]*)

[1]	Datos “vivos” sobre la [tramitación] del [expediente] (ej: estado del expediente, notificaciones, pagos,...)	>	Se ven en [NIRE Karpeta]
[2]	Datos “producto” de la provisión de un [servicio] y que ya no cambian (ej: un certificado, un título, una acreditación,...)	>	Se ven en [NIRE Datuak]
[3]	Servicios no “administrativos” generalmente no basados en [expedientes] (ej: préstamos bibliotecarios, instalaciones deportivas, etc)	>	Se ven en [Servicios]

En esta área las [administraciones] tienen gran cantidad de datos a *mostrar* en [NIRE]; aquí se recogen algunos de ellos:

Préstamos bibliotecarios

La [red de bibliotecas de euskadi] utiliza un [sistema común](#) de [catálogo] y préstamo así que NO es necesario *consultar* a cada [biblioteca]; **basta con construir un conector con el [sistema común](#)**

Instalaciones deportivas

En este caso la integración es algo más compleja puesto que NO hay un sistema común a todas las [administraciones] de reserva de [instalaciones deportivas]

... sin embargo, hay unos pocos sistemas que son utilizados por las diferentes [administraciones], así que construyendo los [conectores] con los sistemas más *extendidos* se pueden tener los [datos] de muchas [administraciones] *reutilizando* el mismo [conector]

Transporte

El [transporte] es un área compleja y que probablemente NO se aborde a corto plazo pero que puede aportar [datos] útiles para las personas como es el caso de la información de las [tarjetas de transporte]



Recordar que al igual que con el resto de [datos], el objetivo de [NIRE] no es sustituir las [app]/web que cada [administración] tiene sobre el transporte sino complementarlas

A nivel muy general (*sin pretender precisión técnica, únicamente con el objetivo de describir el escenario a nivel general*) hay dos [modelos] en el caso de las [tarjetas de transporte]:

Card/Media Based Ticketing (MBT)

Transacciones “contra” una [tarjeta] sin vínculo con la [persona usuaria] y que hay que recargar

Es el modelo más utilizado actualmente

Las [transacciones] se **registran** en la [tarjeta]: cuando se hace [tap] en la [canceladora], se *descuenta* el coste del viaje del [saldo] de la [tarjeta] (el [saldo] está en la propia tarjeta)

No se *conoce* a la [persona usuaria] así que NO se pueden aplicar tarifas personalizadas a cada persona pero si se pueden *desplegar [tarjetas] para [colectivos]* concretos a los que se aplican [tarifas] especiales

Account Based Ticketing (ABT)

Transacciones “contra” una [cuenta de persona usuaria] respaldada por:

- Un saldo que la persona recarga
- Una [tarjeta de crédito/débito] de la que se “descuenta” el coste

Las [transacciones] se **registran** en el [backend] (servidor) en una [cuenta] asociada a la [persona usuaria]: cuando se hace [tap] en la [canceladora], la [transacción] se envía al [backend] (servidor) y ahí se *descuenta* el coste del viaje

- Del [saldo] de la [cuenta de la persona usuaria] (y que ésta debe cargar)
- De una [tarjeta de crédito/débito] asociada a la [cuenta] (SVA: Store Value Accounts)

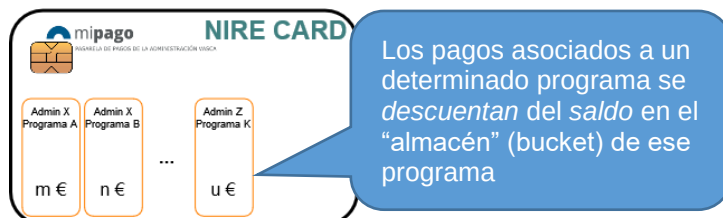
El sistema de tarifas está en el [backend] (servidor); el dispositivo cliente es *simplemente un sistema de identificación* por lo que se pueden aplicar tarifas personalizadas a cada persona en función del uso en el tiempo, trayectos, etc

[NIRE] -*complementariamente a las [app]/web de las [administraciones]*- podrían mostrar información sobre estas [tarjetas de transporte]: saldo, usos, etc

NIRE-Card

Las [Administraciones Públicas Vascas] están trabajando en la viabilidad de crear una [Tarjeta prepago] ([NIRE Card]) que permita la realización de **pagos** por parte de la [persona titular] en el marco de **diferentes [programas de ayuda]** de diferentes [Administraciones Públicas] que son las que **aportan los fondos** y pre-fijan las **condiciones de uso** tanto para la persona beneficiaria como para los [comercios] adheridos.

La tarjeta [NIRE] será cargada para cada [programa de ayuda] por la [administración] impulsora y en un momento dado, la tarjeta puede tener fondos disponibles para ser gastados en varios [programa de ayuda] (*varios [buckets]*):



Si una [Administración X] lanza un [programa de ayuda] a [comercios], el sistema funcionaría de la siguiente forma (*explicado con un nivel de abstracción muy alto*)

1. La [administración] **abre** un [programa de ayuda] en dos pasos:
 - a) **Ingres**a la [dotación presupuestaria] del [programa de ayuda] en una [cuenta corriente] de la [Entidad Financiera] que da soporte a [NIRE Card]
 - b) Utilizando las herramientas de [MiPago] envía a la [Entidad Financiera] todos los **parámetros** del [programa de ayuda] (*fechas, límites geográficos, tipo de comercio, importes máximos, etc*)
2. Los [comercios] **solicitan** su **adhesión** al [programa de ayuda] utilizando los medios que la [administración] impulsora disponga para este fin
3. Las [personas] **solicitan** ser beneficiarias de la [ayuda]
4. La [Administración] estudia y resuelve estas solicitudes de [comercios] y [personas]

La [Administración] periódicamente (*ej: cada hora*) envía utilizando un **[mecanismo de interoperabilidad]** a la [Entidad Financiera] emisora de la [tarjeta NIRE]

 - **[comercios]** que se han ido adhiriendo al [programa de ayuda]
 - El **dinero** con el que pre-cargar la [tarjeta NIRE] para cada [persona]
5. Al tratarse de una **[tarjeta] de pago normal**, la [persona] consumidora simplemente tendrá que hacer un [pago con tarjeta] en el [comercio]

En el momento de **autorizar** la transacción de [pago con tarjeta] la [Entidad Financiera] concesionaria del servicio debería:

- **Comprobar que se cumplen las condiciones** del [programa de ayuda]
- **Comprobar el [saldo]** en la [tarjeta NIRE] del [bucket] correspondiente

Para el [comercio] al ser un *pago con tarjeta*, el proceso es totalmente transparente, recibiendo la *ayuda* de manera inmediata y sin necesidad de enviar ningún justificante a la [Administración]

... la [administración] por otro lado:

- Tiene la seguridad de que el pago se ha realizado cumpliendo las condiciones del [programa de ayuda] (*ej: en un comercio adherido*)
- Recibe de la [Entidad Financiera] los datos de las transacciones (*básicamente para tener información analítica/estadística*)



[NIRE] sería el "lugar" donde las personas podrían consultar:

- **Saldo** de los [buckets] asociados a [programas de ayuda]
- **Movimientos** en cada [bucket] de [programa de ayudas]
 - Cargas (*ingresos*) por parte de la [administración] impulsora
 - Consumos por parte de la persona beneficiaria

3.7 Interfaz de persona usuaria de administración de NIRE

3.7.1 Descripción general de la interfaz de administración

En este punto se describe a muy alto nivel una **interface de persona usuaria (UI)** de [administración del sistema] que es necesaria, entre otras cosas, para:

Parametrizar Para “pintar” la [UI] (*web / móvil*) de [NIRE] (*ver más adelante un resumen de los prototipos*) y como base de la [interoperabilidad] es necesario tener datos de parametrización:

Un registro de [administraciones] El registro tendrá al menos dos niveles:

```
Grupo de Administraciones
+- Administración 1
+- Administración 2
+- ...
```

Un registro de [datos interoperables] Cada [dato interoperable] tendrá asociados unos meta-datos

- Nombre / descripción / etc
- Información sobre [protección de datos]
- Área de la [app] en la que se muestra el [dato interoperable]
- Tipificación:
 - Tipo de dato: carnet, certificado, expediente, etc
 - Catalogación: [temas] y [hechos vitales]
 - etc
- Las [administraciones] que proporcionan [datos] del [dato interoperable] (*orígenes de datos*) y la parametrización del [conector] correspondiente

```
Dato interoperable
+- Administración 1 - Parámetros del [conector]
+- Administración 2 - Parámetros del [conector]
+- ...
```

Los parámetros del [conector] entre otros pueden ser:

- url del [servicio] en la [administración]
- parámetros de la autenticación mutua [CORE NIRE] <-> [administración] (*ver punto de identidad y autenticación*)
- contacto técnico / funcional
- ...

■ Etc

Gestión de las [retrieve rules]

Parametrizar las reglas que *manejan* la *lógica* que utiliza [NIRE] para consultar o no un [origen de datos] que como mínimo pueden ser:

- | | |
|---|---|
| a) Competenciales | Para un [dato interoperable] hay solo una/varias [administraciones] competentes |
| b) Relación persona - administración | Una persona NO tiene datos en todas las [administraciones] |
| c) Actualización de datos | Solo hay que consultar a la [administración] si el dato se ha actualizado |
| d) Última vez que se han recuperado los datos | No consultar los datos en un [origen de datos] si no ha pasado un tiempo X desde que se consultaron |

Trazar peticiones

Trazar (*seguir el camino*) de una [petición de interoperabilidad] por los componentes del [CORE NIRE] con el objetivo de resolver incidencias.

Realizar tareas de auditoría

Consultar el [registro] de [peticiones de interoperabilidad] y tener información sobre quién y cuándo ha consultado un [dato]

**Ver datos
analíticos**

Desde la aplicación se deberían tener una visualización mínima de [datos analíticos]:

Ej: Llamadas a [datos interoperables] por [grupo de administraciones] / [administración] / [origen de datos] y [rango temporal]



Quizá la visión analítica completa debería estar en el [Observatorio de Administración Digital] y aquí “mostrar” algún [widget] muy concreto

Otras

Otras funciones de administración del sistema

3.7.2 Gestión de Autorizaciones

Un aspecto importante de esta [aplicación de administración del sistema] es la [gestión de autorizaciones]: quién puede hacer qué.

Desde la propia [aplicación de administración] las [administraciones] auto-gestionarán las [autorizaciones] de las personas en su ámbito:

- A nivel de [grupo de administraciones] - [administración] (en el [registro de administraciones])

```
Grupo de Administraciones
+- Administración 1
+- Administración 2
+- ...
```
- A nivel de [dato interoperable] – [administración]

```
Dato interoperable
+- Administración 1 - Parámetros del [conector]
+- Administración 2 - Parámetros del [conector]
+- Administración 3 - Parámetros del [conector]
+- ...
```

... de esta forma:

- Una persona que tiene [autorización] a nivel de [grupo de administraciones] tiene [autorización] en todas las [administraciones] de este [grupo de administraciones]:

```
Grupo de Administraciones
+- Administración 1
+- Administración 2
+- ...
```

- Una persona con [autorización] en una [administración] tiene también [autorización] en los [datos interoperables] para esta [administración]

Ej: si una persona está [autorizada] en la [administración 1] estará [autorizada] en la parametrización del [conector] de la [administración 1] en [dato interoperable A] y [dato interoperable B]

```
Grupo de Administraciones      Dato interoperable A
+- Administración 1            +- Administración 1 - Parámetros del [conector]
+- Administración 2            +- Administración 2 - Parámetros del [conector]
+- ...                         +- Administración 3 - Parámetros del [conector]
                                +- ...
                                Dato interoperable B
                                +- Administración 1 - Parámetros del [conector]
                                +- Administración 2 - Parámetros del [conector]
                                +- Administración 3 - Parámetros del [conector]
                                +- ...
```

- Una persona que tiene [autorización] a nivel de [dato interoperable] tiene [autorización] en todas las [administraciones] de ese [dato interoperable]

```
Dato interoperable
+- Administración 1 - Parámetros del [conector]
+- Administración 2 - Parámetros del [conector]
+- Administración 3 - Parámetros del [conector]
+- ...
```

Este tipo de [autorización] no debería ser habitual (pero podría ser posible)

Por simplicidad en cada nivel inicialmente (habrá q analizarlo en detalle) se identifican dos **perfiles / roles** a los que se podrán *asignar* personas de las [administraciones]

- **Técnico** Podrá realizar las acciones técnicas que se identifiquen
- **Responsable** Tiene todas las [autorizaciones] del rol [técnico] y además la capacidad de asignar nuevas personas al perfil / rol [técnico] o [responsable]

... además, existirá un perfil/rol *especial* (**responsable horizontal**) que tendrá [autorización] total sobre cualquier parámetro técnico o funcional del sistema en cualquier nivel



La gestión de [autorizaciones] será **distribuida** de forma que una persona con [autorización] suficiente podrá **“delegar” la administración en otras personas de su organización**: NO existe una gestión de [autorizaciones] centralizada
Idealmente el sistema funciona así:

1. Una persona [responsable horizontal] asigna un rol de [responsable] a una persona de cada [administración]
2. Las personas [responsable] de cada [administración] **autónomamente** gestionan las [autorizaciones] en el ámbito de esta [administración] asignando [autorizaciones] de rol [técnico] o delegando en otras personas [responsables]

3.8 Mensajería PUSH

La [app móvil] y [web] producto del proyecto [NIK]/[NIRE] es una **oportunidad única para crear un [canal de comunicación] común de todas las [administraciones vascas]**: un medio más (*adicional al email o el teléfono*) por donde las [administraciones] y [ciudadanía] pueden **interaccionar**.



Es deseable que sea [NIK] / [NIRE] el [canal] común móvil a utilizar por las [administraciones vascas], siempre con la visión de “neutralidad” e “independencia” de una administración concreta

La alternativa de que cada [administración] cree su propia [app] y tenga su propio [canal] crearía “dispersión” y “confusión” en las personas usuarias que se encontrarían con [notificaciones push] procedentes de una gran cantidad de aplicaciones de la [administración]

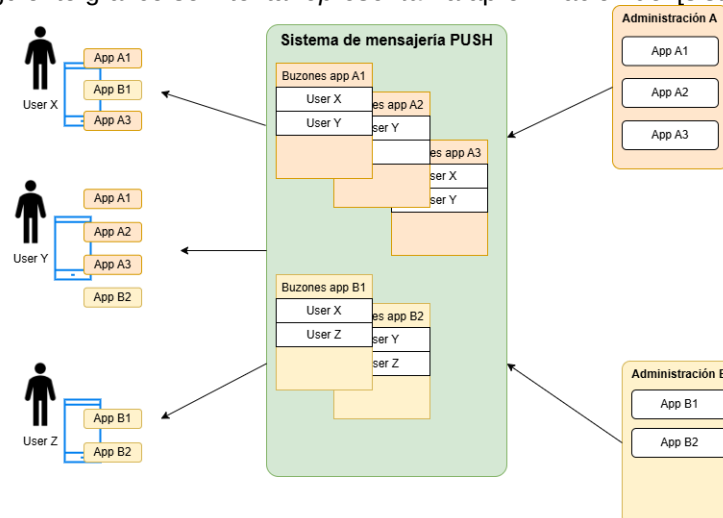
En cualquier caso, el [sistema de mensajería PUSH] que se construya en el marco del proyecto [NIK-NIRE] debe ser **independiente de la [app]** (*NIK, NIRE o cualquier otra*) y **poder ser utilizado en cualquier [app]** de cualquier [administración]. Este módulo tiene por lo tanto vocación de **constituirse en una pieza común más de la [administración digital]** como lo son [MiPago], [NISAE] o el [PUC]

El sistema descrito a continuación está basado en la **experiencia de éxito de la actual aplicación [NIK]** del cual se *toman* funcionalidades y aproximación técnica.



Aunque el [sistema de mensajería PUSH] se *construye* en el ámbito del [programa de proyectos NIK-NIRE], el objetivo es que **pueda ser utilizado por cualquier aplicación más allá de [NIK-NIRE]**

En el siguiente gráfico se intenta *representar* la aproximación del [sistema de mensajería PUSH]



Las [administraciones] utilizan el **sistema común** para enviar [mensajes] a [buzones] asociados a la [app] y [usuario] (*o dispositivo*)



En el sistema propuesto, las [administraciones] envían [mensajes] a [apps] a través de una infraestructura común en la que **se debe garantizar que no se tiene acceso al contenido del mensaje** (*no debe ser posible ver qué envía una [administración] a un [dispositivo]*)

... para asegurar este requisito se utiliza un **[cifrado]** utilizando una pareja [clave pública-privada] de forma que los [mensajes] almacenados en el sistema **únicamente son visibles por la entidad receptora**.

En una visión general de alto nivel el sistema podría funcionar de la siguiente forma:

3.8.1 **Enrollment de [app]**

3.8.1.1 Dispositivo móvil

El objetivo de esta fase de [enrollment] es la **creación de un [buzón]** donde se dejan los [mensajes] para ser “recogidos” por el [dispositivo]



Hay dos posibilidades para crear los [buzones]:

- Que estén asociados al [dispositivo] (*independientemente de la persona que esté “detrás” de la [app]*)
- Que estén asociados a la [persona usuaria] en cuyo caso **antes** de hacer el [enrollment] de la [app móvil], **es imprescindible identificar a la [persona usuaria]** (*ver punto 3.3*)
Si el [buzón] está asociado a la [persona usuaria], el mismo [buzón] puede ser utilizado en [dispositivo web] (*navegador*)

① En el caso de [NIRE], el [buzón] estará asociado con toda seguridad a la [persona usuaria]

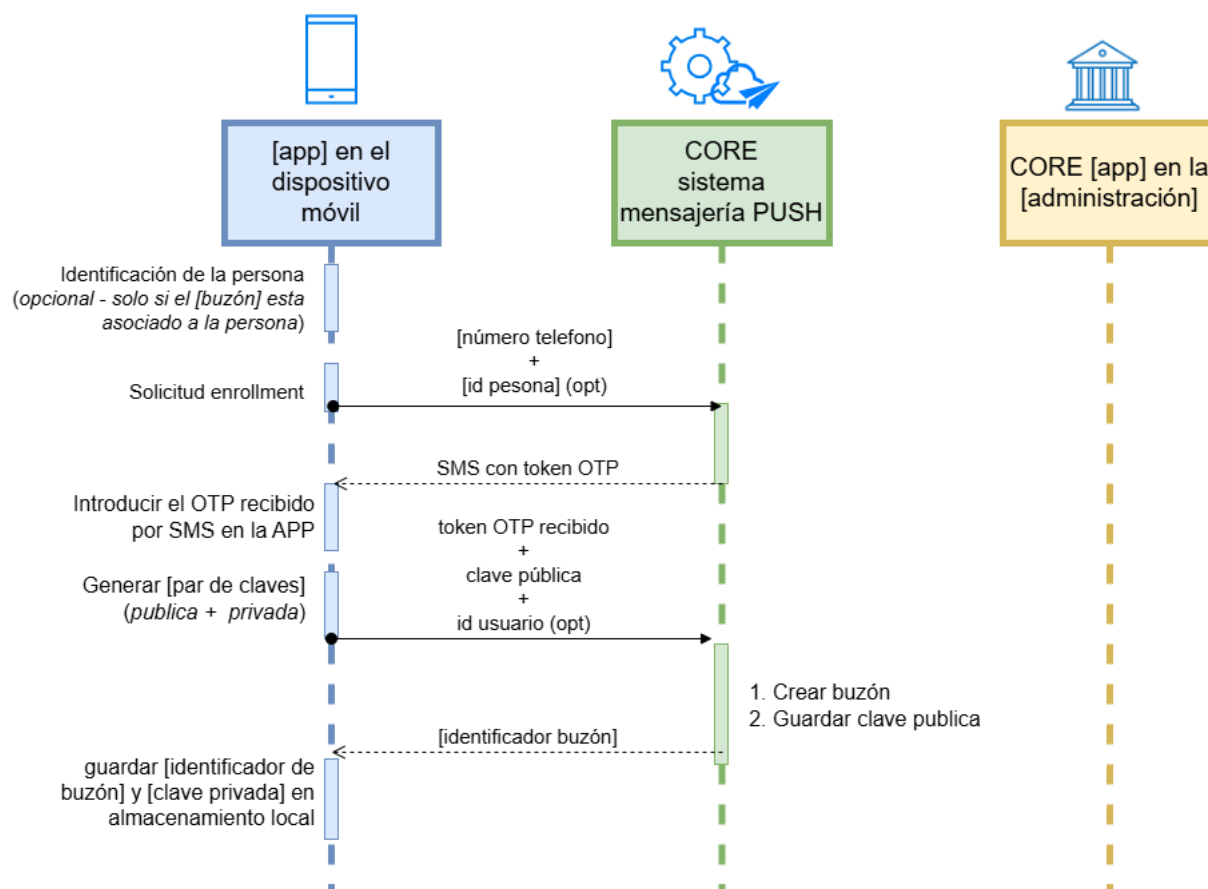
Durante la instalación de la [app móvil] en la **fase de [enrollment]** (*emparejamiento*) del [dispositivo] en la [app] se crea

- Un **[buzón]** (*una “consigna”*) **asociado al [dispositivo] o a la [persona]** donde sistemas externos (*ej: una [administración]*) pueden “dejar” mensajes a [notificar] a la [app]
- Un par [clave pública] – [clave privada] que se utilizan para cifrar los [mensajes] que se “dejan” en el [buzón] y evitar que nadie que no sea el destinatario pueda ver el [mensaje]:
 - La [clave pública] se almacena **remotamente en el [servidor] (CORE)**
 - La [clave privada] se almacena **localmente en el [dispositivo] móvil**
 - La [clave pública] se utiliza **en el [servidor] (CORE) para cifrar** los [mensajes] que un [sistema externo] (*ej: una administración*) quiere enviar a un [dispositivo]
 - La [clave privada] se utiliza **en el [dispositivo] móvil para descifrar** los [mensajes] que se envían por parte de una [administración] cifrados con la [clave pública] que está en el servidor.

Una **propuesta** del proceso de [enrollment] de una [app móvil] sería que tras instalar la [app] hay un **[emparejamiento]** (*enrollment*) en el que se crean el [buzón] y la [pareja de claves] (*clave pública-clave privada*):

- a. La [app] cifrando con una clave [simétrica] (*conocida por la [app] y el [sistema de mensajería PUSH]*) se envía una **[solicitud de emparejamiento]** al [CORE del sistema de mensajería PUSH] que incluye el [teléfono]
- b. El [CORE del sistema de mensajería PUSH] envía al [teléfono] un [OTP] (*one time password*) mediante [SMS]
- c. La persona usuaria introduce el [OTP] recibido en la [app]
- d. La [app] en este momento:
 - Genera una **localmente** una pareja de claves publica y privada
 - Hace una **segunda petición** al [CORE del sistema de mensajería PUSH] adjuntando:
 - El [ID de la persona usuaria] en el caso de que el [buzón] esté asociado a una [persona usuaria] (*recordar que la persona **debe** estar previamente autenticada en la [app] -ver punto 3.3-*)
 - El [OTP] recibido por [SMS], confirmando de esta forma que la persona usuaria está en posesión del [dispositivo]
 - La [clave publica] generada (*se utilizarán más adelante para enviar [mensajes]*)
- e. La parte [CORE del sistema de mensajería PUSH]:
 - Verifica si existe o no un [buzón] asociado a la [persona usuaria] y lo crea si no es así
 - Guarda la [clave pública] recibida y la asocia al [buzón] de la [persona usuaria]

Lo anterior representado en forma de [diagrama de secuencia]:



Una alternativa a esta propuesta **si finalmente se utilizan [passkeys] en la [identificación] de la persona usuaria en la [app]** (ver punto 3.3) es utilizar la pareja clave pública / privada que se generan con el [passkey]

... es una alternativa de la que en este momento se desconoce la viabilidad real pero que sobre el papel podría ser posible.



Una *virtualidad* del sistema de [enrollment] es que se “encarga” de asegurar que el [dispositivo móvil] efectivamente está en posesión de la persona usuaria mediante el intercambio inicial del [OTP] mediante [SMS], *liberando* de esta funcionalidad a las aplicaciones de las [administraciones]

3.8.1.2 App Web (desktop)

En el caso de un [dispositivo móvil] es posible crear un **[buzón] asociado a un [dispositivo]** (*NO asociado a una [persona usuaria]*) y por lo tanto NO se requiere una [autenticación] (*identificación*) de la persona para enviar / recibir [mensajes]

 Esto es posible ya que en la fase de [enrollment] utilizando el [OTP] por [SMS] para asegurar que se *controla* el [dispositivo] que va a recibir los [mensajes]

Sin embargo, en el caso de una [app web] (*desktop*) **es necesario identificar a la [persona usuaria]** para poder *consultar* el [buzón]

Además, se plantea otro reto ya que al NO existir la fase inicial de [enrollment] en la que se generan la pareja de claves pública y privada que se almacenan en el CORE (*la clave pública asociada al [buzón]*) y dispositivo cliente (*la clave privada*) hay que resolver **cuándo se generan esta [pareja de claves]** fundamentales para la privacidad de las comunicaciones.

Algunas alternativas de solución pueden ser:

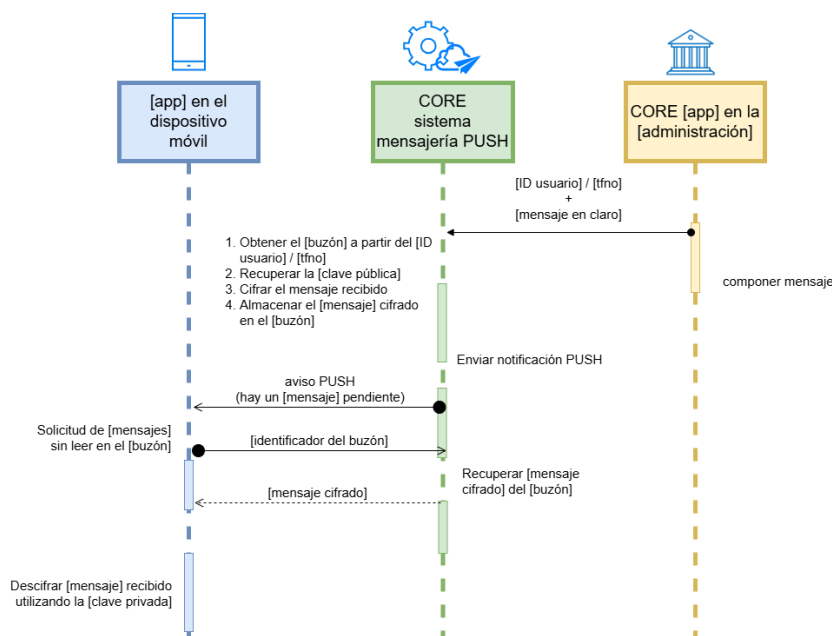
Utilizar [passkeys] (webauthn)	Si finalmente se utilizan [passkeys] en la [identificación] de la persona usuaria en la [app] (<i>ver punto 3.3</i>) es utilizar la pareja clave pública / privada que se generan con el [passkey] ... es una alternativa de la que en este momento se desconoce la viabilidad real pero que sobre el papel podría ser posible.
Generar una [pareja de claves] ad-hoc para la sesión web	Una vez [autenticado] (<i>identificado</i>) generar una [pareja de claves] que únicamente se utilizará mientras dure la sesión desktop
Otras	...

3.8.2 Envío de mensajes

Cuando una [administración] quiere enviar de forma segura y confidencial un [mensaje] a cualquier [app] de cualquier [administración] necesita bien el [ID de usuario] o el [teléfono] (*en el caso de enviar a un [dispositivo]*):

1. La [administración] en el [servidor] recupera el [identificador único del buzón] y la [clave pública]
2. Cifra el [mensaje] a enviar utilizando la [clave pública] (*el mensaje solo podrá ser descifrado en la [app] en el [dispositivo móvil] utilizando la [clave privada] que únicamente reside ahí*)
3. La [administración] *llama* a un servicio del [CORE del sistema de mensajería PUSH] indicando el [ID usuario] / [teléfono] y adjuntando el [mensaje] en claro
4. El [CORE] del [sistema de mensajería PUSH] *simplemente*:
 - a. A partir del [ID usuario] / [teléfono] obtiene
 - El [buzón] asociado
 - La [clave publica] generada en el [enrollment]
 - b. Cifra el [mensaje] recibido utilizando la [clave pública]
 - c. “pone” el [mensaje cifrado] en el [buzón]
 - d. Avisa al [dispositivo móvil] / web de que “tiene un mensaje disponible” utilizando una [notificación PUSH] (*server -> dispositivo móvil*)
5. La [app] en el [dispositivo móvil] / [web]
 - a. Al recibir el aviso (*la [notificación PUSH] recibida*) hace una *llamada* al [CORE] del sistema de mensajería PUSH con el [identificador único del buzón] (*que tenía almacenado en local*) ... como respuesta recibe el [mensaje cifrado] que la [administración] había *dejado* anteriormente en el [CORE] del [sistema de mensajería PUSH] (*o los mensajes si había varios pendientes*)
 - b. La [app] en el [dispositivo móvil] utilizando la [clave privada] (*que tenía almacenada en local*) descifra el [mensaje cifrado] recibido

Lo anterior representado en forma de [diagrama de secuencia]:

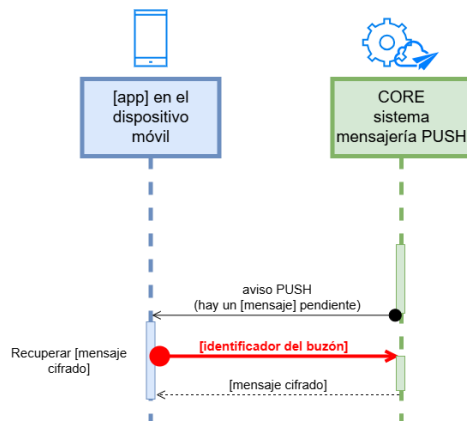


Como se puede observar, utilizando la pareja [clave pública] – [clave privada] se envía un [mensaje] desde la [administración] a la [app] en el [dispositivo móvil] utilizando el [sistema común de mensajería PUSH] **sin que el [mensaje en claro] quede almacenado en el [CORE del sistema de mensajería PUSH]**



Con el objetivo de *simplificar* la explicación, se ha *omitido* que en la llamada que hace la [app] desde el [dispositivo móvil] al [CORE] del [sistema de mensajería PUSH] para recuperar el [mensaje cifrado] se ha de “asegurar” que el dispositivo que *reclama* el [mensaje cifrado] es quien dice ser.

Para esto se vuelve a utilizar la pareja [clave pública] – [clave privada]:



En la *llamada* señalada en **rojo**, el [CORE] debe tener certeza de que el *llamante* (*la [app]*) puede tener acceso al [mensaje] pendiente

Para ello:

1. La [app] en el [dispositivo móvil] “firmará” la *llamada* utilizando la [clave privada] (*que solo está en la [app]*)
2. En el [CORE] del [sistema de mensajería PUSH] se verificará que esta “firma” es válida utilizando la [clave pública] del [buzón]

Hay otro punto del sistema que también por simplificar la exposición se ha omitido: **¿cómo se envían las [notificaciones PUSH] al [dispositivo móvil] desde el [CORE] del [sistema común de mensajería PUSH]?**



Para hacer estos envíos de [notificaciones PUSH] habitualmente se utilizan sistemas cloud como [Google Firebase Messaging] (FCM) o [OneSignal] que entre otras muchas funcionalidades permiten enviar [notificaciones PUSH]:

- A [dispositivos móviles] concretos (*unicast*)
- A un grupo de [dispositivos móviles] (*multicast*)

Estos sistemas cloud habitualmente se basan en un [token] asociado a la [app móvil] que ha de “custodiarse” en el [servidor] desde donde se *inicia* la [notificación PUSH] y utilizarse cuando se quiere enviar una [notificación PUSH]

... en este caso el [token] se almacenará en el [buzón] asociado a la instalación concreta de [app] en el [CORE] del [sistema común de mensajería PUSH] y en concreto

El [token] del sistema de notificación cloud (ej: *firebase*) se creará y almacenará en el [buzón] en el proceso de [enrollment] detallado anteriormente y si es necesario, el [CORE] del [sistema común de mensajería PUSH] se *responsabilizará* del **refresco del [token]** puesto que algunas plataformas (ej: *firebase*) pueden requerirlo

En cualquier caso, el sistema debe permitir enviar [mensajes PUSH] a:

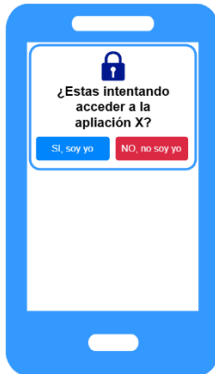
- Las plataformas [móvil] más utilizadas (*Android / IOS*)
- Desktop (*interfaz navegador web de escritorio en las versiones más utilizadas de [Chrome], [Edge], [Safari] y [Mozilla] según [referencia](#)*)

3.8.3 Mensajes PUSH interactivos

La mayor parte de las ocasiones desde el [CORE] de las aplicaciones se envían [mensajes PUSH] **informativos**

... pero hay ocasiones donde se requiere una **acción** por parte de la persona usuaria

El ejemplo más habitual es el de **soporte a la [autenticación]**



El [dispositivo móvil] se utiliza como [segundo factor] de forma que cuando alguien quiere entrar a un recurso protegido se envía una **confirmación vía [notificación PUSH]** al [dispositivo móvil] (*segundo factor*) que muestra a la persona usuaria un mensaje como el de la figura.

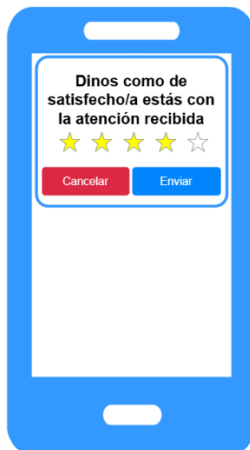
... dependiendo de la respuesta de la persona usuaria, la [aplicación] *origen* tomará una acción u otra

Además de los [mensajes PUSH] de segundo factor en la [autenticación], los [mensajes PUSH] interactivos se pueden utilizar para otros escenarios como:

- Encuestas (*polls*): la persona usuaria puede elegir entre varias opciones
- Feedback: se pide el [grado de satisfacción] después de hacer un trámite
- Consentimientos / autorizaciones
- etc

La implementación de [mensajes PUSH interactivos] es relativamente *simple*: se utiliza un [mensaje] que el contiene las “instrucciones” para que la [app] sea *capaz* de mostrar el [mensaje interactivo]

Por ejemplo, el [mensaje] que la [administración] *deja* en el [buzón] del [dispositivo móvil] puede contener instrucciones para hacer un [rating] en formato [JSON] como:



```
{
  "message" : {
    "type" : "RATING",
    "rating_scale" : "STARS" // podría ser NUMERIC / FACES / etc
    "title" : "Satisfacción con la atención",
    "detail" : "Dinos cómo de satisfecho/a estás con la atención recibida",
    "scale_range" : [0..5]
  }
}
```

En función de estas “instrucciones”, la [app] *pintará* la [UI] de [rating] (*en este caso*) y enviará el resultado al [CORE] del [sistema de mensajería PUSH] que a su vez lo hará llegar a la [administración] que en origen envió el mensaje indicando el [ID usuario] / [teléfono] con lo que *sabrà* de “quién” viene la respuesta

3.8.4 **Suscripciones: multicast a múltiples dispositivos**

Hasta ahora se ha tratado de envío de [notificaciones PUSH] a [dispositivos móviles] individuales (*unicast*), sin embargo, en ocasiones también debería ser posible enviar [notificaciones PUSH] a un grupo de [dispositivos móviles] (*multicast*)

Esta es una funcionalidad que los sistemas cloud de [notificación PUSH] como [[Google Firebase](#) Messaging] ([FCM](#)) resuelven con el concepto de **[topics]**

1. Una persona administradora del sistema **crea un [topic]** en la [consola de administración de firebase]



Es posible la creación de un [topic] programáticamente desde lógica de servidor (CORE) pero la creación puede *demorarse* un tiempo indeterminado de hasta un día

2. **Los [dispositivos móviles] se suscriben al [topic]**

- a. Desde el propio [dispositivo móvil] (*usado habitualmente cuando la suscripción la “decide” la persona usuaria*)
- b. Desde el [servidor] (*usado habitualmente cuando la suscripción la “decide” la [aplicación]*)

3. Desde el [servidor] se envía un mensaje al [topic] que [firebase] hace llegar a todos los [dispositivos móviles] suscritos

El [sistema de mensajería PUSH] que se está describiendo es *en esencia* un *recubrimiento* de un sistema cloud de [notificación PUSH] como [firebase] y por lo tanto funcionaría de una forma similar:

El [sistema de mensajería PUSH] ofrecerá servicios para que cualquier [administración] pueda:

- Crear un [topic] asociado a una [aplicación]
- Suscribirse un [buzón] a un [topic]
- Enviar un [mensaje] a un [topic] para que sea distribuido a todos los [dispositivos móviles]



A priori se plantea un *inconveniente* del [multicast] a múltiples dispositivos:

Cuando se envía un [mensaje] a un **único dispositivo** (*unicast*) la confidencialidad del contenido se puede asegurar ya que el [mensaje] puede ser cifrado / descifrado con el par de claves asociado al buzón.

... pero cuando el mismo [mensaje] ha de enviarse a **múltiples [dispositivos móviles]** NO puede utilizarse el cifrado.

Únicamente se puede:

1. Dejar en el [buzón] de los [dispositivos móviles] suscritos al [topic] el [mensaje] confidencial cifrado con la [clave pública] (*como habitualmente*)



Evidentemente esta aproximación tiene un problema de escalado si se quiere hacer un [multicast] a millones de [buzones] pero se considera que no va a ser el caso ya que a lo sumo se hará [multicast] a unos pocos cientos de miles de [buzones]
... hay que evitar la optimización prematura

2. Difundir (*multicast*) otro [mensaje] NO cifrado (*en claro*) que NO contenga información confidencial (*ej: tienes un mensaje de [NIRE]*)
3. Cuando la persona “pincha” en el [mensaje] y se abre la [app], se *descargará* el [mensaje cifrado] desde el [buzón] y se descifrá en local (*como habitualmente*)

En cualquier caso, a pesar de que en el presente documento se intenta hacer una descripción lo más detallada posible para que las empresas ofertantes puedan hacer una evaluación lo más ajustada posible del proyecto al que presentan oferta, durante la ejecución del proyecto aparecerán necesidades a esta a las que habrá que dar solución.

3.8.5 Datos del sistema

Al igual que se ha detallado anteriormente hay que tener datos sobre el sistema a varios niveles

3.8.5.1 Monitorización / Observabilidad

1 Monitorización de los componentes del sistema	Obtener información sobre el estado de los sistemas de la infraestructura : uso de CPU, memoria, comunicaciones, si los servicios están activos o no, etc
2 Observabilidad: estado del sistema en base al “desempeño” y las interacciones entre componentes	Se utilizarán datos asociados al “desempeño” del sistema como [número de mensajes enviados y recogidos] <i>(si en algún momento este número es bajo respecto a la media se podría inferir que hay algún tipo de problema)</i>

3.8.5.2 Datos analíticos

Se identificarán algunos [datos analíticos] (*métricas / indicadores*) relevantes sobre el sistema como por ejemplo simplemente:

Métrica / indicador	Dimensión (<i>combinable</i>)
- Mensajes enviados - Mensajes recogidos	- fecha - administración - aplicación - buzón - topic

Estos [datos analíticos] además de mostrarse en la [UI de administración] (*ver más adelante*) se enviarán al [Observatorio de Administración Digital]

3.8.5.3 Audit

Todos los **usos** del [sistema de mensajería PUSH] deben guardar información de [auditoría] (*audit*) para conocer:

- Quién** ha utilizado el sistema (*habitualmente una [aplicación] de una [administración] pero también puede ser una persona desde la [consola de administración]*)
- A qué [buzón]** se ha enviado un [mensaje]
- Cuándo**
- Si se ha recogido el [mensaje] o no** (*y en qué momento*)
- ... y cualquier otra información que se considere relevante de cara a la auditoría del uso.



Los datos de [audit] deben estar **disponibles** para su consulta:

- Por parte de personal técnico autorizado de cualquier [administración] desde la [UI] de la [aplicación de gestión del sistema] (*ver más adelante*)
- Como [servicio web] (REST preferentemente) por parte de cualquier sistema autorizado de cualquier [administración]

Se debe asegurar la **integridad** de estos datos de [audit] y se debe impedir:

- Su consulta por parte de personas no autorizadas
- Su modificación en cualquier circunstancia

3.8.6 Interfaz de personas usuaria de administración del sistema de mensajería PUSH

Como cualquier otro módulo común, el [sistema común de mensajería PUSH] tendrá una pequeña [UI de administración] que se organizará en base al siguiente [modelo]:

```
Grupo de Administraciones
+- Administración
    +- Aplicación
        +- Buzones
        +- Topics
```

Los [buzones] y los [topics] estarán asociados a [iniciativas] (*aplicaciones*) en cada [administración]

Desde la propia [aplicación de administración] se gestionarán las [autorizaciones] de las personas de las diferentes [administraciones]:

Las [autorizaciones] a personas se asignarán en los tres primeros niveles (*grupo de admins > admin > app*) de forma que una persona con [autorización] en un nivel superior (ej: [grupo de admins]) tendrá [autorización] en los niveles inferiores.

Por simplicidad en cada nivel inicialmente (*habrá q analizarlo en detalle*) se identifican dos perfiles / roles a los que se podrán asignar personas de las [administraciones]

- **Técnico** Podrá realizar las acciones técnicas que se identifiquen
- **Responsable** Tiene todas las [autorizaciones] del rol [técnico] y además la capacidad de asignar nuevas personas al perfil / rol [técnico] o [responsable]

... además, existirá un perfil/rol especial (**responsable horizontal**) que tendrá [autorización] total sobre cualquier parámetro técnico o funcional del sistema en cualquier nivel



La gestión de [autorizaciones] será **distribuida** de forma que una persona con [autorización] suficiente podrá “delegar” la administración en otras personas de su organización: NO existe una gestión de [autorizaciones] centralizada
Idealmente:

3. Una persona [responsable horizontal] asigna un rol de [responsable] a una persona de cada [administración]
4. Las personas [responsable] de cada [administración] **autónomamente** gestionan las [autorizaciones] en el ámbito de esta [administración] asignando [autorizaciones] de rol [técnico] o delegando en otras personas [responsables]

La **creación** de los *objetos* del sistema será:

```
Grupo de Administraciones
+- Administración
    +- Aplicación
        +- Buzones
        +- Topics
```

- La [estructura orgánica] (*grupo de admins > admin*) se creará **manualmente** por una persona autorizada utilizando la [UI de administración]
- Las [aplicaciones] también se crearán **manualmente** por una persona autorizada en la [administración] impulsora de la iniciativa.
- Los [buzones] se crearán **automáticamente** conforme las personas se van *enrolando* en la [app] (*ver descripción anterior*): los [buzones] NO se pueden crear manualmente
- Los [topics] se podrán crear:
 - Manualmente en la [UI de administración] por una persona autorizada en la [administración] impulsora de la iniciativa
 - Vía [API] por una [aplicación] de la [administración]

En la [UI de administración] se podrán ver [datos analíticos] y [audit] todos los niveles



La descripción anterior NO pretende ser precisa (*exacta*) o exhaustiva -detallar el 100% de funcionalidad o detalles técnicos-; únicamente tiene como objetivo describir a muy alto nivel un sistema que se ha probado efectivo y que *inspira* y sirve como base del [sistema común de notificaciones PUSH] (*el sistema de notificación PUSH de NIK*)

Durante la ejecución del proyecto será necesario hacer un análisis técnico y funcional detallado, no descartándose tampoco implementaciones alternativas o la utilización de sistemas de mercado / opensource si proporcionan la funcionalidad requerida

En el mercado existen sistemas muy sofisticados con decenas de funcionalidades (ej: [OneSignal](#)) pero en un principio (*se puede reconsiderar durante el proyecto*) se descarta el uso de estos sistemas cloud porque la funcionalidad que se requiere de momento es muy simple y NO justifica el gasto recurrente que se *obligaría* a las [administraciones].

Por otra parte, en todo caso hay que hacer un *recubrimiento* de un [sistema cloud] de [mensajería PUSH] como [Google Firebase] para tener en cuenta los requisitos funcionales del sistema; se aprovecharán al máximo las funcionalidades que este [sistema cloud] de [mensajería PUSH] ofrezca con el objetivo de no *reinventar* nada.

La experiencia de [NIK](#) por un lado ha demostrado que con un sistema simple es suficiente y por otro lado supone una buena base para construir un sistema común.

3.9 Seguridad y confidencialidad

La premisa de que **[NIRE] NO almacena los [datos]** (*únicamente se guardan algunos [meta-datos] sobre la actualización de los [datos] como se ha descrito en el punto anterior*) hace que los [datos] almacenados en [NIRE] tengan “poco valor” desde el punto de vista de la [seguridad]



Una *fuga* de los datos almacenados en [NIRE] no supondría un problema grave puesto que únicamente se almacena información sobre el estado de actualización del dato.

Una excepción sería el [repositorio común de datos básicos] que, en caso de construirse, contendrá [datos de contacto] y [cuenta bancaria]

En cualquier caso, **el sistema debe incorporar todas las medidas de seguridad posible** y hacerse una adecuada gestión del acceso a los mismos.

3.10 Privacidad desde el diseño y por defecto

El producto deberá cumplir con la normativa de protección de datos vigente (RGPD y LOPDGDD) y actualizarse según cambie la normativa a lo largo de la duración del contrato.

De esta forma, se deberá tener presente la aplicación del principio de **[privacidad desde el diseño y por defecto]** establecido en el artículo 25 del RGPD en el momento de construir y desplegar los distintos módulos y las funcionalidades del producto.

A este respecto, la [oferta técnica] deberá detallar necesariamente en un punto específico, las **medidas de seguridad y privacidad** establecidas por el licitador para salvaguardar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales previstas en:

- La Guía de Privacidad desde el Diseño v. octubre 2019, o sucesiva, emitida por la Agencia Española de Protección de datos o la adopción del estándar de la privacidad desde el diseño conforme a la ISO 31700, y;
- La Guía de Protección de Datos por Defecto de octubre de 2020, o sucesiva, emitida por la Agencia Española de Protección de datos.

Este detalle a incluir en la [oferta técnica] se hará de forma descriptiva, no reproduciendo los literales de la normativa, guías y de los estándares anteriores.

4 Ciclo de vida del trabajo para la integración de un [dato interoperable] en [NIRE]

[NIRE] es una iniciativa de colaboración de todas las [administraciones vascas] que implica un enorme esfuerzo técnico en construir sistemas comunes que NO serviría para mucho sin la implicación y trabajo de cada una de las [administraciones].

En el presente punto se intenta dar una visión general (*sin llegar a mucho detalle*) del [ciclo de vida] (*los pasos que hay que dar*) para poner un [dato interoperable] en [NIRE]

En primer lugar, en una **primera fase**, el trabajo a hacer se centra en la [construcción del middleware] en el [CORE NIRE] para *dar soporte* a un nuevo [dato interoperable]:

	Área de trabajo	Detalle	Responsable
1	Analizar el [dato interoperable]	- Semántica: modelar el [dato interoperable] - Definir un formato de intercambio estándar	- CORE NIRE - Administración(es) [origen de datos]
2	Construir middleware	- Construir el [middleware] que se integra con los componentes del [CORE NIRE]: - API-Gateway - Retrieve Rules - Monitorización / Observabilidad / Audit / Data Analytics - Integrar el [middleware] en el [CORE de Integración] - Construir un [conector estándar] que conecta a un [servicio REST]: - Autenticado con la solución [zero-trust] en base a un [access server] (ej: keycloak) - Devuelve el [formato estándar de intercambio] - Desarrollar [librerías JAVA] que faciliten la construcción del [servicio] en el [origen de datos] de la [administración]	CORE NIRE
3	Documentar	Documentar y publicar toda la información en el [sitio web del desarrollador] (admindigital.euskadi.eus)	CORE NIRE

A continuación, en una **segunda fase**, sobre la base anterior, para una [administración] que quiera ofrecer un [dato interoperable] a [NIRE] y construir un [servicio] [origen de datos]:

Área de trabajo	Detalle	Responsable
1 Analizar el [dato interoperable]	- Identificar si el [dato interoperable] ya está implementado en [NIRE] contando para ello con el [sitio web del desarrollador] y el soporte de [NIRE] - Si el [dato interoperable] NO está implementado en [NIRE] hay que pasar por el proceso anterior	Administración(es) [origen de datos]
2 Analizar contexto en la administración	- Cómo hacer la [autenticación mutua] [NIRE] <-> [origen de datos] - Preferentemente se utilizará una [autenticación] basada en [zero-trust] (<i>no compartir nada</i>), pero si no es posible se puede utilizar una alternativa de entre las descritas. - Que <i>tipo/tecnología</i> de [servicio] se puede implementar para dar respuesta a las [peticiones de datos] por parte del [CORE NIRE] - Preferentemente se utilizarán [servicios REST] que <i>intercambian</i> mensajes en formato JSON, pero si no es posible se puede utilizar cualquier otro tipo de servicio que devuelve por ejemplo un formato que ya utiliza la [administración] (SOAP, GET que devuelve un formato arbitrario, etc) - Cómo el [origen de datos] envía meta-datos sobre la [actualización de los datos] y que puedan ser utilizados en el sistema de [retrive rules] para <i>minimizar</i> las <i>llamadas</i> desde [NIRE] a un [origen de datos] - Las opciones que se han identificado inicialmente (<i>y que se han descrito antes</i>) son:	Administración(es) [origen de datos]
	Admin-PUSH ONLINE La [administración] "proactivamente" envía on-line (<i>casi al momento</i>) la [meta-información] a [NIRE] Cuando los sistemas [back-end] de la [administración] <i>detectan</i> un cambio en un [dato] asociado a una persona X, <i>simplemente</i> enviarán [meta-información] a [NIRE]	
	NIRE-PULL ONLINE La [administración] "reactivamente" (cuando se le solicita) envía on-line a [NIRE] la [meta-información] a [NIRE] [NIRE] periódicamente consulta a la [administración] sobre si hay algún [dato] nuevo o cambio en uno ya existente en [NIRE]	
	NIRE-PULL BATCH La [administración] "reactivamente" envía off-line (batch, cada cierto tiempo) la [meta-información] a [NIRE]	
	- Cómo dar <i>acceso directo</i> al [dato] en la [sede electrónica] cuando la persona es <i>redirigida</i> desde el [dispositivo cliente] (<i>web / móvil</i>) para ver / descargar la información de detalle - Este <i>acceso directo</i> requiere de: - Integrar la [sede electrónica] con la solución que permite "extender" la [autenticación] de la persona usuaria en el [dispositivo cliente] - Modificaciones / ajustes en la aplicación que muestra el [dato]	

4 Construir el [servicio] del [origen de datos] en la [admin]

Una vez la [administración] *decide* cómo va a exponer los datos, tiene que **construir**:

1. Un [servicio] (*REST, SOAP, etc*) que va a ser *llamado* por el [CORE NIRE] para obtener los [datos] de una persona usuaria
2. La solución para actualizar meta-información sobre la [actualización de los datos] para el sistema de [retrieve rules] que evite *llamadas* al [origen de datos]
3. El *acceso directo* al [dato] en la [sede electrónica] manteniendo la [autenticación] del [dispositivo cliente]

3 Construir el [conector] en la parte de [NIRE]

Una vez que la [administración] avanza con el [paso 4] (*construcción del servicio*) desde el [CORE NIRE] hay que:

1. Construir el [conector] con el [origen de datos]
2. Modificar la app/web [NIRE] si es necesario



NO debería ser necesario modificar la app/web [NIRE] si *aparece* un nuevo [origen de datos]

... para esto *juega un papel* esencial la [administración de NIRE] donde se pueden almacenar parámetros que permiten *pintar* la UI de forma dinámica (*ver antes en este documento*)

■ CORE NIRE

4 Integrar y desplegar

Hacer la integración y el despliegue del nuevo [origen de datos]

■ CORE NIRE

■ Administración(es) [origen de datos]



El proceso de integración de un [dato interoperable] en una administración tiene cierta complejidad, pero en realidad en un gran porcentaje de los [datos interoperables] se trata de *devolver* [datos] que **YA se están ofreciendo en la [sede electrónica]** de la [administración] en un formato *interoperable* (ej: *JSON, XML, CSV, etc*) en lugar de HTML

Ej: Todas las [administraciones] ofrecen en la [carpeta ciudadana] de la [sede electrónica] los [expedientes] en formato web (html)

... la integración en [NIRE] *únicamente* requiere *devolver* los mismos datos que se “pintan” pero en un formato interoperable (json, xml, csv)

En cualquier caso, es evidente que la [administración] tiene que hacer un esfuerzo para:

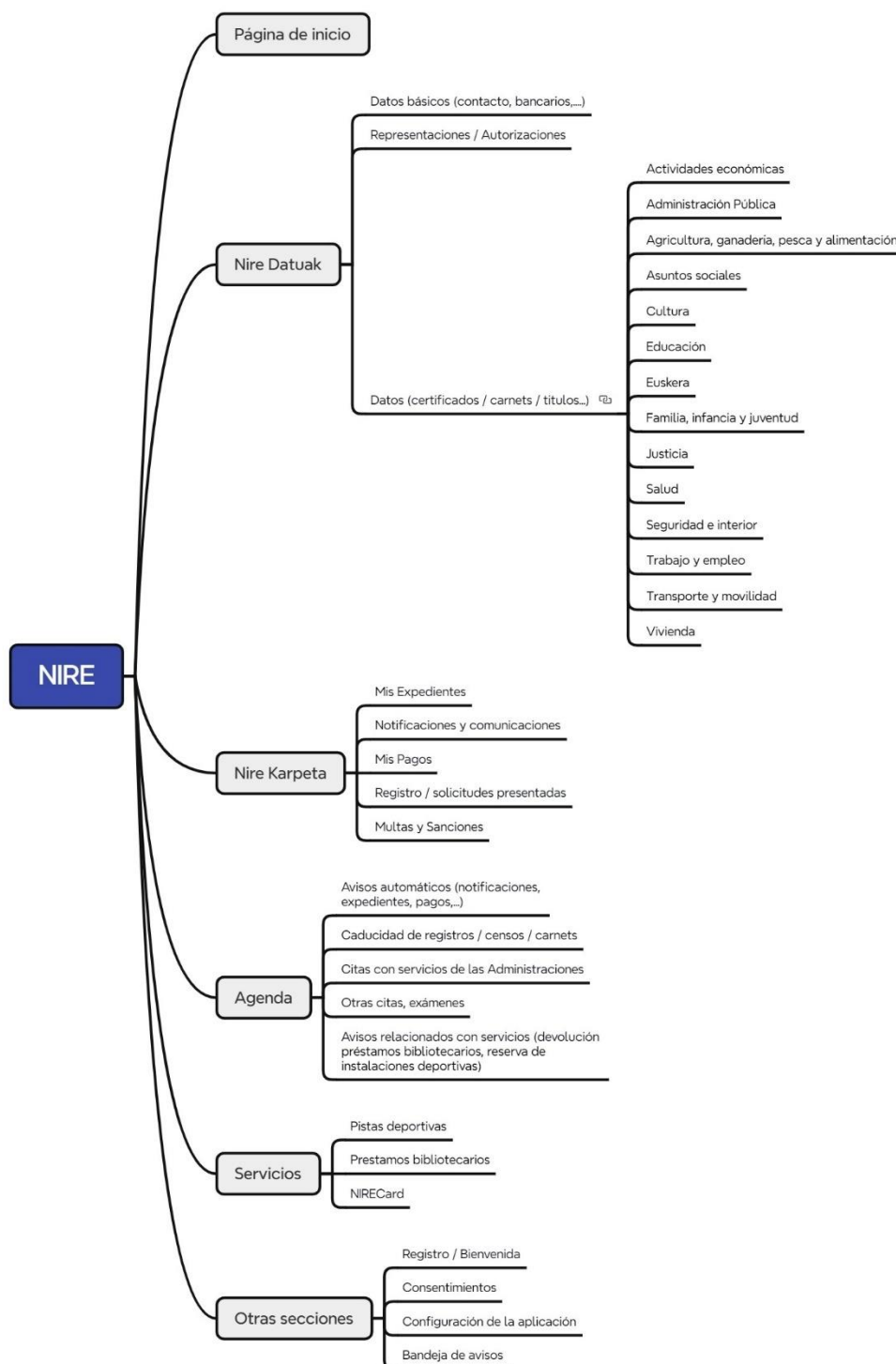
1. Devolver los [datos] en formato interoperable
2. Enviar [meta-información] sobre la actualización de los [datos]
3. Permitir el *acceso directo* a los [datos] en la [sede electrónica] con la [autenticación] de la persona usuaria obtenida en el [dispositivo cliente]

Este esfuerzo NO solo servirá para la integración en [NIRE] sino que sentará las bases de futuras interoperabilidades en otros ámbitos

5 Vistazo general al prototipo de la UI

A continuación, se presentan algunos [prototipos] de la [UI=interfaz de usuario] que las [Administraciones Vascas] han co-diseñado. Este prototipo está diseñado para desarrollar una APP móvil / web (que se construirá bajo otro expediente de contratación, y por tanto no forma parte del alcance de este expediente).

La navegación y organización de las secciones que forman NIRE es la siguiente:



Presented with xmind

[1] – Página de inicio

Tras la identificación de la persona en la aplicación NIRE, la APP le mostrará la **[página de inicio]** donde podrá consultar las **últimas actualizaciones de información** sobre:

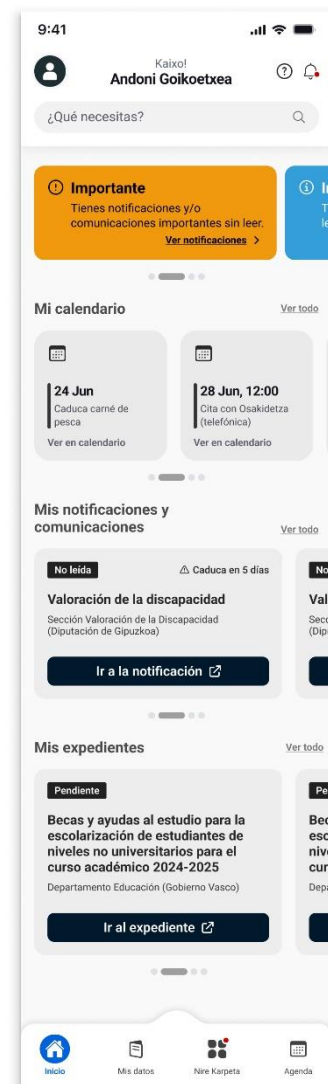
- Últimos [avisos] que las [administraciones] han enviado a través del [sistema de mensajería PUSH].
- Próximas [fechas relevantes] que debe tener en cuenta porque bien se caduca algún certificado, tiene alguna [cita] concertada con algún [servicio] de la [administración] o bien debe realizar alguna acción en la tramitación de un [expediente].
- Últimas [notificaciones] y [comunicaciones] recibidas y que serán consultadas a través del [PUC] (*punto único de comunicación*)
- Últimos [expedientes] que se están tramitando en las diferentes [administraciones], y que se obtendrá a través de la consulta agregada descrita en los puntos anteriores.

Además, desde esta página tendrá acceso a:

- Un [buscador] que le facilite localizar la información que desea.
- Una [guía y ayuda] de la [app].
- Bandeja de los [avisos] que las [administraciones] han enviado a través del [sistema de mensajería PUSH].

Por último, la navegación por la [app] se hará desde dos puntos:

- La barra de navegación inferior (Bottom Bar) que se mantendrá a lo largo de la navegación de toda la [app] y da acceso a las 4 principales secciones que forman [NIRE]: Inicio, Nire Datuak, Nire Karpeta y Agenda.
- La barra superior dará acceso al menú auxiliar de [NIRE] y que dará acceso a otras secciones de la [app], como a la configuración de la aplicación.



[2] – Nire Datuak

Esta sección da acceso a los datos que las [administraciones] tienen de la persona identificada: contacto / bancarios, representaciones, certificados, carnets, ...

Es decir, son datos que no necesariamente están asociados a procedimientos administrativos, sino datos producto de la provisión de un [servicio] y que **no cambian**:

- Se han podido generar tras la finalización de un expediente (*por ejemplo, la solicitud de la inscripción en un registro, al finalizar la instrucción, la persona puede tener el certificado de inscripción en ese registro*)
- o bien porque son datos generados por la propia relación de la persona con la Administración (*por ejemplo, certificado obtenido por la aprobación de un examen o por realizar una formación*)

Los [datos] se organizan en [temas] o [hechos vitales] de forma que con el objetivo de facilitar la localización de los [datos], en una primera página se puede *entrar* a un [tema] o [hecho vital] y acceder a los [datos] de ese ámbito

Es posible acceder a un mismo datos por diferentes caminos (*por ejemplo, desde una temática o un hecho vital se podrá tener acceso a un mismo certificado, como por ejemplo el que acredita un nivel de Euskera*)



[2.1] – Mis datos de contacto

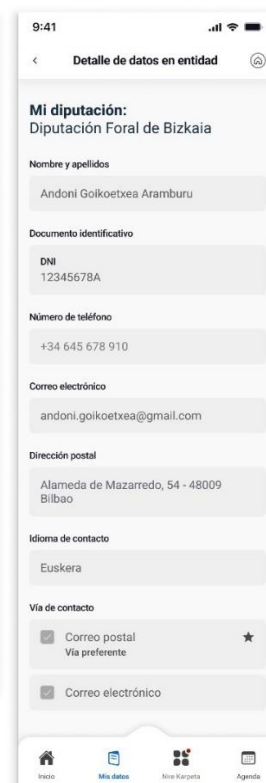
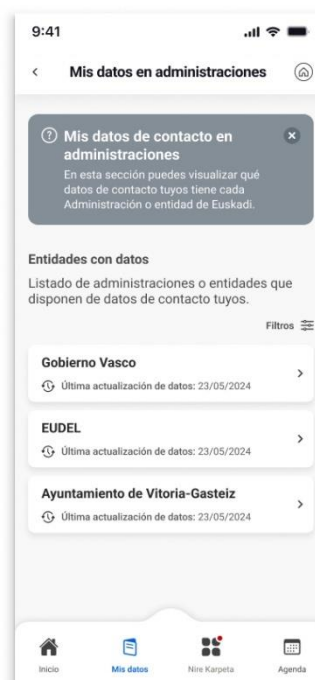
Esta sección da acceso a los datos básicos de identidad y contacto (*nombre/apellidos, teléfono, email, etc*), así como otros datos (*cuenta bancaria*) que existen dispersos en diferentes puntos de las [administraciones].

Desde esta sección, la persona identificada podrá conocer en qué [administraciones] existen datos sobre ella misma, y poder comprobar si el [dato] está o no actualizado

Esta interfaz refleja como [NIRE] actúa como una **federación de repositorios** de [datos básicos] de las personas y en la que [NIRE] es un **punto común** (hub) desde donde se podrá **consultar** y **actualizar** estos datos.

Como [NIRE] no determina lo que debe hacer cada uno de los repositorios con las actualizaciones de datos, la interfaz de usuario deberá reflejar las diferentes situaciones en las que puede encontrarse el cambio:

- Actualización realizada, y por tanto el cambio de los datos consolidado.
- Cambio pendiente de consolidar.
- Cambio descartado.

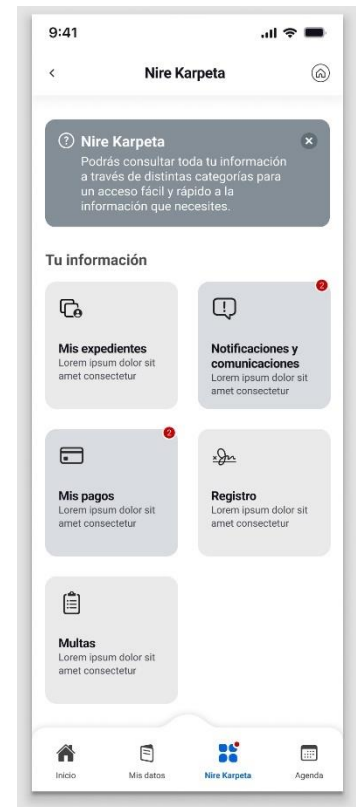


[3] – Nire Karpeta

Esta sección da acceso a los datos asociados a [expedientes] (*datos “vivos” sobre la tramitación del expediente como su estado, notificaciones, pagos,...*) que las [administraciones] tienen de la persona identificada, normalmente en la [carpeta ciudadana] construida en su [sede electrónica], donde proporcionan una visión unificada de los expedientes que gestiona esa administración.

Esta página actúa como una página distribuidora cuyo objetivo es dirigir a la persona usuaria a las diferentes secciones donde podrá localizar información concreta asociada a los trámites de sus expedientes:

- Mis expedientes, donde poder consultar en un único punto los expedientes que está gestionando la persona identificada con las diferentes administraciones.
- Notificaciones y comunicaciones, donde poder consultar los hechos relevantes de la tramitación de un expediente que una administración comunica de manera fehaciente. Esta consulta se realizará a través del [PUC].
- Mis pagos, donde poder consultar tanto pagos no domiciliados como pagos domiciliados; y también poder realizar el pago de un pago pendiente o con una carta de pago.
- Registros, donde poder consultar los registros que una persona ha presentado ante una [administración]. Hay que tener en cuenta que esta fuente de datos es una fuente importante en algunas [administraciones]



[3.1] – Mis expedientes

Esta página mostrará un listado de los [expedientes] que la persona identificada en [NIRE] está tramitando (o ha tramitado) con las diferentes [administraciones].

Es una única página que deberá agregar los datos provenientes de las diferentes administraciones para mostrarlos en este listado único.

Además de poder consultar la metainformación básica de cada expediente (*como el estado, el nombre del expediente y su código, las fechas destacables*) dará acceso a la ficha del expediente en la sede electrónica concreta de la administración que gestiona dicho expediente (*hay que recordar que, en esta primera fase, [NIRE] es fundamentalmente un sistema de consulta de los datos en diferentes administraciones, en modo de lectura, y es por eso que en muchos puntos de la interfaz se enlaza con el sistema origen que gestiona el dato que la persona está consultando.*).

También dará acceso a un buscador de expedientes para que la persona identificada pueda localizar expedientes por:

- Administrador que tramita el expediente
- Estado del expediente
- Fechas relevantes
- ...



[4] – Agenda

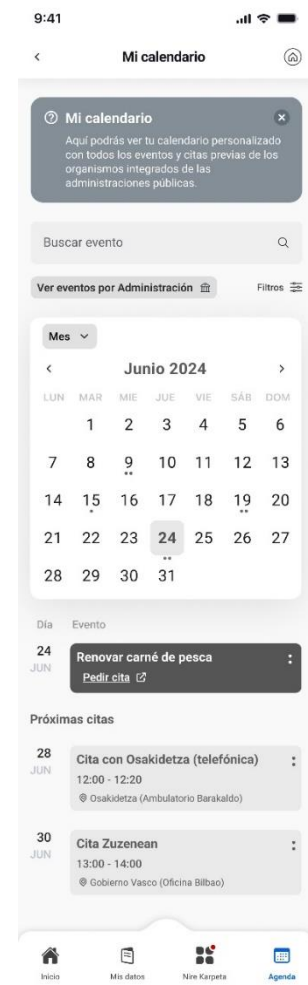
Esta sección da acceso a los datos que tienen que ver con eventos que tienen lugar en un punto en el tiempo, con diferente naturaleza:

- Citas (*Osakidetza, servicios de orientación en Lanbide, servicios de atención a la ciudadanía,...*)
- Hitos asociados a [expedientes] (*ej: fecha fin de pago, fecha fin de una justificación,...*)
- Fechas de exámenes, OPEs
- Fechas relacionadas con servicios de las administraciones (*devolución de préstamos bibliotecarios, reserva de instalaciones deportivas,...*)
- Caducidad de registros / certificados / credenciales.

Esta página mostrará con diferentes vistas (mensuales, semanales), los próximos eventos, mostrando para cada evento la metainformación básica en función del tipo de evento que se trate.

Por ejemplo:

- Caducidad de un carnet:
 - Título/carnet que caduca
 - Administración responsable de su gestión
 - Enlace de acceso al servicio de cita para su renovación.
- Cita con Osakidetza
 - Tipo de cita (telefónica / presencial)
 - Administración responsable de la cita.
 - Hora y lugar



6 Objeto del contrato

6.1 Visión de alto nivel

En el marco del [programa de proyectos NIK-NIRE]: servicios de [construcción y despliegue] de los siguientes [paquetes de trabajo]:

- **Infraestructura y entornos**
- **CORE de interoperabilidad persona <-> administraciones**
- **Identidad y autenticación**
- **Datos básicos** (*contacto, bancarios, etc*)
- **Datos del sistema** (*audit, monitorización / observabilidad, traza y datos analíticos*)
- **Consentimientos**
- **Construcción de [conectores] con los [orígenes de datos] en las [administraciones]**
- **Interfaz de persona usuaria de administración**
- **Mensajería PUSH**
- **Documentación para desarrolladores y entornos sandbox**
- **Auditoría del sistema**



Hay que recordar una vez más que todo lo que se recoge en este documento se basa en el conocimiento a día de hoy del [proyecto], que es mucho, pero no exhaustivo y al último nivel de detalle.

Durante la ejecución del proyecto pueden detectarse nuevas actividades no previstas o no llegar a realizarse otras previstas.

El elevado nivel de detalle de este documento tiene como objetivo facilitar la evaluación del proyecto por parte de las empresas ofertantes.

Se diferencia entre dos tipos de [paquetes de trabajo]:

Paquetes de trabajo con alcance cerrado	Servicios en los que el entregable está definido Es el caso de todos los [paquetes de trabajo] excepto el de construcción del [middleware] y [conector](es) con los [orígenes de datos] en las [administraciones]
Paquetes de trabajo de carácter variable	En el caso de la construcción del [middleware] y [conector](es) con los [orígenes de datos] en las [administraciones], el [alcance] NO está definido al 100% y aunque se está trabajando en un [roadmap] donde se reflejarán los compromisos de integración en [NIRE] por parte de las [administraciones], en estos momentos es difícil hacer una [planificación] de: ▪ Cuántos [middleware] / [conector](es) hay que construir ▪ Cuándo hay que trabajar en [middleware] / [conector](es) ▪ El alcance de la construcción de [middleware] / [conector](es) ya que aunque el [middleware] es común, la construcción del [conector] con cada [administración] supondrá un <i>reto</i> diferente ... por esta razón, a diferencia del resto de [paquetes de trabajo] del [proyecto], este [paquete de trabajo] NO se plantea como un “entregable cerrado” sino que se trabajará como sub-proyectos dentro del [contrato] cuyo [ciclo de vida] es el siguiente: 1. Desde [EJIE] + [Oficina Técnica] se trasladará la necesidad de trabajar en un [middleware] / [conector] en forma de [alcance] documentado con un nivel de detalle suficiente como para que la empresa adjudicataria del presente [expediente de contratación] pueda hacer una estimación 2. La empresa adjudicataria hará una planificación vinculante en los siguientes parámetros: a. Recursos: jornadas / perfil

- b. Calendario
 - c. Coste teniendo en cuenta las [jornadas/perfil] y los [precios/perfil] ofertados (*ver PCAP*)
 - d. Riesgos
- se incluirá también un **[calendario de facturación]** de los trabajos
- 3. [EJIE] y la [Oficina Técnica] revisarán, solicitarán aclaraciones / modificaciones a la [planificación] y finalmente en el momento que se considere adecuada, la **aceptarán**
 - 4. La empresa adjudicataria **ejecutará** el trabajo en las condiciones planificadas en [2]

Se facturará al [contrato] en función de los [hitos] pactados en la [planificación] siempre que exista una **aceptación por parte de [EJIE] de los [entregables]** asociados



Los [servicios de carácter variable] para la construcción y despliegue de [middleware] + [conector](es) **NO presuponen una facturación determinada**, independientemente de que exista importe sin ejecutar en el contrato.

Únicamente se facturarán los trabajos que pasan por todas las fases:

- 1. [Solicitud] por parte de [EJIE]
- 2. [Valoración] por parte del [proveedor]
- 3. Aceptación de la [valoración] por parte de [EJIE]
- 4. [Construcción y despliegue] por parte del [proveedor]
- 5. Certificación (*aceptación*) de los [entregables] por parte de [EJIE]

6.2 Detalle actividades identificadas a día de hoy

En el presente punto se enumeran (*no exhaustivamente*) algunas de las [actividades] a realizar en cada uno de los [módulos] objeto del proyecto:



En la ejecución de todas las [actividades] se trabajará y colaborará estrechamente con:

- El equipo de [EJIE] del proyecto
- Las personas del área correspondiente en [EJIE] (*centro de mando, infraestructura, seguridad, cambios, etc*)
- La [Oficina Técnica NIK-NIRE]
- Personas técnicas de otras [administraciones]
- Empresas adjudicatarias de los futuros [expedientes de contratación] para construir las [UI] móvil y web

Los servicios a proporcionar, así como los módulos a construir en el marco de este [expediente de contratación] son **estratégicos** para [EJIE] y requieren de la participación de **perfiles altamente cualificados** y con **amplia experiencia** en tecnologías CORE: cloud, interoperabilidad, seguridad, etc

En el presente punto en primer lugar se detallan algunas [**actividades transversales**] a todos los módulos para posteriormente enumerar las [**actividades específicas**] de cada uno de los módulos:

6.2.1 Actividades Transversales

Las actividades *comunes* que en las que hay que trabajar en todos los módulos y que se han identificado a día de hoy son:

Tooling

- Preparación del **tooling** de desarrollo y despliegue:
 - Repositorios GIT
 - Entorno de desarrollo local: IDEs, containers / dbs, etc en local
 - Issue tracking (*ej: gitlab, Jira, ...*)
 - Gestión de pruebas: control de calidad
 - Gestión de la documentación técnica
 - Herramientas CI/CD (*integration / delivery*)
 - ...

Calidad

- **Control de la calidad** en los [productos] (*componentes e infraestructuras*)
 - **Verificación** de los requisitos: definir [pruebas funcionales] y [conjunto de datos] necesarios que garanticen el testeo de los casos de uso
 - Pruebas **técnicas**
 - Pruebas **unitarias** en cada componente
 - Pruebas de **integración** de todos los componentes
 - Pruebas de **rendimiento**: capacidad, elasticidad y resiliencia
 - Pruebas de **entorno**
 - ⓘ Es importante testear el funcionamiento del sistema en diferentes escenarios (*timeouts, respuesta incorrecta, respuesta sin cumplir el contrato establecido, conectividad inexistente, ...*)
 - Revisiones y **auditorías** de código
- ⓘ En este punto será importante disponer de casos reales de conectividad con las [administraciones], así como simulaciones de las mismas

Provisión y Despliegue

- **Provisión** de la infraestructura (*entorno de ejecución kubernetes, comunicaciones, almacenamiento, ...*)



Todos los [productos] del [proyecto] se desplegarán en una infraestructura propia y ad-hoc: **un nuevo [tenant] en [BATERA] (EJIE)**

La **provisión** de esta infraestructura ha de ser gestionada por el [adjudicatario] del presente [expediente de contratación] trabajando con:

- Personal técnico de todas diferentes áreas de [EJIE]
- Oficina Técnica [NIK-NIRE]

esta provisión de infraestructura incluye entre otras las siguientes [actividades]:

- **Identificar** arquitectura y necesidades
- **Gestionar las peticiones** técnicas en los sistemas de [gestión de peticiones de cambios] de [EJIE]
- **Colaborar** con las personas responsables de infraestructura de [EJIE] y soportes técnicos en la provisión de la infraestructura
- **Recepción y verificación** de las infraestructuras

- **Despliegue** de los productos en cuatro entornos:

- Canary
- Development
- Sandbox
- Production

Seguridad

- **Certificar la seguridad** global del sistema en base a:
 - **Revisiones** de código (*automatizados y manuales*)
 - **Auditoría de seguridad:** tests de intentos de hackeo (*pentesting*)
 - ...

! Entre los entregables (*como se verá más adelante*) se incluirá una [certificación de seguridad] basada en las actividades anteriores

Monitorización / observabilidad / traza

- Identificar **parámetros a monitorizar** en cada uno de los componentes
- **Configurar los [cuadros de mando]** en los sistemas de operación en el [centro de mando] para:
 - Prevenir problemas: identificar signos de que puede ocurrir un problema
 - Identificar un problema una vez que este ha ocurrido
- Crear los [**procedimientos**] de actuación en caso de identificarse un problema
- **Formar** a las personas responsables del [centro de mando] en [EJIE]

Datos analíticos

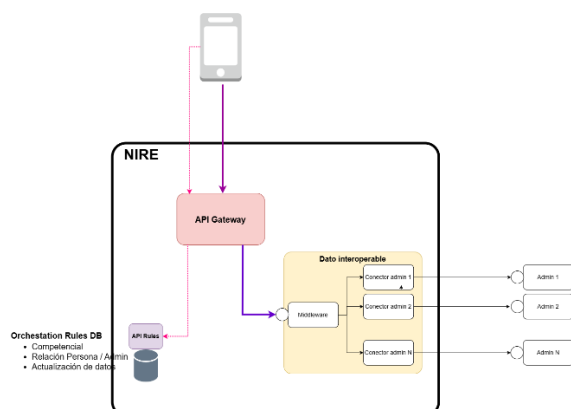
- Identificar [datos analíticos] para el [**Observatorio de Administración Digital**]
- Integración con el [Observatorio de Administración Digital] para *enviar* estos datos (*preferente utilizando streaming en tiempo casi-real*)

Gestión del cambio técnico

- **Gestión de peticiones para la provisión** de infraestructuras utilizando las herramientas de [gestión de servicios] de [EJIE]
- **Documentación** del sistema en el [sitio web del desarrollador]: admindigitala.euskadi.eus
- **Formación** a soportes técnicos y funcionales de [EJIE] y otras [administraciones]
- **Tutorización**
- **Transición:** soporte a [EJIE] durante la adopción del servicio

A continuación, se enumeran las [actividades específicas] de cada uno de los módulos:

6.2.2 CORE de interoperabilidad persona <-> administraciones



Esta parte de [NIRE] se centra en los componentes necesarios para *intercambiar* [datos interoperables] entre el [dispositivo cliente] de la persona usuaria (*móvil / web*) y los [orígenes de datos] en las diferentes [administraciones]

Las [actividades] en este punto identificadas a día de hoy son:

Arquitectura

Sobre la base de alto nivel descrita en el presente documento **iterar** hasta definir la [arquitectura] final entre otras en las siguientes áreas:

- **Componentes** de la arquitectura y funciones de cada uno
- Identificar la **plataforma / tecnología** a utilizar en cada componente
 - API Gateway
 - Servicio de optimización de invocaciones a [orígenes de datos] (*retrieve rules & API*)
 - Middleware y conectores
 - Access Management
 - Trace / Audit / Data Analytics
 - ...
- **Infraestructura:** arquitectura y dimensionamiento
 - Plataforma de ejecución (*kubernetes*)
 - Comunicaciones
 - Almacenamiento
 - Entornos (*canary, develop, sandbox, production*)
 - ...

Construcción

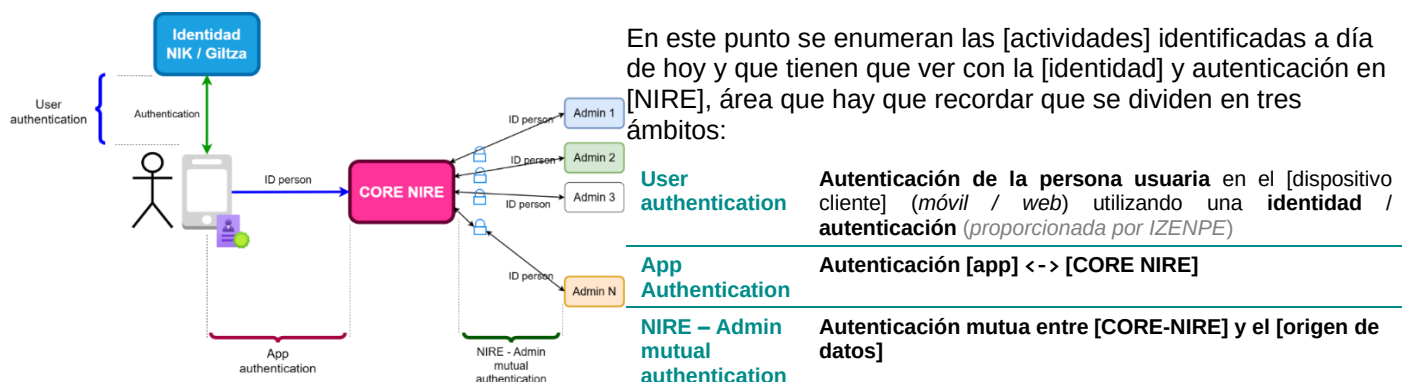
- **Construcción e integración** de los componentes del [CORE de interoperabilidad]

Actividades transversales en el módulo

Aplicar las [actividades transversales] a los [productos] del módulo:

- | | |
|--|---|
| ▪ Calidad | - Control de calidad de los [productos] |
| ▪ Provisión y despliegue | - Integración de los productos en el pipeline CI/CD
- Provisión de la infraestructura para los componentes
- Despliegue en los entornos definidos |
| ▪ Seguridad | - Certificación de seguridad |
| ▪ Monitorización / Observabilidad | - Integrar los componentes en el [cuadro de mando] del [centro de mando] de [EJIE] |
| ▪ Datos analíticos | - Integración con el [Observatorio de Admin Digital] |
| ▪ Gestión del cambio técnico | - Documentación
- Formación / tutorización
- Transición de los [productos] a [EJIE] |

6.2.3 Identidad y Autenticación



6.2.3.1 User Authentication

En este *ámbito* de la [autenticación] **la mayor parte del trabajo implica al [dispositivo cliente]** (*app / web*) aunque también al [CORE] en lo que tenga que ver con los componentes de [servidor]. Por esta razón, es un [paquete de trabajo] que **se trabajará en común** entre el presente [expediente de contratación] y los otros futuros adjudicatarios de los [expedientes de contratación] de la construcción de las [UI] web y móvil

Las [actividades] en este punto identificadas a día de hoy son:

Arquitectura

- **Definir la solución** de identificación y autenticación en el [dispositivo] (*móvil / web*) junto con la [Oficina Técnica NIK-NIRE], [EJIE]
 - ! Si para hacer la [autenticación] de la persona usuaria en el [dispositivo cliente] son necesarios componentes del lado del [servidor] (CORE NIRE), estos componentes son responsabilidad del adjudicatario del presente [expediente de contratación]
 - Las empresas adjudicatarias de los futuros [expedientes de contratación] para construir las [UI] móvil y web serán responsables de integrar estos sistemas en la [UI]

Construcción

- **Construcción / integración** de los productos que posibiliten la [autenticación] de persona usuaria en el [dispositivo cliente] (*móvil / web*)

Integración con el [dispositivo cliente]

- Soporte en la integración a las empresas adjudicatarias de los futuros [expedientes de contratación] para construir los [UI] móvil y web

Integración con proveedores de [identidad] y [autenticación]

- Integrar los componentes relacionados con la [user authentication] con [IZENPE] como proveedor de [identidad] y [autenticación] de personas usuarias

6.2.3.2 App Authentication

Este *ámbito* de la [autenticación] es **100% responsabilidad del [CORE NIRE]**

Las [actividades] en este punto identificadas a día de hoy son:

Arquitectura	▪ Definir la solución de autenticación del [dispositivo cliente] en el [CORE NIRE] <i>transportando</i> la [identificación] de la persona [autenticada] en el [dispositivo cliente].
Construcción	▪ Construcción / integración de los productos que posibiliten la [autenticación] del [dispositivo cliente] (<i>móvil / web</i>) en el [CORE NIRE]
Integración con el [dispositivo cliente]	▪ Soporte en la integración a las empresas adjudicatarias de los futuros [expedientes de contratación] para construir los [UI] móvil y web

6.2.3.3 NIRE – Admin mutual authentication

Este *ámbito* de la [autenticación] es **100% responsabilidad del [CORE NIRE]** y tiene la complejidad de que **implica también a las [administraciones] con las que [NIRE] se integra** por lo que será fundamental colaborar en este punto con la [Oficina Técnica NIK-NIRE] que coordinará toda la relación técnica con las [administraciones] en este ámbito

Las [actividades] en este punto identificadas a día de hoy son:

Arquitectura	▪ Definir la solución de [autenticación] mutua entre [CORE NIRE] y [orígenes de datos] en las [administraciones] proporcionando diferentes alternativas para las posibles <i>casuísticas</i> en las [administraciones]
Construcción	▪ Construcción / integración de los productos que posibiliten esta [autenticación] mutua [CORE NIRE] < - > [origen de datos]
Integración con la interfaz de persona usuaria de administración del sistema	▪ Construir las posibles integraciones entre los componentes de [autenticación] en este ámbito con la [administración del sistema] con el objetivo de centralizar toda la administración en un único punto.
Soporte a la construcción de [conectores] con [orígenes de datos]	▪ Proporcionar soporte al [paquete de trabajo] de construcción de [conectores] con los [orígenes de datos] en las [administraciones]

6.2.3.4 Extensión de la autenticación desde el [dispositivo cliente] a la [sede electrónica] de la [administración]

Este *ámbito* de la [autenticación] es **100% responsabilidad del [CORE NIRE]** y tiene la complejidad de que **implica también a las [administraciones] con las que [NIRE] se integra** por lo que será fundamental colaborar en este punto con la [Oficina Técnica NIK-NIRE] que coordinará toda la relación técnica con las [administraciones] en este ámbito

Las [actividades] en este punto identificadas a día de hoy son:

Arquitectura

- **Definir la solución** de extensión de la [autenticación] del [dispositivo cliente] a las [sedes electrónicas] de las [administraciones] de forma que la persona usuaria NO tenga que volver a *autenticarse* cuando es *redirigida* desde [NIRE] a la [sede electrónica] correspondiente.

Construcción

- **Construcción / integración** de los productos que posibiliten esta extensión de la [autenticación] a las [sedes electrónicas]

Soporte a la administración

- Proporcionar soporte a la [administración] en este punto

Las [actividades] transversales a este módulo son:

- | | |
|--|---|
| ▪ Calidad | - Control de calidad de los [productos] |
| ▪ Provisión y despliegue | - Integración de los productos en el pipeline CI/CD
- Provisión de la infraestructura para los componentes
- Despliegue en los entornos definidos |
| ▪ Seguridad | - Certificación de seguridad |
| ▪ Monitorización / Observabilidad | - Integrar los componentes en el [cuadro de mando] del [centro de mando] de [EJIE] |
| ▪ Datos analíticos | - Integración con el [Observatorio de Admin Digital] |
| ▪ Gestión del cambio técnico | - Documentación
- Formación / tutorización
- Transición de los [productos] a [EJIE] |

6.2.4 Datos Básicos

En este [paquete de trabajo] para interoperar algunos [datos básicos] de [identidad], [contacto] y [bancarios] las [actividades] identificadas a día de hoy son:

Definición funcional y Arquitectura

- **Sobre** la base de alto nivel descrita en el presente documento **iterar** hasta definir la funcionalidad y arquitectura técnica final del sistema de [datos básicos]:
 - **Interoperabilidad** con otras [bases de datos de personas] en el ámbito de [datos básicos]:
 - Identidad (*nombre, apellidos*)
 - Contacto (*direcciones, teléfonos, emails, etc*)
 - Datos bancarios
 - Otros
 - ... tanto para [consulta] como [actualización] (*si el [origen de datos] lo considera viable*)
 - **[Repositorio común de datos básicos]** depurados por las [personas usuarias] y servicios asociados de [consulta] para las [administraciones]

Construcción

- **Construcción** de la funcionalidad definida

Documentación

- **Documentación** del módulo de [consentimientos] en el [sitio web del desarrollador] (admindigitala.euskadi.eus)

Soporte a la integración en otros módulos

En un principio, el módulo de [datos básicos] se utilizará desde:

- Las [UI] (*web / móvil*) para [consultar] y/o [actualizar] en las [DB de terceros] de las [administraciones] a través de los [servicios de interoperabilidad]
- Las [administraciones] para [consultar] datos de la [db común de datos básicos]
- Otros sistemas

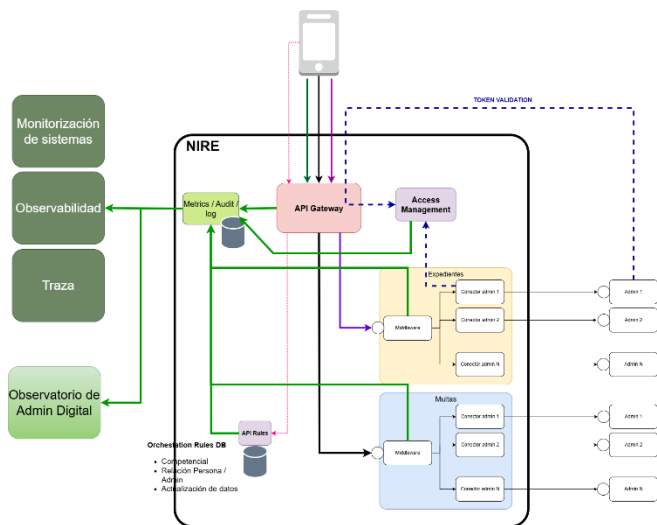
Algunas de estas integraciones se harán en el ámbito del presente [contrato] y otras en otros externos como los futuros para construir las [UI] web y móvil

Actividades transversales en el módulo

Aplicar las [actividades transversales] a los [productos] del módulo:

- | | |
|--|--|
| ▪ Calidad | - Control de calidad de los [productos] |
| ▪ Provisión y despliegue | - Integración de los productos en el pipeline CI/CD |
| | - Provisión de la infraestructura para los componentes |
| | - Despliegue en los entornos definidos |
| ▪ Seguridad | - Certificación de seguridad |
| ▪ Monitorización / Observabilidad | - Integrar los componentes en el [cuadro de mando] del [centro de mando] de [EJIE] |
| ▪ Datos analíticos | - Integración con el [Observatorio de Admin Digital] |
| ▪ Gestión del cambio técnico | - Documentación |
| | - Formación / tutorización |
| | - Transición de los [productos] a [EJIE] |

6.2.5 Datos del sistema



En este punto se enumeran las [actividades] identificadas a día de hoy y que tienen que ver con datos de monitorización / observabilidad, analíticos y auditoría:

- 1 Monitorización / observabilidad / Traza**
 - Salud del sistema: ¿puede dar servicio de forma normal?
 - Traza: información (logs) que permitan depurar una [petición de interoperabilidad]
- 2 Datos analíticos: Observatorio de Administración Digital**
 - Recolección de [indicadores] con el objetivo de ser "mostrada" en los [cuadros de mando] del [Observatorio de Administración Digital]
- 3 Audit de uso de los [servicios de interoperabilidad]**
 - Información de [auditoría] de quién / cuándo utiliza los [servicios de interoperabilidad]

Arquitectura

- Definir la solución para:
 - monitorización / observabilidad
 - traza para la depuración de incidencias
 - almacenamiento y recuperación (*acceso / búsqueda*) a los datos de auditoría
 - integración de [datos analíticos] con el [Observatorio de Administración Digital]

Construcción

- Construcción / integración** de los productos en cada uno de los ámbitos anteriores

Despliegue de la monitorización

- Integración de la monitorización / observabilidad en los sistemas del [centro de mando] de [EJIE]

Integración con el [Observatorio de la Admin Digital]

- Integración (*utilizando streaming en tiempo real preferentemente*) con el [data-lake] del [Observatorio de Administración Digital]

Integración en la administración del sistema

- Integrar en la interfaz de persona usuaria de [administración del sistema]:
 - Datos de monitorización / observabilidad
 - Datos analíticos mínimos
 - Herramientas de traza (seguimiento de peticiones) para resolver incidencias

Actividades transversales en el módulo

Aplicar las [actividades transversales] a los [productos] del módulo:

- Provisión y despliegue**
 - Provisión de la infraestructura para los componentes
 - Despliegue en los entornos definidos
- Gestión del cambio técnico**
 - Documentación
 - Formación / tutorización
 - Transición de los [productos] a [EJIE]

6.2.6 Consentimientos

Este módulo de [consentimientos] se está construyendo en el marco del [programa de proyectos NIK-NIRE] ya que quizá es el lugar donde es más necesario, sin embargo, es un [módulo] que puede ser utilizado desde muchos otros sistemas de las [administración digital]

Las [actividades] en este punto identificadas a día de hoy son:

Definición funcional y Arquitectura

- **Sobre** la base de alto nivel descrita en el presente documento **iterar** hasta definir la funcionalidad y arquitectura técnica final del sistema de [consentimientos]:
 - Almacenamiento de [consentimientos] con evidencias de ser informados y expresos
 - Servicios a exponer a otros módulos para almacenar / recuperar / validar / etc [consentimientos]

Construcción

- **Construcción** de la funcionalidad definida

Documentación

- **Documentación** del módulo de [consentimientos] en el [sitio web del desarrollador] (admindigitala.euskadi.eus)

Soporte a la integración en otros módulos

En un principio, el módulo de [consentimientos] se utilizará desde:

- Las [UI] (*web / móvil*) para recabar / mostrar los [consentimientos]
- Opcionalmente desde los [orígenes de datos] en las [administraciones] para tener *certeza* de que el [identificador de consentimiento] incluido en las [peticiones de datos] es *válido*
- La [UI] de [administración del sistema] para *depurar* (trazar) [peticiones de datos]
- Otros sistemas

Algunas de estas integraciones se harán en el ámbito del presente [contrato] y otras en otros externos como los futuros para construir las [UI] web y móvil

Actividades transversales en el módulo

Aplicar las [actividades transversales] a los [productos] del módulo:

- | | |
|--|---|
| ▪ Calidad | - Control de calidad de los [productos] |
| ▪ Provisión y despliegue | - Integración de los productos en el pipeline CI/CD
- Provisión de la infraestructura para los componentes
- Despliegue en los entornos definidos |
| ▪ Seguridad | - Certificación de seguridad |
| ▪ Monitorización / Observabilidad | - Integrar los componentes en el [cuadro de mando] del [centro de mando] de [EJIE] |
| ▪ Datos analíticos | - Integración con el [Observatorio de Admin Digital] |
| ▪ Gestión del cambio técnico | - Documentación
- Formación / tutorización
- Transición de los [productos] a [EJIE] |

6.2.7 Datos que se interoperan

Este punto está centrado en la construcción de los [middleware] / [conectores] que *intermedian* con los [orígenes de datos] en las [administraciones]



Así como en el resto de [paquetes de trabajo] del [proyecto] se puede identificar el [producto] y cuantificar en [coste], **en el caso de los [datos interoperables], el escenario no está tan definido** y aunque **se está trabajando en un [roadmap]** donde se reflejarán los compromisos de integración en [NIRE] por parte de las [administraciones], **en estos momentos es difícil hacer una [planificación]** de:

- **Cuántos** [middleware] / [conector](es) hay que construir
- **Cuándo** hay que trabajar en [middleware] / [conector](es)
- El **alcance** de la construcción de [middleware] / [conector](es) ya que aunque el [middleware] es común, la construcción del [conector] con cada [administración] supondrá un *reto* diferente

... por esta razón, a diferencia del resto de [paquetes de trabajo] del [proyecto], **la construcción de [middleware] / [conector](es) NO se plantea como un “entregable cerrado”** sino que se trabajará como **sub-proyectos** dentro del [contrato] con el siguiente [ciclo de vida] (*descrito en detalle anteriormente*)

1. Solicitud por parte de [EJIE] > [alcance] **documentado**
2. Evaluación y [planificación] por parte de la empresa adjudicataria
3. Aceptación (*o no*) por parte de [EJIE] de la [planificación]
4. Ejecución por parte de la [empresa adjudicataria]
5. Facturación al [contrato] en función de los [hitos] pactados en la [planificación] siempre que exista una **aceptación por parte de [EJIE] de los [entregables]** asociados

Recordar una vez más que:



Los [servicios de carácter variable] para la construcción y despliegue de [middleware] + [conector](es) **NO presuponen una facturación determinada**, independientemente de que exista importe sin ejecutar en el contrato.

Únicamente se facturarán los trabajos que pasan por todas las fases del [ciclo de vida] anterior

En el presente punto se incluyen las [actividades] que será necesario que ejecutar para integrar cada [dato interoperable] y [origen de datos] en [NIRE]: para construir el [middleware] + [conector](es)

(estas [actividades] ya se introdujeron en un punto anterior donde se resumía el [ciclo de vida] del trabajo para la integración de un [origen de datos]; se incluyen de nuevo aquí por mantener la coherencia del documento)

La incorporación de un [dato interoperable] en [NIRE] tiene dos fases:

FASE I: construcción del [middleware]	Es la base común, independiente de una [administración] concreta y en ella: 1. se define el modelo, semántica, etc 2. se integra el [middleware] en el [CORE de interoperabilidad]
FASE II: construcción de los [conectores]	Es el trabajo a realizar ad-hoc para cada [origen de datos] en cada [administración]

6.2.7.1 Construcción del [middleware] para un determinado [dato interoperable]

Las [actividades] identificadas en este momento para este [paquete de trabajo] son:

	Área de trabajo	Detalle	Responsable
1	Analizar el [dato interoperable]	- Semántica: modelar el [dato interoperable] - Definir un formato de intercambio estándar	- CORE NIRE - Administración(es) [origen de datos]
2	Construir middleware	- Construir el [middleware] que se integra con los componentes del [CORE NIRE]: - API-Gateway - Retrieve Rules - Monitorización / Observabilidad / Audit / Data Analytics Integrar el [middleware] en el [CORE de Integración] - Construir un [conector estándar] que conecta a un [servicio REST]: - Autenticado con la solución [zero-trust] en base a un [access server] (ej: keycloak) - Devuelve el [formato estándar de intercambio] - Desarrollar [librerías JAVA] que faciliten la construcción del [servicio] en el [origen de datos] de la [administración]	CORE NIRE
3	Documentar	Documentar y publicar toda la información en el [sitio web del desarrollador] (admindigital.euskadi.eus)	CORE NIRE

6.2.7.2 Construcción del [conector] para un [origen de datos]

Sobre la base anterior, para una [administración] que quiera ofrecer un [dato interoperable] a [NIRE] y construir un [servicio] [origen de datos]:

Área de trabajo	Detalle	Responsable						
1 Analizar el [dato interoperable]	- Identificar si el [dato interoperable] ya está implementado en [NIRE] contando para ello con el [sitio web del desarrollador] y el soporte de [NIRE] - Si el [dato interoperable] NO está implementado en [NIRE] hay que pasar por el proceso anterior	Administración(es) [origen de datos]						
2 Analizar contexto en la administración	- Cómo hacer la [autenticación mutua] [NIRE] <-> [origen de datos]  Preferentemente se utilizará una [autenticación] basada en [zero-trust] (<i>no compartir nada</i>), pero si no es posible se puede utilizar una alternativa de entre las descritas. - Que <i>tipo/tecnología</i> de [servicio] se puede implementar para dar respuesta a las [peticiones de datos] por parte del [CORE NIRE]  Preferentemente se utilizarán [servicios REST] que <i>intercambian</i> mensajes en formato JSON, pero si no es posible se puede utilizar cualquier otro tipo de servicio que devuelve por ejemplo un formato que ya utiliza la [administración] (SOAP, GET que devuelve un formato arbitrario, etc) - Cómo el [origen de datos] envía meta-datos sobre la [actualización de los datos] y que puedan ser utilizados en el sistema de [retrive rules] para <i>minimizar</i> las <i>llamadas</i> desde [NIRE] a un [origen de datos]  Las opciones que se han identificado inicialmente (<i>y que se han descrito antes</i>) son:<table><tr><td>Admin-PUSH ONLINE</td><td>La [administración] “proactivamente” <i>envía</i> on-line (<i>casi al momento</i>) la [meta-información] a [NIRE] Cuando los sistemas [back-end] de la [administración] <i>detectan</i> un cambio en un [dato] asociado a una persona X, <i>simplemente</i> enviarán [meta-información] a [NIRE]</td></tr><tr><td>NIRE-PULL ONLINE</td><td>La [administración] “reactivamente” (<i>cuando se le solicita</i>) <i>envía</i> on-line a [NIRE] la [meta-información] a [NIRE] [NIRE] periódicamente consulta a la [administración] sobre si hay algún [dato] nuevo o cambio en uno ya existente en [NIRE]</td></tr><tr><td>NIRE-PULL BATCH</td><td>La [administración] “reactivamente” <i>envía</i> off-line (batch, cada cierto tiempo) la [meta-información] a [NIRE]</td></tr></table> - Cómo dar <i>acceso directo</i> al [dato] en la [sede electrónica] cuando la persona es <i>redirigida</i> desde el [dispositivo cliente] (<i>web / móvil</i>) para ver / descargar la información de detalle  Este <i>acceso directo</i> requiere de: c) Integrar la [sede electrónica] con la solución que permite “extender” la [autenticación] de la persona usuaria en el [dispositivo cliente] d) Modificaciones / ajustes en la aplicación que muestra el [dato]	Admin-PUSH ONLINE	La [administración] “ proactivamente ” <i>envía</i> on-line (<i>casi al momento</i>) la [meta-información] a [NIRE] Cuando los sistemas [back-end] de la [administración] <i>detectan</i> un cambio en un [dato] asociado a una persona X, <i>simplemente</i> enviarán [meta-información] a [NIRE]	NIRE-PULL ONLINE	La [administración] “ reactivamente ” (<i>cuando se le solicita</i>) <i>envía</i> on-line a [NIRE] la [meta-información] a [NIRE] [NIRE] periódicamente consulta a la [administración] sobre si hay algún [dato] nuevo o cambio en uno ya existente en [NIRE]	NIRE-PULL BATCH	La [administración] “ reactivamente ” <i>envía</i> off-line (batch, cada cierto tiempo) la [meta-información] a [NIRE]	Administración(es) [origen de datos]
Admin-PUSH ONLINE	La [administración] “ proactivamente ” <i>envía</i> on-line (<i>casi al momento</i>) la [meta-información] a [NIRE] Cuando los sistemas [back-end] de la [administración] <i>detectan</i> un cambio en un [dato] asociado a una persona X, <i>simplemente</i> enviarán [meta-información] a [NIRE]							
NIRE-PULL ONLINE	La [administración] “ reactivamente ” (<i>cuando se le solicita</i>) <i>envía</i> on-line a [NIRE] la [meta-información] a [NIRE] [NIRE] periódicamente consulta a la [administración] sobre si hay algún [dato] nuevo o cambio en uno ya existente en [NIRE]							
NIRE-PULL BATCH	La [administración] “ reactivamente ” <i>envía</i> off-line (batch, cada cierto tiempo) la [meta-información] a [NIRE]							

4 Construir el [servicio] del [origen de datos] en la [admin]

Una vez la [administración] *decide* cómo va a exponer los datos, tiene que **construir**:

1. Un [servicio] (*REST, SOAP, etc*) que va a ser *llamado* por el [CORE NIRE] para obtener los [datos] de una persona usuaria
2. La solución para actualizar meta-información sobre la [actualización de los datos] para el sistema de [retrieve rules] que evite *llamadas* al [origen de datos]
3. El *acceso directo* al [dato] en la [sede electrónica] manteniendo la [autenticación] del [dispositivo cliente]

3 Construir el [conector] en la parte de [NIRE]

Una vez que la [administración] avanza con el [paso 4] (*construcción del servicio*) desde el [CORE NIRE] hay que:

1. Construir el [conector] con el [origen de datos]
2. Modificar la app/web [NIRE] si es necesario



NO debería ser necesario modificar la app/web [NIRE] si aparece un nuevo [origen de datos]

... para esto *juega un papel* esencial la [administración de NIRE] donde se pueden almacenar parámetros que permiten *pintar* la UI de forma dinámica (*ver antes en este documento*)

4 Integrar y desplegar

Hacer la integración y el despliegue del nuevo [origen de datos]

- CORE NIRE
- Administración(es) [origen de datos]

Además de las [actividades] anteriores hay otras dos **muy importantes** en el caso de los [datos interoperables]



Proporcionar [soporte técnico y funcional] a las [administraciones] en el proceso de incorporación a [NIRE] (*antes, durante y después*)



Existe un [entorno sandbox] idéntico al entorno [productivo] que permite a los equipos de desarrollo **probar los servicios**

Es muy importante “cuidar” este [entorno sandbox] y que sea totalmente funcional para todos los datos, en particular las interfaces que permiten “probar” los [servicios] en el [sitio web del desarrollador] (*ver como ejemplo la [documentación del api de Euskalmet]*)

Finalmente, recordar que como en todos los módulos hay que trabajar en una serie de [actividades transversales]:

▪ Calidad	-	Control de calidad de los [productos]
▪ Provisión y despliegue	-	Integración de los productos en el pipeline CI/CD
	-	Provisión de la infraestructura para los componentes
	-	Despliegue en los entornos definidos
▪ Seguridad	-	Certificación de seguridad
▪ Monitorización / Observabilidad	-	Integrar los componentes en el [cuadro de mando] del [centro de mando] de [EJIE]
▪ Datos analíticos	-	Integración con el [Observatorio de Admin Digital]
▪ Gestión del cambio técnico	-	Documentación
	-	Formación / tutorización
	-	Transición de los [productos] a [EJIE]

6.2.8 Interfaz de persona usuaria de administración de NIRE

En la construcción de la [UI] de [administración del sistema] a día de hoy se han identificado las siguientes [actividades]:

Definición funcional y Arquitectura

- **Sobre** la base de alto nivel descrita en el presente documento **iterar** hasta definir la funcionalidad y arquitectura técnica final del sistema de la [UI de administración del sistema]

Construcción

- **Construcción** de la funcionalidad definida

Documentación

- **Documentación** en el [sitio web del desarrollador] (admindigitala.euskadi.eus)

Actividades transversales en el módulo

Aplicar las [actividades transversales] a los [productos] del módulo:

- | | |
|--|--|
| ▪ Calidad | - Control de calidad de los [productos] |
| ▪ Provisión y despliegue | - Integración de los productos en el pipeline CI/CD |
| | - Provisión de la infraestructura para los componentes |
| | - Despliegue en los entornos definidos |
| ▪ Seguridad | - Certificación de seguridad |
| ▪ Monitorización / Observabilidad | - Integrar los componentes en el [cuadro de mando] del [centro de mando] de [EJIE] |
| ▪ Datos analíticos | - Integración con el [Observatorio de Admin Digital] |
| ▪ Gestión del cambio técnico | - Documentación |
| | - Formación / tutorización |
| | - Transición de los [productos] a [EJIE] |

6.2.9 Mensajería PUSH

En la construcción de la [mensajería push] a día de hoy se han identificado las siguientes [actividades]:

Definición funcional y Arquitectura	Sobre la base de alto nivel descrita en el presente documento iterar hasta definir la funcionalidad y arquitectura técnica final del sistema de la [UI de administración del sistema]
Construcción	Construcción de la funcionalidad definida
Documentación	Documentación en el [sitio web del desarrollador] (admindigitala.euskadi.eus)
Soporte a la integración en la UI (web / móvil)	Soporte a las empresas adjudicatarias de los futuros contratos para la construcción de las [UI] web y móvil en cuanto a la integración de la [mensajería PUSH]
Actividades transversales en el módulo	Aplicar las [actividades transversales] a los [productos] del módulo: Calidad - Control de calidad de los [productos] Provisión y despliegue - Integración de los productos en el pipeline CI/CD - Provisión de la infraestructura para los componentes - Despliegue en los entornos definidos Seguridad - Certificación de seguridad Monitorización / Observabilidad - Integrar los componentes en el [cuadro de mando] del [centro de mando] de [EJIE] Datos analíticos - Integración con el [Observatorio de Admin Digital] Gestión del cambio técnico - Documentación - Formación / tutorización - Transición de los [productos] a [EJIE]

6.2.10 Auditoría

En este punto se detallan dos [actividades] fundamentales a realizar una vez todos los [productos] del [proyecto] sean desplegados en los [entornos] **productivos** (*no es necesario realizar estas auditorías en entornos previos*)

Estas [actividades] tienen como objetivo **certificar** que el [producto] puede proporcionar con seguridad el servicio para lo que se ha construido:

Rendimiento / Capacidad y resiliencia

Rendimiento

Asegurar que el sistema responde con la rapidez esperada incluso en momentos de gran carga

Capacidad elasticidad

/ Asegurar que el sistema *soporta* el número de personas usuarias esperado: *asegurar que los recursos del sistema se reconfiguran (crecen / decrecen) para adaptarse a la carga*

Resiliencia

Asegurar que el sistema puede *seguir funcionando con normalidad* en caso de que alguno o todos los componentes fallen: *asegurar que los **mecanismos de contingencia** funcionan correctamente*

Seguridad

Certificar que el sistema cumple con los requisitos de seguridad en base a:

- Simulaciones de penetración (pen-testing)
- Auditorías de configuración de componentes y código



Los [requisitos] a nivel de rendimiento / capacidad y resiliencia así como de seguridad serán fijados por [EJIE] y la [OT NIK-NIRE] en función del número de [personas usuarias] estimadas y del número de [orígenes de datos] integrados

6.2.11 Actividades de Gestión

El presente proyecto tiene un carácter **eminente técnico** para la definición y construcción de un sistema de interoperabilidad y dado que **se cuenta con el soporte en lo relativo a las tareas de gestión por parte de la [PMO=Project Management Office] de la [Oficina Técnica NIK-NIRE]**, las [actividades] de gestión a realizar en el proyecto se reducen al mínimo.

Específicamente en el [ciclo de vida] *clásico* de [Gestión de Proyectos] las [actividades] a realizar:

Iniciación En esta fase se *crea* el proyecto y la mayor parte de las [actividades] están ya realizadas por [EJIE] y la [Oficina Técnica NIK-NIRE] *culminando* con el presente [expediente de contratación]

Planificación La [planificación]:

- Se elaborará en equipo La [planificación] se hará conjuntamente entre el [adjudicatario] del presente [expediente de contratación], [EJIE] y la [Oficina Técnica NIK-NIRE]
- Se basará en la [descomposición de trabajos] (WBS) La [WBS] (*work breakdown structure*) es la herramienta básica de planificación
- Será progresiva NO se hará una planificación inicial completa, sino que:
 1. Se hará una **secuenciación** de los [paquetes de trabajo]
 2. Se planificarán en el tiempo los primeros [paquetes de trabajo]
 3. Se irá iterando
- Se considerarán las siguientes áreas planificables
 - **Alcance:** WBS (*paquetes de trabajo*)
 - **Participantes** en cada [paquete de trabajo]
 - **Tiempo** (*calendario*) de cada [paquete de trabajo]
 - **Riesgos** globales y asociados a cada [paquete de trabajo]
 - **Costes** (*en los [paquetes de trabajo] de coste variable*)

① Solo se hará planificación de [costes] en los [paquetes de trabajo] cuyo [coste] no está cerrado por contrato (*el especificado en la oferta*)

Es decir, solo se hará [planificación de costes] en el [paquete de trabajo] dedicado a la construcción de [middleware] y [conectores] con los [orígenes de datos]

Ejecución Durante la [ejecución] se facilitarán [datos] a la [Oficina Técnica NIK-NIRE] para que pueda hacer las tareas de [monitorización y control]

Monitorización y Control Se colaborará con la [Oficina Técnica NIK-NIRE] para la elaboración de [informes de seguimiento]
Si se considera necesario se participará en las [reuniones de seguimiento] del proyecto global

Cierre Colaborar con la [Oficina Técnica NIK-NIRE] en el cierre ordenado, archivado de documentación etc



La planificación incluida en este punto tiene como objetivo **servir como base** para que el ofertante haga una **valoración propia** que ha de incluir en su oferta

Además, hay que tener en cuenta que en la fase actual del proyecto y con el conocimiento que se tiene del mismo, el margen de error de la planificación es de entre un 15%:- 25%

... especialmente en un proyecto de esta naturaleza en el que el alcance es amplio

De todas las áreas planificables (costes, alcance, calendario, recursos humanos, riesgos, calidad, etc)

- La planificación en **costes, alcance y RRHH** incluidas en la propuesta se considerarán como **vinculantes**
- El **calendario** (*la planificación temporal*) será considerada como **orientativa** puesto que es difícilmente exigible atenerse a una planificación temporal o de recursos cuando no se conocen todos los condicionantes organizativos y técnicos.

En líneas generales, la [Triple Constraint] (*Project management triangle*) establece tres variables relacionadas en un proyecto: [alcance], [coste] y [tiempo].

Si se fijan dos de las variables (*alcance y coste*) en base a la oferta, la tercera NO puede fijarse de antemano y debe ser definida en la planificación una vez iniciado el proyecto

La [planificación temporal] final se definirá en la [fase 0] de análisis / planificación trabajando con [EJIE] y la [Oficina Técnica NIK-NIRE]

No obstante de lo anterior, los ofertantes deberán incluir una **planificación temporal tentativa** con un doble objetivo:

- Permitir a [EJIE] **valorar el entendimiento del proyecto** en la fase de valoración subjetivas de ofertas.
- **Tener una idea aproximada de la duración del proyecto:** aunque la planificación temporal final se hará durante la fase de [planificación], una vez arrancado el proyecto, la estimación incluida en la [oferta] típicamente tendrá una desviación de entre un 15% y un 25% con lo que se puede aproximar la duración total del proyecto a partir de la planificación temporal ofertada.



La planificación definitiva del proyecto se realizará durante la fase de planificación del proyecto una vez adjudicado y conforme el [adjudicatario] adquiere un conocimiento más profundo del [proyecto]

En el presente punto se incluye una plantilla de planificación que el ofertante deberá concretar y extender en su propuesta y que como ya se ha señalado únicamente tiene como objetivo **valorar el entendimiento del proyecto**

En el presente punto se incluye una **plantilla de planificación** que las empresas ofertantes **deben incluir en su [oferta de servicios]**



Con el objetivo de poder comparar las diferentes [ofertas de servicios], la [planificación] debe **ajustarse** a lo que se expone a continuación en lo que se refiere a:

- [paquetes de trabajo] (**NO eliminar ningún [paquete de trabajo]** aunque SI se puede añadir alguno “debajo” de otro existente)
- [perfiles profesionales] (utilizar **estrictamente** los perfiles profesionales indicados)

El hecho de NO ajustarse a lo anterior implicará que la oferta NO será tomada en cuenta al NO poder compararse en igualdad de condiciones con el resto

La [planificación] se hace de la siguiente forma:

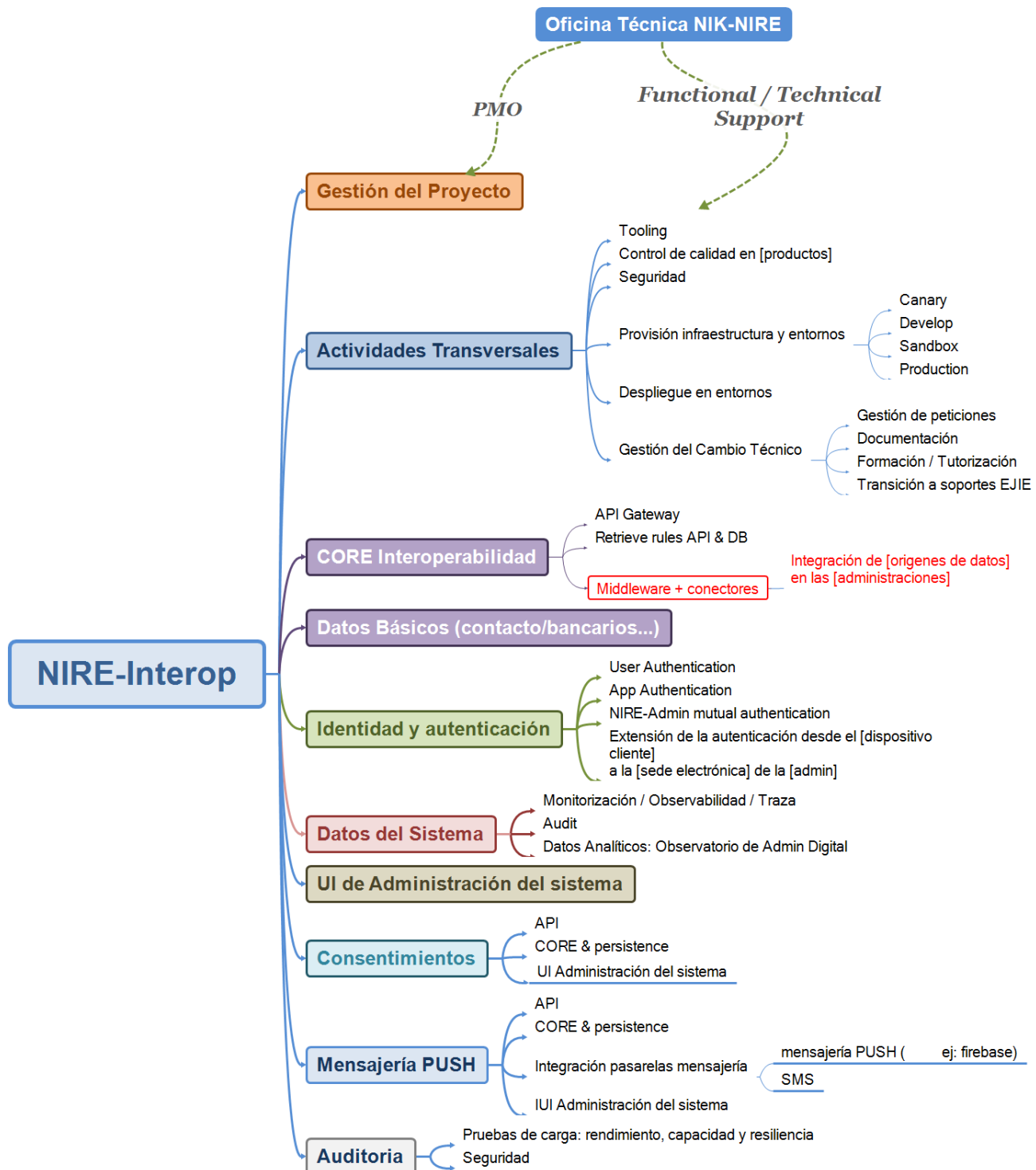
1. Se parte de un WBS (*work-breakdown-structure*): una descomposición de [paquetes de trabajo]
2. Se estiman los [recursos] a utilizar en cada [paquete de trabajo] y el [tiempo] a imputar en cada [paquete de trabajo]
3. Se secuencian [paquetes de trabajo] y se crea un [calendario]
4. Se estiman otros aspectos como [participantes] (*interesados / stakeholders*) o [riesgos]

Es importante tener en cuenta que **hay dos tipos de [paquetes de trabajo]**:

Paquetes de trabajo con alcance cerrado	Servicios en los que el entregable está definido Es el caso de todos los [paquetes de trabajo] excepto el de construcción del [middleware] y [conector](es) con los [orígenes de datos] en las [administraciones]
Paquetes de trabajo de carácter variable	En el caso de la construcción del [middleware] y [conector](es) con los [orígenes de datos] en las [administraciones], el [alcance] NO está definido al 100% y aunque se está trabajando en un [roadmap] donde se reflejarán los compromisos de integración en [NIRE] por parte de las [administraciones], en estos momentos es difícil hacer una [planificación] de: ▪ Cuántos [middleware] / [conector](es) hay que construir ▪ Cuándo hay que trabajar en [middleware] / [conector](es) ▪ El alcance de la construcción de [middleware] / [conector](es) ya que aunque el [middleware] es común, la construcción del [conector] con cada [administración] supondrá un <i>reto</i> diferente ... por esta razón, a diferencia del resto de [paquetes de trabajo] del [proyecto], este [paquete de trabajo] NO se plantea como un “entregable cerrado” sino que se trabajará como sub-proyectos dentro del [contrato]: 1. Desde [EJIE] + [Oficina Técnica] se trasladará la necesidad en forma de [alcance] documentado 2. La empresa adjudicataria hará una planificación vinculante en tiempo y coste incluyendo un [calendario de facturación] de los trabajos 3. [EJIE] y la [Oficina Técnica] aceptarán la [planificación] si es adecuada 4. La empresa adjudicataria ejecutará el trabajo en las condiciones planificadas en [2] y se irá facturando al [contrato] en función de los [hitos] pactados en la [planificación]

7.1 Alcance

El [alcance] se resume en la siguiente [descomposición de tareas] en la que se han señalado en **[rojo]** los [paquetes de trabajo] que tienen un alcance indeterminado / variable (**middleware + conectores**) y se tratarán como **[servicios variables]** tal y como se ha descrito antes.



Los [paquetes de trabajo son los siguientes:

Cod	Work-Package
1	Gestión del proyecto
2	Actividades transversales
2.1	Tooling
2.2	Control de [calidad] en [productos]
2.3	Seguridad
2.4	Provisión infra y entornos
2.5	Despliegue en entornos
2.6	Gestión del Cambio Técnico
3	CORE Interoperabilidad
3.1	API Gateway
3.2	Retrieve rules & DB
3.3	Middleware & conectores
4	Datos Básicos (contacto, bancarios...)
5	Identidad y autenticación
5.1	User Authentication
5.2	App Authentication
5.3	NIRE-Admin mutual authentication
5.4	Extensión autenticación a [sede electrónica]
6	Datos del Sistema
6.1	Monitorización / Observabilidad / Traza
6.2	Audit
6.3	Datos Analíticos: Observatorio Admin Digital
7	UI de Administración del Sistema
8	Consentimientos
8.1	API
8.2	CORE
8.3	UI Administración del sistema
9	Mensajería PUSH
9.1	API
9.2	CORE & persistence
9.3	Integración pasarelas mensajería
9.4	UI Administración del sistema
10	Auditoría
10.1	Pruebas de carga / rendimiento / resiliencia
10.2	Seguridad y privacidad (<i>pen testing, code audit...</i>)

7.2 Calendario

En una plantilla como la siguiente se indicará la planificación:

Cod	Work-Package	Month1		Mont2		Month3				MontN	
		Q1	Q2	Q3	Q4	Q5	Q5			Q _{n-1}	Q _n
1	Gestión del proyecto										
2	Actividades transversales										
2.1	Tooling										
2.2	Control de [calidad] en [productos]										
2.3	Seguridad										
2.4	Provisión infra y entornos										
2.5	Despliegue en entornos										
2.6	Gestión del Cambio Técnico										
3	CORE Interoperabilidad										
3.1	API Gateway										
3.2	Retrieve rules & DB										
3.3	Middleware & conectores	NO planificar recursos									
4	Datos Básicos (contacto, bancarios...)										
5	Identidad y autenticación										
5.1	User Authentication										
5.2	App Authentication										
5.3	NIRE-Admin mutual authentication										
5.4	Extensión autenticación a [sede electrónica]										
6	Datos del Sistema										
6.1	Monitorización / Observabilidad / Traza										
6.2	Audit										
6.3	Datos Analíticos: Observatorio Admin Digital										
7	UI de Administración del Sistema										
8	Consentimientos										
8.1	API										
8.2	CORE										
8.3	UI Administración del sistema										
9	Mensajería PUSH										
9.1	API										
9.2	CORE & persistence										
9.3	Integración pasarelas mensajería										
9.4	UI Administración del sistema										
10	Auditoría										
10.1	Pruebas de carga / rendimiento / resiliencia										
10.2	Seguridad y privacidad (<i>pen testing, code audit...</i>)										

7.3 Recursos

Con el fin de simplificar la descripción y la evaluación, los [recursos] que van a intervenir en la ejecución del presente expediente de contratación se van a agrupar en los siguientes [perfiles]:

MGR	Manager / Consultor de referencia	▪ Project Management ▪ Consultores de referencia que participan en el proyecto proporcionando guía y conocimiento técnico / funcional de referencia
ESP	Técnico/a especialista de alto nivel	▪ Arquitecto/a de soluciones ▪ Especialista de seguridad ▪ Especialista en Interoperabilidad ▪ Especialista DevOps ▪ Consultor/a funcional
TEC	Técnico/a	▪ Desarrollador/a ▪ Test QA



- La oferta se ajustará a los [perfiles] anteriores y **NO otros** para poder comparar propuestas
- El ofertante *asimilará* en los anteriores cualquier [perfil] que vaya a participar en el proyecto
- Cualquier oferta que incluya [perfiles] distintos a los anteriores **quedará automáticamente descartada**

En función de estos [perfiles] se estimará la **participación en jornadas normales de 8 horas** en cada uno de los [paquetes de trabajo]



- Utilizar estrictamente los [perfiles] indicados en la tabla anterior (MG/ESP/TEC)

Se indicará la [planificación de recursos en el tiempo]: para cada mes de trabajo se indicará el [número de jornadas] por [perfil] en el siguiente formato:

Y como **resumen** de lo anterior:

Cod	Work-Package	Jornadas MGR	Jornadas ESP	Jornadas TEC
1	Gestión del proyecto			
2	Actividades transversales			
2.1	Tooling			
2.2	Control de [calidad] en [productos]			
2.3	Seguridad			
2.4	Provisión infra y entornos			
2.5	Despliegue en entornos			
2.6	Gestión del Cambio Técnico			
3	CORE Interoperabilidad			
3.1	API Gateway			
3.2	Retrieve rules & DB			
3.3	Middleware & conectores			
4	Datos Básicos (contacto, bancarios...)			
5	Identidad y autenticación			
5.1	User Authentication			
5.2	App Authentication			
5.3	NIRE-Admin mutual authentication			
5.4	Extensión autenticación a [sede electrónica]			
6	Datos del Sistema			
6.1	Monitorización / Observabilidad / Traza			
6.2	Audit			
6.3	Datos Analíticos: Observatorio Admin Digital			
7	UI de Administración del Sistema			
8	Consentimientos			
8.1	API			
8.2	CORE			
8.3	UI Administración del sistema			
9	Mensajería PUSH			
9.1	API			
9.2	CORE & persistence			
9.3	Integración pasarelas mensajería			
9.4	UI Administración del sistema			
10	Auditoría			
10.1	Pruebas de carga / rendimiento / resiliencia			
10.2	Seguridad y privacidad (<i>pen testing, code audit...</i>)			

7.4 Coste

IMPORTANTE: En ningún caso se deberá incluir [información económica] (costes) en el documento de [propuesta de aplicación de criterios subjetivos] (*propuesta técnica*); **TODA la información económica (costes) debe incluirse en su totalidad en la [propuesta de aplicación de fórmulas] (económica y otros criterios)**

En la [propuesta de aplicación de fórmulas] (*nunca en la [propuesta técnica de aplicación de criterios subjetivos]*) se incluirá el [**Presupuesto Total**] del proyecto (*valor estimado*) que será el utilizado para valorar económicamente la oferta (*ver [Criterios de Valoración] en el [Documento de Condiciones Administrativas Particulares]*)

Con el objetivo de tener una **mayor información sobre el origen de este presupuesto total**, en la [propuesta de aplicación de fórmulas] (*nunca en la [propuesta técnica]*) se incluirá un detalle orientativo del cálculo del [presupuesto] por parte del ofertante.

El [presupuesto] total debería basarse en la agregación de los [costes unitarios] de cada [paquete de trabajo] calculada en función de las [tarifas] de los [recursos] y el número de [jornadas] planificadas:

$$\text{coste actividad} = \text{coste recursos} \times \text{jornadas planificadas}$$

Se utiliza como base a un cuadro de tarifas por [perfil] anterior:

Cod	Recurso
MG	Manager / Consultor de referencia
ESP	Técnico/a especialista de alto nivel
TEC	Técnico/a

 **La oferta se ajustará a los [perfiles] anteriores y NO otros** para poder comparar propuestas

El ofertante *asimilará* en los anteriores cualquier [perfil] que vaya a participar en el proyecto

Cualquier oferta que incluya [perfiles] distintos a los anteriores **quedará automáticamente descartada**

... y en base la agregación del coste / perfil / [jornadas normales] (8 horas) aplicadas a los [paquetes de trabajo] identificados en el [alcance] se obtiene el [coste] total del proyecto



En el [documento de condiciones administrativas] se encuentra la **plantilla de proposición económica**

7.5 Productos Entregables

En este punto se describen a alto nivel los (*productos*) [entregables] que son *creados* ejecutando las [actividades] descritas en el punto [objeto del contrato]

Los [productos] entregables y las condiciones aplicables a los mismos se resumen a continuación:

7.5.1 Infraestructura y entornos



Todos los [productos] del [proyecto] se desplegarán en una **infraestructura propia** y ad-hoc: **un nuevo [tenant] en [BATERA]** (*EJIE*)

La **provisión** de esta infraestructura ha de ser gestionada por el [adjudicatario] del presente [expediente de contratación] trabajando con:

- Personal técnico de todas diferentes áreas de [EJIE]
- Oficina Técnica [NIK-NIRE]

Algunos componentes de la [infraestructura] que en función de las necesidades de arquitectura puede ser necesario provisionar en [BATERA] son:

Gestión de cargas (*workloads*) basadas en [containers]

- Entorno [kubernetes] basado en la tecnología que designe [EJIE]

Persistencia de datos

- Estructurados: [ORACLE](#) / [MySQL](#) / [PostgreSQL](#)
- NO estructurados: [MongoDB](#)
- Object (BLOB): S3 compatible storage (ej: [scality](#))
- Otros que se puedan identificar como necesarios

Cache

- [Redis](#) / [Hazelcast](#) / *otro que se identifique en el [proyecto]*

Comunicaciones / Seguridad

- WAF (*web application firewall*)
- Proxies / ingress controllers / etc
- Servidores web ([apache](#))

Access Management

- [Keycloak](#) / *otro que se identifique en el [proyecto]*

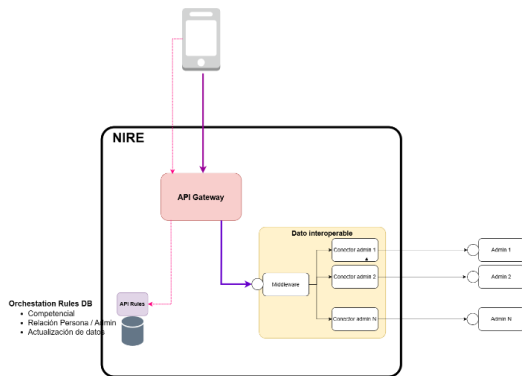
API Management

- Producto de gestión de API que se identifique en el [proyecto] ([WSO2](#), [Kong](#), etc)



La infraestructura final a provisionar se definirá junto con [EJIE] y la [OT NIK-NIRE] durante la ejecución del proyecto en base a la arquitectura definida.

7.5.2 CORE Interoperabilidad



El [CORE interoperabilidad] está compuesto por la **integración de [componentes]**, algunos basados en productos de mercado y otros componentes desarrollados ad-hoc:

- API Gateway
- Rules API & DB
- Middleware + conectores

Para los [componentes] desarrollados ad-hoc:

- Lenguaje: JAVA (JDK > 17)
- Servidor de aplicaciones: Apache Tomcat / SPRING Boot
(se definirá para cada necesidad en la ejecución del proyecto junto con [EJIE] y la [Oficina Técnica])

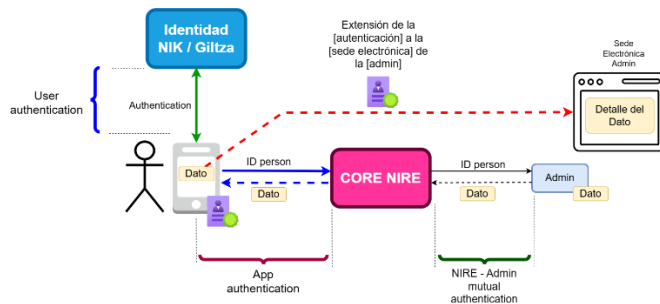
En lo que se refiere a los [desarrollos ad-hoc]:



Todos los [productos] se entregarán completamente funcionales en todos los entornos

La **aceptación** de los [productos] entregados **dependerá del criterio de [EJIE]** contando con la ayuda de la [OT NIK-NIRE] teniendo en cuenta:

- El correcto funcionamiento del sistema en todos los entornos
- Los informes y certificaciones de:
 - Rendimiento / Capacidad y resiliencia
 - Seguridad

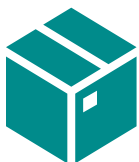


User authentication	Autenticación de la persona usuaria en el [dispositivo cliente] (móvil / web) utilizando una identidad / autenticación (<i>proporcionada por IZENPE</i>)
App Authentication	Autenticación [app] <-> [CORE NIRE]
NIRE – Admin mutual authentication	Autenticación mutua entre [CORE-NIRE] y el [origen de datos]



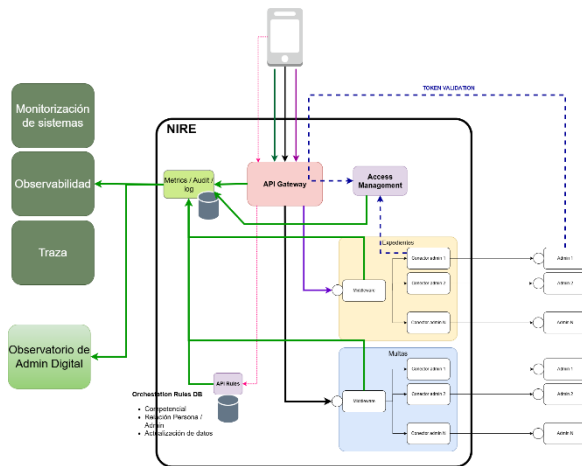
- El correcto funcionamiento del sistema en todos los entornos
- Los informes y certificaciones de:
 - Rendimiento / Capacidad y resiliencia
 - Seguridad

- **Interoperabilidad** con [orígenes de datos] en las [administraciones] a través de [NIRE-Interop] tanto para la [consulta de datos] como para la [actualización] (en aquellos casos que se considere necesario)
- **[Repositorio común de datos básicos]** depurados por las propias personas usuarias y utilizables por cualquier [administración]



- El correcto funcionamiento del sistema en todos los entornos
- Los informes y certificaciones de:
 - Rendimiento / Capacidad y resiliencia
 - Seguridad

7.5.5 Datos del sistema



El entregable en esta área es la integración de [componentes] (*productos estándar y desarrollos / parametrizaciones ad-hoc*) para:

- | | |
|--|---|
| <p>1 Monitorización / observabilidad / Traza</p> | <ul style="list-style-type: none"> ■ Salud del sistema: ¿puede dar servicio de forma normal? ■ Traza: información (logs) que permitan depurar una [petición de interoperabilidad] |
| <p>2 Datos analíticos:
Observatorio de Administración Digital</p> | <ul style="list-style-type: none"> ■ Recolección de [indicadores] con el objetivo de ser “mostrada” en los [cuadros de mando] del [Observatorio de Administración Digital] |
| <p>3 Audit de uso de los [servicios de interoperabilidad]</p> | <ul style="list-style-type: none"> ■ Información de [auditoría] de quién / cuándo utiliza los [servicios de interoperabilidad] |



- Los sistemas de [monitorización] / [observabilidad] se entregarán integrados en el [centro de mando] de [EJIE] para todos los entornos
La **aceptación** de los [productos] en este punto entregados **dependerá del criterio de [EJIE]** (*específicamente del [centro de mando]*)
- Los sistemas que permiten [trazar] una [petición de datos] serán **aceptados en función del criterio de [EJIE]** contando con la ayuda de la [OT NIK-NIRE] teniendo en cuenta el correcto funcionamiento del sistema en todos los entornos
- Los sistemas que permiten la [auditoría] de una [petición de datos] serán **aceptados en función del criterio de [EJIE]** contando con la ayuda de la [OT NIK-NIRE] teniendo en cuenta el correcto funcionamiento del sistema en todos los entornos
- Los [datos analíticos] se considerarán *entregados* cuando estos datos sean cargados automáticamente en el [data-lake] del [Observatorio de Administración Digital] conforme a lo definido.

7.5.6 UI de Administración del sistema

La [UI de Administración del sistema] es un **desarrollo a medida** (*ad-hoc*) en base a las siguientes tecnologías:

UI	Java (Vaadin > v24) <i>Se podría valorar la utilización de [react] pero inicialmente y de forma preferente se utilizará [Vaadin] con el objetivo de agilizar y simplificar el desarrollo e integración en base a una tecnología única en Java</i>
API	Java Servicios REST
CORE	Java (Apache Tomcat / SPRING Boot)
DB	Oracle / MySql / PostgreSQL / otras



Todos los [productos] se entregarán completamente funcionales en todos los entornos

La **aceptación** de los [productos] entregados **dependerá del criterio de [EJIE]** contando con la ayuda de la [OT NIK-NIRE] teniendo en cuenta:

- El correcto funcionamiento del sistema en todos los entornos
- Los informes y certificaciones de:
 - Rendimiento / Capacidad y resiliencia
 - Seguridad

7.5.7 Consentimientos

El sistema de [consentimientos] es un **desarrollo a medida** (*ad-hoc*) en base a las siguientes tecnologías:

UI	Java (Vaadin > v24) <i>Se podría valorar la utilización de [react] pero inicialmente y de forma preferente se utilizará [Vaadin] con el objetivo de agilizar y simplificar el desarrollo e integración en base a una tecnología única en Java</i>
API	Java Servicios REST
CORE	Java (Apache Tomcat / SPRING Boot)
DB	Oracle / MySql / PostgreSQL / otras



Todos los [productos] se entregarán completamente funcionales en todos los entornos

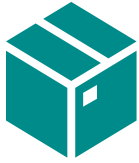
La **aceptación** de los [productos] entregados **dependerá del criterio de [EJIE]** contando con la ayuda de la [OT NIK-NIRE] teniendo en cuenta:

- El correcto funcionamiento del sistema en todos los entornos
- Los informes y certificaciones de:
 - Rendimiento / Capacidad y resiliencia
 - Seguridad

7.5.8 Mensajería PUSH

El sistema de [mensajería PUSH] es un **desarrollo a medida** (*ad-hoc*) en base a las siguientes tecnologías:

UI	Java (Vaadin > v24) <i>Se podría valorar la utilización de [react] pero inicialmente y de forma preferente se utilizará [Vaadin] con el objetivo de agilizar y simplificar el desarrollo e integración en base a una tecnología única en Java</i>
API	Java Servicios REST
CORE	Java (Apache Tomcat / SPRING Boot)
DB	MongoDB / Oracle / MySql / PostgreSQL / otras



Todos los [productos] se entregarán completamente funcionales en todos los entornos

La **aceptación** de los [productos] entregados **dependerá del criterio de [EJIE]** contando con la ayuda de la [OT NIK-NIRE] teniendo en cuenta:

- El correcto funcionamiento del sistema en todos los entornos
- Los informes y certificaciones de:
 - Rendimiento / Capacidad y resiliencia
 - Seguridad

7.5.9 Middleware y conectores con los [orígenes de datos] en las [administraciones]

El [middleware] y [conectores] son [productos] que se construyen y entregan en base a sub-proyectos ad-hoc *encargados* al contrato en base a un análisis y planificación previos aceptados por [EJIE]



Todos los [middleware] y [conectores] deberán ser funcionales en todos los entornos



En aquellos entornos donde NO se pueda acceder a datos reales (*todos aquellos “previos” a [PROD]*) **se simulará el [origen de datos]** para conseguir que el [middleware] y [conector] sea totalmente funcional.

La **aceptación** de los [productos] entregados **dependerá del criterio de:**

- **[EJIE]** contando con la ayuda de la [OT NIK-NIRE]
- La **[administración] origen de datos**

... se tendrá en cuenta:

- El correcto funcionamiento del sistema en todos los entornos
- Los informes y certificaciones de:
 - Rendimiento / Capacidad y resiliencia
 - Seguridad

7.5.10 Documentación para desarrolladores y entorno sandbox

La [documentación para desarrolladores] y el [entorno sandbox] son **fundamentales en el proyecto** dado que van a ser utilizados por desarrolladores externos al proyecto de otras administraciones

Lo anterior es de especial aplicación con los [productos] entregables de:

- Identidad y autenticación > autenticación mutua [CORE NIRE] <-> [admin]
- Middleware y conectores con los orígenes de datos
- Mensajería PUSH
- Consentimientos



Ninguno de los [entregables] relacionados con los [productos] anteriores se considerará “entregado” hasta que no esté correctamente **documentado en la [web del desarrollador]** y se pueda **testear** en el entorno [sandbox]

7.5.11 Auditoria

Se entregarán las [certificaciones] realizadas por entidades especializadas en las siguientes áreas:

Rendimiento / Capacidad y resiliencia	Rendimiento	Asegurar que el sistema responde con la rapidez esperada incluso en momentos de gran carga
	Capacidad elasticidad	/ Asegurar que el sistema <i>soporta</i> el número de personas usuarias esperado: <i>asegurar que los recursos del sistema se reconfiguran (crecen / decrecen) para adaptarse a la carga</i>
	Resiliencia	Asegurar que el sistema puede <i>seguir funcionando con normalidad</i> en caso de que alguno o todos los componentes fallen: <i>asegurar que los mecanismos de contingencia funcionan correctamente</i>
Seguridad	Certificar que el sistema cumple con los requisitos de seguridad en base a: ▪ Simulaciones de penetración (pen-testing) ▪ Auditorías de configuración de componentes y código	
Privacidad desde el diseño y por defecto	Certificar que el sistema cumple con los requisitos de privacidad en base a: ▪ Auditorías de cumplimiento de medidas que aseguren la aplicación del principio de [privacidad desde el diseño y por defecto] establecido en el artículo 25 del RGPD.	



Los [requisitos] a nivel de rendimiento / capacidad y resiliencia así como de seguridad serán fijados por [EJIE] y la [OT NIK-NIRE] en función del número de [personas usuarias] estimadas y del número de [orígenes de datos] integrados



La **aceptación** de las [certificaciones] entregados **dependerá del criterio de [EJIE]** contando con la ayuda de la [OT NIK-NIRE] teniendo en cuenta la calidad / metodología de las pruebas (*rendimiento / capacidad / resiliencia y seguridad*) realizadas

7.6 Calidad

La [calidad] se trabajará en dos ámbitos:

Calidad en los [procesos]

Gestión del proyecto

Es **responsabilidad de la [PMO] de la [Oficina Técnica NIK-NIRE]** así que en este punto se seguirán las directrices de la [PMO] y se colaborará con ella

Calidad en los [productos]

En el punto [6 – Objeto del Contrato] se han detallado las áreas de [calidad de los productos] en las que hay que trabajar

■ Calidad en las **infraestructuras y productos**



- La instalación de [productos] *comodity (de mercado / open source)* que se utilicen en la arquitectura será coordinada con [EJIE] y preferentemente se ejecutarán en **entorno [Kubernetes]** con el objetivo de tener la elasticidad y resiliencia de esta plataforma.

■ Calidad en los **desarrollos**

En lo que se refiere a los componentes que se basan en [desarrollos a medida (ad-hoc)], los requisitos comunes en cuanto a [calidad] en los [productos] entregables son:



- Todos los [componentes] deberán poder ser desplegados y ser funcionales en un [entorno local] de [PC] con el soporte si es necesario de [containers] pero sin dependencias de servicios externos que NO se ejecuten en el [entorno local]
... es decir: **el [CORE Interop] (todos sus componentes) debe funcionar al 100% en un [entorno local]**
- Se utilizarán sistemas de [control de calidad del código] automatizadas de forma sistemática para detectar:
 - Problemas de [seguridad] derivados de vulnerabilidades de código (ej: *sql inyección, etc*)
 - Complejidad del código, copy & paste, etc
 - etc
- En todos los desarrollos y con el objetivo de asegurar la [calidad] se utilizarán:
 - El [tooling] que [EJIE] y la [OT NIK-NIRE]
 - Los [frameworks de desarrollo] que [EJIE] y la [OT NIK-NIRE] designen
 - Los [patrones de diseño] que [EJIE] y la [OT NIK-NIRE] designen
 - La estructura de proyectos que [EJIE] y la [OT NIK-NIRE] designen
 - Las directrices y normas de [naming], [code style], etc que [EJIE] y la [OT NIK-NIRE] designen

! [EJIE] y la [OT NIK-NIRE] auditarán todos los aspectos anteriores para asegurarse de su correcta aplicación; si NO es así **NO se aceptarán** los [componentes] correspondientes

7.7 Comunicaciones

7.7.1 Stakeholders

A nivel de comunicaciones hay que tener en cuenta el [catálogo de involucrados] (*stakeholders*) que en una primera aproximación de alto nivel (*y que la [PMO] refinará de forma continua*) es el siguiente:

Entidad	Nivel	Rol
Dirección de Estrategia Digital	Dirección Funcional	- Definición de la estrategia [NIK-NIRE] - Coordinación con las [entidades IT] de otras [administraciones] - Responsable de la gobernanza del dato - Participa en la definición funcional
Dirección de Atención a la Ciudadanía e Innovación Administrativa	Dirección Funcional	- Definición de la estrategia [NIK-NIRE] - Coordinación con otras [administraciones] - Responsable de la definición funcional - Validación de la solución funcional - Gestión del cambio organizativo
Administración Digital EJIE	Dirección Funcional Técnico	- Dirección del proyecto - Definición funcional y técnica - Validación de la solución funcional y técnica - Gestión del cambio en [EJIE] - Proporciona soporte técnico - Coordinación con áreas técnicas de [EJIE]
Oficina de proyectos [NIK-NIRE]	Dirección Funcional Técnico	- Gestión del proyecto - Participa en la [planificación] y maneja las [líneas base] - Monitorización y control de la ejecución: - verificación de que se está trabajando en el [alcance] planificado y con la calidad esperada - reporte a nivel de seguimiento - Identificación de riesgos - Gestiona la documentación del proyecto - Validación de la solución funcional y técnica - Gestión del cambio global - Coordinación con: [Administración Digital EJIE] - Áreas técnicas de [EJIE] [Administraciones] (EJGV, Diputaciones, Aytos, etc) - Otros proyectos del [programa NIK-NIRE] - Soporte técnico y funcional
Adjudicatario del proyecto	Funcional Técnico	- Participa en la definición funcional y técnica - Participa en la planificación - Construye los productos - Reporta a la [OT-NIRE] la evolución de la ejecución - Define y ejecuta las pruebas de los productos - Informa y ayuda a la [oficina técnica] en su labor de [PM] (<i>en particular de reporte</i>) y [gestión del cambio]

Otros [proyectos] del [programa NIK-NIRE]	Funcional Técnico	Proporcionan requisitos a algunos módulos a construir en el presente [proyecto]
Administraciones Vascas y Sociedades Públicas Informáticas	Funcional Técnico	- Definición funcional y técnica - Validación de la solución funcional y técnica - Construyen los [órdenes de datos]

7.7.2 Estructuras de control y comunicaciones

El modelo organizativo de estructuras de control y comunicaciones es el siguiente:

7.7.2.1 Comité Director: visión del proyecto a nivel de dirección

Componentes	→ Dirección Área de [EJIE] → Responsable de cuenta por parte del [adjudicatario] → Responsable del proyecto por parte del [adjudicatario] → Responsable de la [Oficina Técnica NIK-NIRE] → Cualquier persona de la que se considere necesario su asistencia
Reuniones	→ Lugar: EJIE / remoto → Periodicidad: Trimestral y en función de las necesidades puntuales del proyecto, en base a convocatorias formales por parte de la dirección por parte del [adjudicatario] o de [EJIE]
Temas	→ Seguimiento ejecutivo → Entorno del proyecto: protección de las condiciones de existencia del mismo. → Variaciones en el alcance → Penalizaciones → Cualquier tema relativo al [contrato] que se considere necesario

7.7.2.2 Seguimiento Funcional / Técnico

Componentes	→ Responsable del proyecto por parte del [adjudicatario] → Responsables de proyectos por parte de [EJIE] → Personas técnicas relevantes del proyecto → Personas técnicas de la [Oficina de Proyecto NIK-NIRE] → Cualquier persona de la que se considere necesario su asistencia
Reuniones	→ Lugar: EJIE / remoto → Periodicidad: Mensual y en función de las necesidades puntuales del proyecto, en base a convocatorias formales por parte de la dirección por parte del [adjudicatario] o de [EJIE]
Temas	→ Monitorización y Control: seguimiento detallado → Aprobación de nuevas necesidades de construir [middleware] / [conectores] → Revisión de cambios → Monitorización de riesgos → Cualquier tema relativo al [contrato] que se considere necesario

7.8 Riesgos

En la ejecución del presente contrato **inicialmente** se identifican algunos riesgos que se enumeran a continuación.

Riesgo	Servicio	Impacto
Problemas en la comunicación con la [OT NIK-NIRE]	Gestión del Proyecto	Medio
Problema para la incorporación de Administraciones a las iniciativas	Construcción e Implantación	Alto
Documentación proporcionada a las [administraciones] de baja calidad que <i>ralentiza</i> los trabajos responsabilidad de las [administraciones]	Construcción	Alto
Inestabilidad en el equipo de trabajo	Todos	Alto
No es posible el cumplimiento del calendario al ritmo esperado	Todos	Alto
Problemas en la provisión de la infraestructura (<i>indefinición, retrasos, etc</i>)	Construcción e Implantación	Alto

8 Contenido de la Oferta Técnica

La [propuesta técnica] será utilizada para evaluar el entendimiento del servicio a prestar en base a lo especificado en el presente documento de condiciones técnicas



El contenido de la propuesta debe seguir obligatoriamente el siguiente índice
(las ofertas que NO sigan este índice serán descartadas)

Incide de la propuesta

1. Resumen y elementos diferenciales de la oferta

2. Arquitectura propuesta

Utilizando como base el punto [3 - Descripción del proyecto y los [productos] a construir] **desarrollar** (*profundizar*) en **cada uno de los [paquetes de trabajo]** desde un punto de vista funcional / técnico:

1. Detallando la **solución propuesta** a partir de lo recogido en el presente documento (*se pueden proponer alternativas*)
2. Identificando **puntos de mejora / optimización**
3. Identificando **[problemas] / [riesgos]** y posibles estrategias de mitigación
4. ... y cualquier otro elemento que se considere relevante para el entendimiento de la solución propuesta

Los [paquetes de trabajo] en los que hay que incluir lo anterior son:

- 2.0 Provisión de Infraestructura y entornos
- 2.1 CORE de interoperabilidad persona-administración
- 2.2 Identidad y autenticación
- 2.3 Datos básicos (*contacto, bancarios, etc*)
- 2.4 Datos del sistema: trace / monitorización/observabilidad / audit / datos analíticos
- 2.5 Consentimientos
- 2.6 Datos que se interoperan
- 2.7 UI de Administración del sistema
- 2.8 Mensajería PUSH
- 2.9 Auditoria del sistema



El contenido de este [documento de condiciones técnicas] y la [oferta técnica] serán los **puntos de partida** del trabajo de definición de la [arquitectura] final.

Por esta razón, la [oferta técnica] es fundamental para evaluar el entendimiento del [proyectos] por parte del [ofertante].

El contenido del presente documento si bien llega a un elevado nivel de detalle, no llega a profundizar en todos los aspectos, tecnologías o funcionalidades y en ocasiones se detallan diferentes alternativas sin apostar claramente por una en concreto

... la [oferta técnica] tiene que profundizar en base a los puntos anteriores



La propuesta técnica se tomará como punto de partida para los [productos] a construir y se trabajará y refinará junto con [EJIE] y la [Oficina Técnica NIK-NIRE] modificando los puntos que se considere necesario.



En caso de no llegar a un acuerdo en algún punto de la [arquitectura] final, prevalecerá el criterio de [EJIE]

... en otras palabras: la solución (*productos, arquitectura, etc*) incluidos en la [oferta técnica] pueden ser modificadas total o parcialmente durante el trabajo inicial con [EJIE] y [OT NIK-NIRE] para definir la [arquitectura] final

En todo caso, **la propuesta se utilizará para la evaluación de la [oferta] según los [criterios] que se recogen en el [documento de condiciones administrativas]**

Además de la [arquitectura propuesta] se incluirán algunos puntos de la [planificación]:

3. Planificación

3.1. Alcance

Incluir la [planificación de alcance] del punto [7.1 – Planificación de alcance] bajando de nivel en algún [paquete de trabajo] si se considera necesario



NO cambiar la [WBS] del punto [7.1] salvo la inclusión de [paquetes de trabajo] *debajo* de los propuestos si se considera necesario

Si se cambia la [WBS] no se podrán comparar las [ofertas] en igualdad de condiciones y la oferta quedará descartada

3.2. Calendario

Incluir la [planificación de calendario] siguiendo el modelo del punto [7.2 – Planificación de calendario]

3.3. Recursos

Incluir la [planificación de recursos] siguiendo el modelo del punto [7.3 – Planificación de Recursos]

Además, para cada uno de los [paquetes de trabajo] se detallará el **[equipo]** que participará en el [paquete de trabajo] cumplimentando la siguiente [tabla] para cada uno de ellos:

Persona (iniciales)					
Perfil / funciones (solo uno - el mismo que se utiliza en la [planificación])	MGR	Manager / Consultor de referencia	[]	Project Management	
			[]	Consultor de referencia que participa en el proyecto proporcionando guía y conocimiento técnico / funcional de referencia	
	ESP	Técnico/a especialista de alto nivel	[]	Arquitecto/a de soluciones	
			[]	Especialista de seguridad	
			[]	Especialista en Interoperabilidad	
			[]	Especialista DevOps	
			[]	Consultor/a funcional	
	TEC	Técnico/a	[]	Desarrollador/a	
			[]	Test QA	
	Conocimientos técnicos / funcionales aplicables al [paquete de trabajo]			Únicamente un máximo de 5 ítems en una lista enumerada	
	Número estimado de [jornadas] completas de 8 horas a dedicar al [paquete de trabajo]				
	Otros [paquetes de trabajo] en los que participará			Enumerar los [paquetes de trabajo]	

(NO incluir en la [oferta técnica] ningún dato económico)

3.4. Riesgos

Incluir la [planificación de riesgos] siguiendo el modelo del punto [7.8 – Riesgos] modificando o ampliando la identificación que se incluye en el documento



NO es necesario incluir nada sobre la [planificación de calidad] o [planificación de comunicaciones] ya que NO se tendrán en cuenta en la evaluación técnica



Como ya se ha señalado en varios puntos del documento, se ha trabajado intensamente en un diseño / arquitectura **a muy alto nivel** como **punto de partida** para el trabajo a desarrollar en el presente contrato.

En este sentido, se ha trabajado en una [POC=*Prueba de Concepto*] de la parte de [interoperabilidad] y que **se pone a disposición de las empresas ofertantes** para que puedan **evaluar con mayor conocimiento** al menos una de las partes del sistema a construir.

Todo el contenido de la [POC] está disponible en la siguiente dirección electrónica: [\[descarga POC\]](#)



Se trata de una [POC] que como tal se ha construido de forma rápida con el objetivo de:

- **eliminar incertidumbres técnicas**
- **facilitar el entendimiento por parte de los ofertantes**

Como tal [POC] NO se han *tenido en cuenta* muchos de los aspectos que se están exponiendo en el presente documento y que **SI habrá que tener en cuenta en el [producto final]**, es decir, **la [POC] solo debe ser tomada en cuenta como referencia funcional y de arquitectura.**

En cualquier caso, esta [POC] es una **primera aproximación de una parte de la [arquitectura]**: *faltan módulos y aspectos que SI estarán en la [arquitectura] final.*

Durante la ejecución del proyecto y en la primera fase de definición de la [arquitectura] se partirá de dos cosas:

- La [oferta] de la empresa ofertante
- La [POC]

... para *-como se ha destacado antes-* y trabajando con [EJIE], [OT-NIRE] y [administraciones] definir esa [arquitectura final]