


**Resumen de Situación
GUIA**

11 de abril de 2014


	Resumen de Situación
	GUIA

Hoja de Control del Documento

Información del Documento			
Título	Resumen de Situación GUIA		
Nombre del fichero	DGPD.IV-20140411-Informe_Resumen_Proyecto_GUIAv1.1.odt		
Versión	1.1		
Elaborado por	Antonio Blanco Morales	Fecha Elaboración	11/04/2014
Aprobado por		Fecha Aprobación	
Confidencialidad			


Control de Versiones			
Versión	Descripción de los cambios	Elaborado por	Fecha Elaboración
1.0	Elaboración inicial del documento	ABM	02/04/2014
1.1	Inclusión de carga de organismos y Administración funcional	ABM	11/04/2014

Lista de Distribución	
Apellidos, Nombre	Cargo / Función

	Resumen de Situación
	GUIA

Índice

1.INTRODUCCIÓN.....	4
2.FUNCIONALIDAD.....	4
2.1.Ciclo de Vida de la Identidad.....	4
2.2.Directorio Corporativo.....	6
2.2.1.Estructura Funcional.....	6
2.2.2.Repositorio Central de Datos de Usuario.....	7
2.3.Integración.....	7
2.3.1.Virtualización de directorios.....	8
2.3.2.Integraciones actuales.....	8
2.3.3.Integraciones adicionales.....	9
2.4.Acceso al puesto.....	11
2.4.1.Login con tarjeta.....	11
2.4.2.Single Sign-On de escritorio.....	12
2.4.3.Single Sign-On vía web.....	12
3.MEJORAS EVOLUTIVAS.....	13
3.1.Evolución de la gestión de autorizaciones de acceso.....	13
3.2.Conectores adicionales.....	15
3.3.Evolución de la plataforma de base.....	15
3.4.Otras líneas de evolución.....	15
4.TAREAS OPERATIVAS PARA SU PUESTA EN MARCHA Y MANTENIMIENTO.....	16
4.1.Incorporación del resto de organismos.....	18
4.2.Carga de personas externas.....	19
4.3.Administración funcional.....	19
5.DEPENDENCIAS CON OTROS SISTEMAS (NAOS).....	20

	Resumen de Situación
	GUIA

1. INTRODUCCIÓN

Se pretende aportar en un documento, lo más escueto y directo posible, la situación actual del proyecto GUIA, incluyendo evolución, estimaciones y necesidades para la implantación.

Este documento se elabora a partir de una petición realizada por la Coordinadora de Política Informática y cubrirá:

1. Funcionalidad
2. Mejoras evolutivas
3. Tareas operativas para su puesta en marcha y mantenimiento
4. Dependencias con otros sistemas (NAOS)

2. FUNCIONALIDAD

GUIA es un sistema muy complejo, por lo que se expondrá la funcionalidad organizada entorno a cuatro áreas funcionales:

1. Gestión del Ciclo de Vida de la Identidad
2. Directorio Corporativo
3. Integración
4. Acceso al puesto

2.1. Ciclo de Vida de la Identidad


Se cubre todo el conjunto de eventos asociados a una identidad digital, desde su incorporación a la organización hasta el cese de relación.

Los **usuarios** de esta funcionalidad son:


- Área de Personal/Recursos Humanos¹
- Responsables de Unidades (equiparables a Jefaturas de Servicio y cargos superiores con responsabilidad en unidades dentro de la organización).
- Cada persona: Es un sistema que potencia el autoservicio para:
 - Cambios de contraseña mediante certificado digital
 - Edición de datos de ubicación y contacto

Se destacan los eventos más importantes y que más lógica implican:

¹ No es requisito que sea este área. Su principal función es ubicar a las personas dentro de la estructura del Organismo.

	Resumen de Situación
	GUIA

- Entrada en la organización:
 - Para personal propio se obtienen los datos del sistema de RR.HH. (actualmente SIRhUS, pero estudiados el resto, entre ellos GERHONTE). Hay intervención para situar a la persona dentro del organigrama en la unidad en la que prestará sus servicios. GUIA lanza la creación de la cuenta de correo corporativo automáticamente.
 - Para personal externo los datos se obtienen de su certificado digital mediante solicitud de auto-registro y es el responsable de cada unidad quien acepta (si procede) la solicitud, con lo que quien realmente conoce a la persona y su función es quien interactúa con el sistema. GUIA lanza la creación de credenciales en el directorio de correo (sin buzón).
- Traslado dentro de la organización: Se inicia como propuesta automáticamente a partir del sistema de RR.HH. (SIRhUS). Intervienen en el proceso los responsables de las unidades de la que sale la persona y a la que llega. El sistema permite reflejar las situaciones en las que se está trabajando “a caballo” en ambas unidades (hasta que la unidad de la que sale da su visto bueno). El sistema genera automáticamente las tareas de bajas de autorizaciones de acceso.
- Salida de la organización: El sistema lanza automáticamente la baja de los sistemas a los que está autorizado a acceder. Incluye un último paso manual para que un responsable técnico verifique que no se ha quedado ningún sistema pendiente (para sistemas no integrados). Finalmente se deshabilita la identidad, no borrándose por razones de históricos.
- Gestión de Autorizaciones: Este sistema es crítico y destacamos:
 - Delimitación de responsabilidades: Actualmente, muchos sistemas, se asume desde el área TIC la responsabilidad de autorizar el acceso, cuando es una función que corresponde al área funcional. GUIA aporta la herramienta y el procedimiento para que sea el competente quien autorice.
 - Traza, auditoría e histórico: Información actual e histórica de quién está autorizado a acceder a un sistema así como de a qué sistemas está autorizado a acceder una persona dada. Este último informe es un gran valor añadido ya que hoy sería prácticamente imposible obtenerlo.

	Resumen de Situación
	GUIA

- Cumplimiento de normativa: A través de la generación gestión del histórico de autorizaciones (quién solicitó, a qué sistema, con qué condiciones, quién autorizó, quién realizó la configuración para el acceso, etc.) y también a través de la asignación de los roles a las personas competentes.
- Caducidad de las autorizaciones: GUIA permite asignar caducidad a las autorizaciones. Llegada la fecha de caducidad y tras varios avisos, si no se renueva el acceso, GUIA tramita la baja. Esto permitiría eliminar las cuentas “huérfanas” existentes en la actualidad y que suponen un gran riesgo en cuanto a seguridad y confidencialidad.

2.2. Directorio Corporativo

GUIA ofrece un Directorio Centralizado con los datos (una vez incorporados, lógicamente) de las personas que usan los Sistemas de Información de la Junta de Andalucía.

Estos datos se pueden consumir y modificar por distintas herramientas (ver apartado sobre Integración más adelante).

El directorio está diseñado para ser robusto (alta disponibilidad) y escalable.


2.2.1. Estructura Funcional

El Directorio incorpora, como novedad respecto al resto de directorios existentes (listines telefónicos, directorio de correo, etc.) la **estructura organizativa a nivel funcional**, que no tiene por qué ser la estructura orgánica formal.

Es cada Organismo quien determina su estructura funcional. Normalmente se llega a nivel de Servicio, aunque en la CEICE se incluyeron unidades de trabajo existentes ajenas a SIRhUS, como una Oficina de Gestión Económica.

Cada identidad puede pertenecer a una unidad o más (préstamos temporales, trabajos horizontales en varios organismos o dentro de un organismo, etc.).

El hecho de que una persona (id1) pertenezca a una unidad (uo1) sólo significa que el responsable de la unidad uo1 es quien debe pedir autorización de acceso a sistemas de información para id1. Si id1 trabajase en ou1 y ou2, la persona responsable de cada unidad podrá pedir autorizaciones para que id1 use los sistemas de información que requiere para desempeñar sus funciones.

	Resumen de Situación
	GUIA

2.2.2. Repositorio Central de Datos de Usuario

Los datos incorporados a GUIA tienen garantizada la **calidad** por la fuente de los mismos (fuentes autoritativas) que son los sistemas de RR.HH. como SIRhUS y los certificados digitales (en el caso del personal externo).

El propósito es que todos los sistemas de información de la Junta de Andalucía consuman los datos personales de este directorio, resolviéndose definitivamente la problemática de nombres compuestos, apellidos, distintos teléfonos de contacto, distintos centros de trabajo, etc.

Disponer de todos los datos, con calidad, en un repositorio central, con una infraestructura común y compartida, permite abordar futuros proyectos de gestión de sedes, etc. en definitiva, aporta información transversal y permite aplicación directa y global de medidas y políticas de seguridad.

El sistema además permite la autenticación por cualquiera de los múltiples atributos únicos del directorio: uid de correo corporativo, DNI (de ser único), anagrama fiscal o cualquier otro atributo que se defina, como por ejemplo el usuario GIRO si así se decidiese.

Asimismo se convierte en una fuente de información estadística y de uso de sistemas.

El sistema incorpora información de género.


2.3. Integración

GUIA ofrece un catálogo documentado de servicios y mecanismos de integración, basado en protocolos estándares y aplicando medidas de seguridad.

- LDAPS: (LDAP Seguro). Adicionalmente, no se permiten consultas anónimas de datos del directorio.
- Servicios Web: Catálogo para consumir los datos del directorio y del propio modelo de datos de GUIA (sistemas integrados y roles asociados).
- API: Desarrollada por GUIA para facilitar la integración a sistemas, evitando las dependencias de versiones de componentes XML, etc.

Además se han desarrollado las **pautas** (publicadas en MADEJA) que permiten desarrollar la integración desde la perspectiva del sistema que desea integrarse.

Se ofrecen distintos entornos para que el sistema a integrar desarrolle sus componentes y realice pruebas, incluyéndose una

	Resumen de Situación
	GUIA

máquina virtual que cualquiera puede descargarse y desplegar en sus instalaciones que permite realizar todo el trabajo de desarrollo y prueba de integración.

2.3.1. Virtualización de directorios


GUIA ofrece la funcionalidad de virtualizar cualquier fuente de datos (Bases de datos, hojas de cálculo, etc.) e integrarlo de manera virtual con los datos del Directorio de GUIA. Esto permite que los distintos organismos y sistemas puedan incorporar datos que les son propios sin que realmente formen parte del directorio global.

Este sistema también permite adaptar distintos tipos de directorio, enmascarando la versión concreta y el fabricante (por ejemplo, permite ofrecer acceso a un OpenLDAP como si se tratase de un Active Directory). Esto se hace mediante un producto de Oracle llamado Oracle Virtual Directory.

2.3.2. Integraciones actuales

A día de hoy están construidas y operativas las siguientes integraciones:

- SIRhUS: Se obtienen los datos a partir de una vista que se actualiza cada día. Es la fuente de datos para el personal interno.
- @firma: Se emplea como mecanismo para la autenticación en el sistema (en la aplicación llamada “Aplicación de Gestión Operativa” que es la propia de GUIA). Permite cambiar la contraseña de usuario sin tener que recurrir a ningún tipo de soporte.
- Correo Corporativo:
 - Alta de usuario: Al realizarse un alta en GUIA se crea la cuenta del directorio de correo corporativo (incluyendo buzón sólo para personal interno).
 - Sincronización de contraseñas: Al cambiar la contraseña en GUIA se cambia también en Correo Corporativo. También funciona en sentido inverso.
 - Cambios de organismos: Al cambiarse una identidad de organismo en GUIA, se envía el cambio al directorio de correo corporativo (correo deja de hacer sus cambios automáticos cuando las identidades pasan a ser gestionadas por GUIA).

	Resumen de Situación
	GUIA

- NAOS: Se obtienen los datos a partir de GUIA
- AGATA: GUIA permite definir grupos. AGATA utiliza esta información de grupos.
- SSOWeb: Se trata en su apartado, más adelante.

Además de estos sistemas, se ha trabajado hasta varios niveles de detalle con otros sistemas como:

- Controlador de dominio (SAMBA+OpenLDAP): El sistema se integró con el Controlador de Dominio de la anterior CEIC. Se permite la creación, modificación y eliminación de usuarios del dominio (carpetas de red Windows) automáticamente desde GUIA.
- CRONO (control horario): Se detuvieron los trabajos al trasladarse el proyecto a la Consejería de Hacienda y Administración Pública.
- Séneca (Consejería de Educación): Acceso a datos propios del sistema a través del virtualizador de directorio.

2.3.3. Integraciones adicionales

El núcleo de GUIA es un producto de Oracle llamado Oracle Identity Manager (OIM en adelante), que incluye un sistema de Conectores para integrar sistemas propietarios, así como un conector genérico para posibilitar integraciones personalizadas.

Actualmente GUIA dispone de un conector que permite integrar un LDAP (se emplea para la integración con Correo Corporativo y para la integración del controlador de dominio de la anterior CEIC¹).

Este mismo conector se ha empleado en pruebas de laboratorio para integrar con Active Directory (sin sincronización de contraseñas).


Adicionalmente se dispone de un conector nativo para RAC-F (que no se está utilizando).

El catálogo de conectores de Oracle disponibles es muy amplio e incluye tanto SAP como Active Directory con la capacidad de sincronizar los datos y las contraseñas bidireccionalmente. Estos conectores tienen coste.

Active Directory de la CHAP

Actualmente en pruebas de laboratorio. Se está teniendo problemas para la configuración de la conexión y se está

1 Esta integración se quedó sin implantar en producción por el traslado de la dirección del proyecto GUIA a la Consejería de Hacienda y Administración Pública. No obstante se probó y recibió el visto bueno del organismo.

	Resumen de Situación
	GUIA

haciendo uso de la garantía del proveedor de GUIA (AYESA) para resolver los problemas y las dudas, todo esto a pesar de haber cumplido sobradamente el periodo de dicha garantía. En un escenario de mejora continua y evolución del proyecto se debería contemplar la adquisición del conector específico de OIM con Active Directory para permitir la réplica bidireccional de contraseñas, permitiéndose así integrar en el sistema otros dominios que están pendientes, como el del Sistema Andalúz de Salud.

SUR y DATAMART-SUR

Los trabajos para el análisis e integración de estos sistemas no se han iniciado. Están supeditados a los trabajos de evolución de la gestión de autorizaciones en GUIA (ver apartado propio más adelante)

GIRO

SAP se compone de varios módulos, cada uno de ellos con gestión de usuarios independiente. Este sistema se vería muy beneficiado con la integración con un Sistema de Gestión de Identidades (como prueba de esto, SAP ha construido uno y lo ofrece en su portafolio de soluciones).

Se plantean varios escenarios para la integración de GIRO con GUIA:

1. Gestión de autorizaciones de acceso

El alta final del usuario en GIRO se hace a mano. Esta integración aporta control del flujo de peticiones y autorizaciones.


Esta es la solución más viable para el arranque del proyecto GIRO y requiere del desarrollo evolutivo planteado en GUIA (véase más adelante en Mejoras Evolutivas).

2. Login único

Se integrarían los sistemas SAP en el servicio de Login Único vía web de GUIA. Esta opción permitiría resolver el problema del tamaño del identificador de usuario detectado en SAP, permitiendo además implementar un mecanismo de usuario y contraseña únicos.

Esta solución requiere de estudio de la arquitectura por parte de la UTE de GIRO. El nivel de conocimientos en esta materia del personal de la UTE supone un riesgo importante para la viabilidad de esta aproximación.

3. Aprovisionamiento

	Resumen de Situación
	GUIA

Los usuarios autorizados a través de GUIA se generan, modifican y cancelan en todo GIRO de manera automática de acuerdo con los flujos de gestión de la identidad digital implementados en GUIA.

Esta solución requiere de los desarrollos evolutivos descritos en el escenario 1 y de la adquisición del conector correspondiente entre OIM y SAP. Asimismo esta solución es compatible con el escenario 2.

Todos los escenarios de integración con GIRO están siendo objeto de estudio en estos momentos. Difícilmente se podrán abordar soluciones de integración con los plazos y recursos actuales, pero se pretende marcar el camino para lograr mejoras muy sensibles una vez el sistema esté operativo.

GERHONTE

Para la integración de las identidades del Servicio Andaluz de Salud es necesario contar con una fuente autoritativa de datos (una fuente de datos fiable y que garantiza tanto la calidad del dato como el disparo de los eventos de alta, baja, traslado, etc. desde la perspectiva de RR.HH.).

Esta integración se plantea de forma análoga a como se ha realizado la de SIRhUS, siendo necesario sólo el acceso a una vista de datos diaria que GUIA procesaría e interpretaría.

2.4. Acceso al puesto


Se engloba en este grupo de funcionalidad la de Acceso al puesto con tarjeta y la de login único tanto de escritorio como vía web.

2.4.1. Login con tarjeta

Se dispone de dos productos diferenciados para el login al sistema operativo mediante tarjeta:

IdOne: Producto para ordenadores Windows que permite utilizar una tarjeta para identificar a la persona usuaria del ordenador. Este sistema permite solicitar un pin de desbloqueo como medida adicional de seguridad.

Las licencias de este producto se contratan anualmente y de forma diferenciada a las del resto de productos de GUIA. Se abandonó su renovación al cesar la financiación del proyecto. Este producto requiere de un servicio de Active Directory (o un módulo adicional sobre Samba+OpenLDAP, por lo que siempre hará uso de licencia CAL de Windows, lo que no supone un problema para organismos con Active Directory, como nuestra Consejería).

	Resumen de Situación
	GUIA

PasswordBank¹: Producto para ordenadores Linux que permite tanto el login con tarjeta como el Single Sign-On de escritorio (descrito más adelante). Este sistema fue proporcionado por Oracle como medio alternativo para cumplir su compromiso de uso de su propia herramienta para S.O. Linux.

2.4.2. Single Sign-On de escritorio

Esta funcionalidad se logra con un agente (un programa) que se instala en cada PC y que es capaz de reconocer las ventanas de las distintas aplicaciones, introduciendo automáticamente el identificador y la contraseña de la persona usuaria. No es por tanto un sistema de usuario único, realmente evita tener que recordar los distintos nombres de usuarios de los distintos sistemas (y sus respectivas contraseñas) así como el tener que introducirlas al abrir la aplicación.

De nuevo nos encontramos dos soluciones diferenciadas para Windows y para Linux.

Oracle Enterprise Single Sign-On: para Windows. Disponemos de licencias perpetuas e ilimitadas.

PasswordBank²: para Linux. Disponemos del mismo número de licencias ya que se deriva del compromiso adquirido por Oracle de que su sistema funcionaría en Linux y, ante la imposibilidad de tal extremo, localizó y ofreció esta solución.

2.4.3. Single Sign-On vía web


Sistema basado en estándares (SAMLv2) que permite el login único en las aplicaciones web, independientemente de la tecnología con la que estén construidas.

El sistema proporciona el código para las aplicaciones Java o Php (la mayoría de sistemas ya vienen con la opción preparada y no requieren de este software). Este código reemplaza la pantalla de entrada a la aplicación, accediendo la persona siempre al sistema de login único.

El sistema de login único emite tokens seguros firmados digitalmente que la aplicación recibe y de los que obtiene los datos de identificación de la persona que ha entrado al sistema. Los datos que se incluyen en el token se han acordado entre el sistema de login único y la aplicación durante el proceso de integración y pueden ser diferentes a los usado por la persona que entra al sistema. Por ejemplo, se puede acceder al Single Sign-On mediante certificado digital o mediante usuario de

1 El pasado año Symantec adquirió el sistema de Single Sign-on de la empresa PasswordBank

2 Ver nota 1.

	Resumen de Situación
	GUIA

correo y contraseña, y la aplicación puede recibir el anagrama fiscal o el nif junto a nombre y apellidos, etc.

Actualmente están integrados en el sistema de login único vía web de GUIA: Red Profesional, redmine (herramienta de gestión de proyectos) y el Catálogo de Servicios Web de PLATINA. Además se está finalizando la integración de la herramienta de reserva de salas de la Consejería de Justicia e Interior.

También se han hecho pruebas satisfactorias con sistemas de portal Moodle.

El Correo Corporativo se encuentra en fase de integración (es un escenario más complejo puesto que no se trata de una aplicación web, sino que además incluye varios servicios como son POP, SMTP, IMAP, etc.).

GIRO

SAP soporta el estándar SAMLv2 como mecanismo de Single Sign-on vía web para todos sus sistemas en Java. Esto abre la opción (en estudio por la UTE del proyecto) de autenticar a las personas usuarias contra el sistema de Single Sign-on de GUIA, que generaría un token SAMLv2 que incluiría el identificador de usuario SAP (que por las limitaciones descubiertas actualmente no puede ser el mismo que el del correo corporativo salvo que se actualicen las versiones de SAP instaladas). El token SAMLv2 llegaría a un servidor de aplicaciones Java de SAP (actualmente tenemos esos sistemas disponibles en SAP-PI y en SAP Portal, habría que estudiar la viabilidad de emplearlos), que generarían un token propio de SAP llamado “SAP Logon Token” que es interpretado y aceptado por el ERP.

Tras la reunión mantenida con SAP (02/04/2014) se ha detectado que las nuevas versiones de los productos SAP podrían incluso realizar ellos internamente el mapeo entre el usuario de GUIA (Correo Corporativo) y el usuario SAP.


3. MEJORAS EVOLUTIVAS

3.1. Evolución de la gestión de autorizaciones de acceso

Actualmente GUIA cubre prácticamente toda la funcionalidad para la gestión del ciclo de vida de la identidad.

El mecanismo implementado para la gestión de la autorización es básico y, si bien cubre los requisitos elementales, no resulta usable en un entorno de alto número de usuarios, alto número de perfiles, aplicaciones, etc.

El flujo implementado es el siguiente:

	Resumen de Situación
	GUIA

1. La persona responsable de unidad elige un sistema de información (entre todos los horizontales visibles para toda la Junta de Andalucía y los verticales, exclusivos de su organismo). Además elige una persona que trabaja en su unidad.
2. Una vez identificado el sistema y la persona elige qué quiere pedir, si un alta o una baja de permisos. En este punto se incluye la fecha de caducidad del acceso que se solicita y se aportan la documentación y las observaciones oportunas (texto libre y opcional).
3. La petición le llega como un tique pendiente a la persona responsable de autorizar los accesos al sistema de información solicitado, que puede aprobarla o no. Esta opción es posible realizarla en el sistema **Portafirmas**.
4. Si se ha aprobado la petición llega al técnico que tiene que verificar que la petición es correcta (GUIA realiza la verificación en este punto, en la versión actual no es posible hacerlo a la hora de la solicitud). Después procede a configurar el acceso propiamente dicho sobre el sistema correspondiente y finaliza el flujo de trabajo.


Este sistema es poco usable por no aplicar filtros en el momento de la petición, por no permitir seleccionar más de un sistema sobre el que pedir acceso, por no poder pedir acceso a subsistemas, etc.

Este evolutivo **no** se considera imprescindible para el arranque del sistema GIRO, pero sí es muy importante incorporarlo lo antes posible para la gestión correcta de las autorizaciones. Siendo necesario para reemplazar el sistema de gestión actualmente implementado en Natural y que se espera que dejará de estar operativo en el primer semestre de 2.015. Este sistema gestiona los usuarios de:

- Carpetas de Red de la Consejería de Hacienda y Administración Pública (y otros sistemas integrados con Active Directory, como Alfresco).
- SUR
- Datamart SUR

Este evolutivo se encuadraría en una línea de mejora para ambos sistemas (GIRO y GUIA) que añade funcionalidad completa en cada iteración, con objetivos concretos y en plazos razonables.

Las tareas mínimas imprescindibles para abordar este evolutivo han sido estimadas en aproximadamente **310.000€**

	Resumen de Situación
	GUIA

3.2. Conectores adicionales

Para la integración plenamente operativa con SAP y con Active Directory se propone la adquisición de los conectores propios de OIM con dichos sistemas.

Se debe pedir **presupuesto** al proveedor (Oracle).

Como referencia, en el año 2006, y en el marco de la contratación del proyecto GUIA, cada conector tuvo un coste de 312,74€. Esta cantidad obviamente no refleja el precio de mercado, por lo que se debe pedir presupuesto.

3.3. Evolución de la plataforma de base

El software de base de GUIA, productos del fabricante Oracle, lleva instalado y ejecutándose de forma estable desde la entrada en producción del sistema en enero de 2011.

En este tiempo el fabricante ha evolucionado su solución de gestión de identidades, quedándose obsoletas las versiones desplegadas en la Junta de Andalucía, por lo que es conveniente actualizarlas para que la solución sea soportada.

La actualización de la pila de productos Oracle de GUIA estaba planificada para haberse acometido en 2012 pero se abandonaron los trabajos, que incluyen desde el Sistema Operativo de los servidores hasta los productos de gestión de identidades (OIM, OID y OVD).

Los trabajos de migración propiamente dicho se realizarían desde el área de producción del proyecto (Servicio de Sistemas Corporativos II).


Adicionalmente, para la migración se requiere de soporte por parte del fabricante (Oracle), que está disponible a través del Contrato de Soporte Corporativo, y también por parte del equipo de desarrollo de GUIA para la adaptación a la nueva versión de todas las integraciones con OIM.

Este proyecto se propone como a realizar a medio plazo y habiendo licitado el **soporte** de GUIA, incluyéndolo como parte de los trabajos a realizar.

3.4. Otras líneas de evolución

Desde su implantación en la antigua Consejería de Economía, Innovación y Ciencia, el proyecto ha recibido propuestas de mejoras y se han detectado fallos.

Las principales líneas de trabajo que no deben abandonarse son:

	<p style="text-align: center;">Resumen de Situación</p>
	<p style="text-align: center;">GUIA</p>

Habilitación de funcionalidad de administración delegada: A día de hoy una delegación provincial o territorial debe tratarse o bien como un organismo independiente o gestionarse de forma integrada y no diferenciada dentro del organismo.

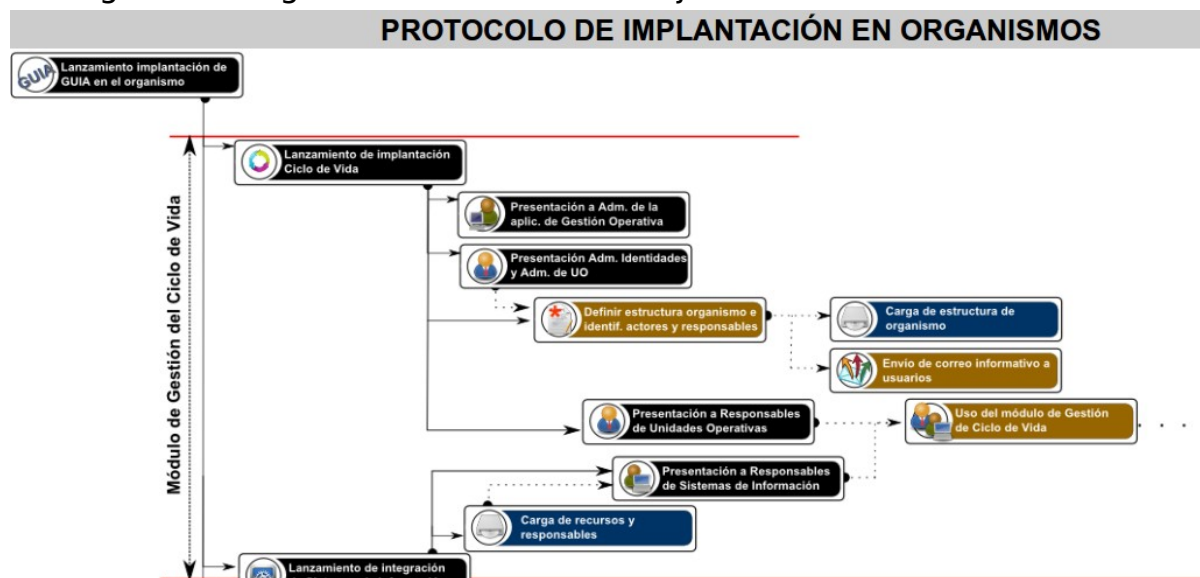
Desacople entre el sistema de tramitación (NAOS-GUIA) y la Aplicación de Gestión Operativa (ver más adelante)

4. TAREAS OPERATIVAS PARA SU PUESTA EN MARCHA Y MANTENIMIENTO

Para la puesta en marcha de GUIA, el primer paso es el “**Poblado del Directorio Corporativo**”, que es un procedimiento prediseñado del que contamos con manuales, presentaciones, material de formación, etc. para su ejecución. Se ha diseñado en base a los trabajos de las dos implantaciones incrementales realizadas en la anterior Secretaría General de Telecomunicaciones y Sociedad de la Información.

El procedimiento se ha utilizado con éxito durante la implantación de GUIA en los Servicios Centrales de la anterior Consejería de Economía, Innovación y Ciencia.

El siguiente diagrama muestra los trabajos a realizar:




A grandes rasgos el procedimiento adaptado a nuestra Consejería es el siguiente:

1. Presentación del sistema a la Secretaría General Técnica y el Servicio de Personal

Presentación de alto nivel a realizar preferentemente por el Director General o la Coordinadora.

De esta presentación se obtienen los interlocutores para el resto de trabajos y se fija el alcance de la implantación, obteniéndose

	Resumen de Situación
	GUIA

el compromiso de proporcionar al proyecto la estructura de Unidades Organizativas y la persona responsable de cada una de ellas.

Se identifica a las personas que realizarán la administración de identidades (Servicio de Personal).

Se entregan formularios de recogida de información de estructura y responsables para su remisión al proyecto.

2. Presentación al Servicio de Personal de la Aplicación de Gestión Operativa

Se describe la funcionalidad asociada a los roles de Administración de Identidades y Administración de Unidades Organizativas.

Se entrega material de formación y guías de uso. Se realizan casos prácticos.

3. Carga de la estructura definida por la S.G.T.

Desde el proyecto realizamos la carga de la estructura de la Consejería asignando la jefatura de las mismas según la información recibida de la S.G.T.

Temporalmente se añade como autorizado un usuario propio del proyecto para realizar las tareas hasta que se gane la plena autonomía por parte de las personas responsables.

4. Presentación a las personas responsables de unidad (jefatura de servicio)

Se describe la funcionalidad asociada al rol Responsable de Unidad Operativa.

Se entrega material de formación y guías de uso. Se realizan casos prácticos.

Se informa de la posibilidad de designar personas autorizadas y se solicita su designación para cada unidad.

Se mantienen varias sesiones para facilitar la asistencia.


5. Formación a la persona responsable técnico del organismo

Se describe la funcionalidad asociada al rol Responsable técnico del organismo. Se trata de un rol técnico TIC de producción.

Se entrega material de formación y guías de uso. Se realizan casos prácticos.

Se informa de la posibilidad de designar personas autorizadas.

6. Asignación de personas a unidades

	Resumen de Situación
	GUIA

Acompañados por una persona del proyecto, el Servicio de Personal ubica a cada identidad en la unidad que le corresponde dentro del organigrama operativo de la Consejería.

Con esto se implanta la gestión del ciclo de vida de la Identidad. Para incorporar la funcionalidad de gestión de autorizaciones de acceso a sistemas se forma a los responsable funcionales de cada sistema y se notifica a los responsables de unidad que se comienza a utilizar esta funcionalidad.

4.1. Incorporación del resto de organismos

Para la carga del resto de organismos de la Junta de Andalucía y sus entidades instrumentales se distinguen dos casos principales:

- Implantación mínima
- Implantación completa

El paso desde el primer caso al segundo es abordable de forma gradual y planificada, aportando beneficio en cada iteración que se realice.


Implantación mínima

El procedimiento de carga completa de SIRhUS en GUIA se diseñó con las siguiente premisa: Se define una única Unidad Organizativa donde se incluirían todas las identidades del organismo, que provendrían de la fuente autoritativa identificada (SIRhUS). En esta situación todos los roles de la Gestión de Identidades se asumen desde la Dirección General de Política Digital.

Para su integración en GIRO, el enfoque se concretaría más:

1. Creación de una UO por cada persona Responsable de Usuarios en el organismo a incorporar
2. Asignación a la persona Responsable de Usuario del rol "Responsable de UO". Se acompaña de formación.
3. Asignación de las personas que usan GIRO a la UO correspondiente.
4. Configuración de los recursos que pueden solicitarse desde el organismo (áreas o subsistemas de GIRO que pueden solicitar).

Con esto se consigue directamente replicar el esquema de solicitudes actual, con la diferencia de que autorizaría otro rol, idealmente la persona competente (es un rol asignable a la misma persona). Garantizamos un impacto mínimo en la operativa.

	Resumen de Situación
	GUIA

El resto de roles necesarios para la gestión se asume desde la Dirección General de Política Digital (incluye la asignación de personas a UO).

Implantación completa

Se realiza siguiendo el procedimiento descrito para nuestra Consejería.

En caso de organismos con estructura y funcionamiento distinto a una Consejería hay que realizar con antelación la identificación de áreas responsables y su correspondencia a las definidas en el procedimiento.

Situaciones intermedias

Desde la implantación mínima a la implantación completa se puede pasar por cualquier estado intermedio.

El primer paso para avanzar desde el estado inicial será la transferencia al organismo de los roles de administración de identidades, administración de unidades y responsable técnico. Para esto se requerirá la formación correspondiente, a impartir por la Dirección General de Política Digital.

A partir de ese primer paso, el organismo podrá ir incorporando las unidades de forma autónoma o coordinada con la Dirección General de Política Digital, en cuyo caso se colaboraría en la difusión y formación a los distintos actores.


4.2. Carga de personas externas

Para la incorporación de personas externas se ha diseñado un procedimiento de autorregistro mediante el que, con su certificado digital (lo que garantiza la calidad del dato y la presencia física de la persona en cuestión) accede a GUIA solicitando su incorporación a una unidad organizativa determinada. Esto genera una petición que, en caso de ser aprobada por el responsable de la unidad en la que la persona ha solicitado su inclusión, resultará con la incorporación de la identidad al Directorio Corporativo, es decir, hasta el una jefatura de servicio no lo acepta, no se incorpora una persona externa al sistema.

Normalmente este proceso se lanza tras la carga de todo el personal interno.

4.3. Administración funcional

La administración funcional del Sistema GUIA la realiza el Servicio de Sistemas Corporativos II con el apoyo de la Dirección del Proyecto GUIA y la Oficina Técnica de proyectos.

	Resumen de Situación
	GUIA

A día de hoy las peticiones e incidencias se gestionan mediante NAOS. Habría que trasladar estas funciones al CEIS.

La coherencia de los datos, salvo cuando surge algún problema puntual, se mantiene desde la propia herramienta, es decir, el Servicio de Personal y las jefaturas de Servicio mantienen los datos al día. En el momento en que se comienza a utilizar la herramienta también para mantener los permisos de acceso a sistemas, esta afirmación cobra más peso por los propios procesos de solicitud y autorización.

Desempeño de roles por la Dirección General de Política Digital

La gestión del sistema GUIA, como se ha dicho, está diseñada para que los propios organismos y personas que tienen asignados los roles del sistema mantengan los datos actualizados por la propia necesidad del funcionamiento y acceso a los sistemas integrados.

No obstante en el escenario de integración no total de un organismo, la Dirección General de Política Digital debe asumir los roles de Administración de identidades, de unidades organizativas, de recursos, etc.

Asimismo, durante el periodo de aprendizaje de uso de la herramienta por parte de nuestra propia Consejería, también se debe asumir por parte de la Dirección General la función de autorizados en todos los roles del sistema para acompañar e impulsar la tramitación de las peticiones.

En todo caso, la resolución de dudas, incidencias, etc. requerirá de seguimiento igualmente.

Estos roles los está desempeñando en la actualidad Jesús Villegas.


Los trabajos aquí descritos se podrían englobar dentro de la función de “Administración de Sistemas Corporativos de la Dirección General de Política Digital”, de manera análoga a la realizada por el Servicio de Administración SIRhUS en su sistema.

5. DEPENDENCIAS CON OTROS SISTEMAS (NAOS)

Para su funcionamiento, GUIA depende a día de hoy de varios sistemas como SIRhUS o el Correo Corporativo.

Además de estos sistemas externos, GUIA integra diversas herramientas para la gestión del ciclo de vida de la identidad:

- Aportadas por proveedores externos
 - Oracle Identity Manager

	Resumen de Situación
	GUIA

- Oracle Internet Directory
- Oracle Virtual Directory
- Adoptada de soluciones propias de la Junta de Andalucía:
 - NAOS

En cualquier caso, todas estas herramientas deben verse como parte de GUIA, no como productos diferenciados. Esta afirmación también es cierta para NAOS, ya que se usa una instancia independiente y de uso exclusivo para el proyecto GUIA. Esta instancia se llama NAOS-GUIA.

NAOS-GUIA es una instancia de NAOS en versión 2.4 sobre la que se han realizado trabajos de integración mediante el sistema de “Clases Externas” de NAOS.

Actualmente el nivel de acoplamiento entre la Aplicación de Gestión Operativa (GUIA) y NAOS-GUIA es alta e imposibilitan la sustitución de NAOS-GUIA como tramitador.

Se ha realizado el trabajo de análisis para el desacople entre NAOS-GUIA y el resto del sistema GUIA, pero no se ha abordado por falta de financiación. El objetivo que nos planteamos desde el proyecto era la aplicación de los conceptos de encapsulación y desacople que permitieran la eventual sustitución de NAOS como tramitador por otro propio de cada organismo o global a toda la junta.