GUIA

Gestión de Identidades en la Junta de Andalucía

Situación del proyecto
abril de 2.014

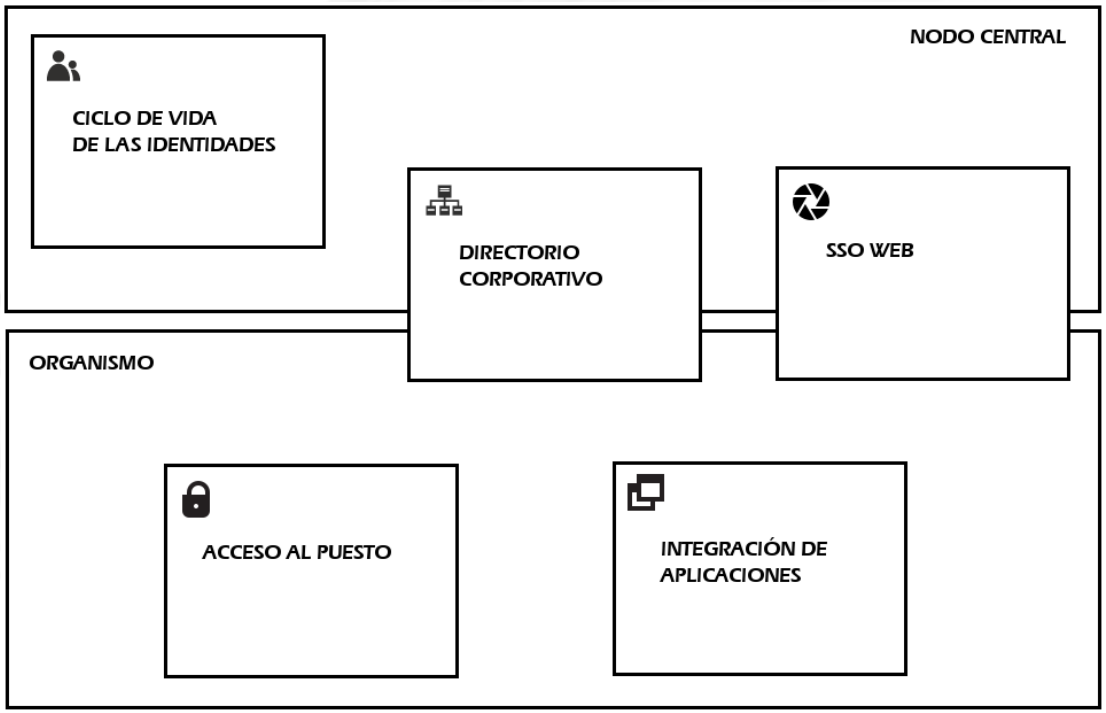
JUNTA DE ANDALUCIA

Índice

- **Funcionalidad**
  - Ciclo de vida de la identidad
  - Directorio Corporativo
  - Integración
  - Acceso al puesto
- Mejoras evolutivas
  - Evolución de la gestión de autorizaciones de acceso
  - Conectores adicionales
  - Evolución de la plataforma base
  - Otras líneas de evolución
- Tareas operativas para puesta en marcha/mantenimiento
  - Incorporación del resto de organismos
  - Carga de personas externas
  - Administración funcional
- Dependencia con otros sistemas (NAOS)

Funcionalidad

- GUIA es un sistema muy complejo que se estructura en cuatro áreas funcionales
  - Gestión del Ciclo de Vida de la Identidad
  - Directorio Corporativo
  - Integración
  - Acceso al puesto



JUNTA DE ANDALUCIA

Funcionalidad – Ciclo de vida de la identidad

- Áreas usuarias:
  - Personal/RR.HH.
  - Responsables de Unidades (Jefaturas de servicio)
  - Cada persona usuaria final
- Eventos del Ciclo de Vida:
  - Alta
    - Internos
    - Externos
  - Traslados
  - Bajas
  - Gestión de **Autorizaciones**
- Gestión de Autorizaciones:
  - Delimitación de responsabilidades
  - Traza, auditoría e histórico
  - Cumplimiento de normativa: LOPD
  - Caducidad de autorizaciones: Anulación de cuentas

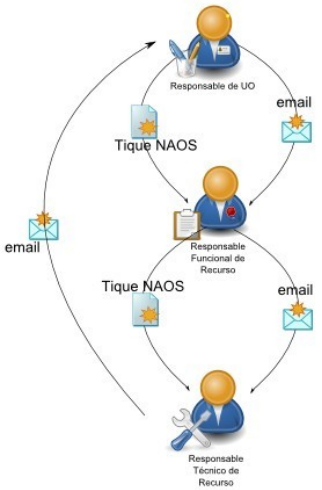
JUNTA DE ANDALUCIA

Funcionalidad – Ciclo de vida de la identidad

TRASLADO DE IDENTIDAD INTERNA ENTRE UO DE DISTINTO ORGANISMO

1. El **Administrador de Identidades** solicita el traslado
2. El **Responsable de UO DESTINO** es notificado mediante correo electrónico y a través de un tique NAOS
3. El **Responsable** puede aprobar o denegar la solicitud
4. Si el **Responsable de UO DESTINO** aprueba la solicitud el **Responsable UO ORIGEN** es notificado mediante correo electrónico y tique NAOS
5. El **Responsable UO ORIGEN** puede aprobar o denegar la solicitud
6. Si el **Responsable de UO ORIGEN** aprueba la solicitud el **Responsable Técnico** es notificado mediante correo electrónico y tique NAOS
7. El **Responsable Técnico,** notifica que ha desasignado los recursos a la identidad

GESTIÓN DE ASIGNACIÓN DE RECURSOS



1. El Responsable de UO solicita una operación de gestión de asignación de recurso sobre una identidad
2. El Responsable Funcional del Recurso es notificado mediante correo electrónico y tique NAOS
3. El Responsable Funcional del Recurso puede aprobar o denegar la solicitud
4. Si el Responsable Funcional del Recurso aprueba la solicitud, el Responsable Técnico del Recurso es notificado mediente correo electrónico y tique NAOS
5. El Responsable Técnico del Recurso puede aprobar o denegar la solicitud
6. El Responsable de UO es notificado del resultado del trámite que inició

JUNTA DE ANDALUCIA

Funcionalidad – Directorio Corporativo

- Directorio centralizado:
  - Diseñado para ser consumido por el resto de sistemas de información de la Junta de Andalucía
  - Robusto y seguro
  - Garantía de calidad en el dato (SIRhUS y Certificados digitales)
- Refleja la estructura organizativa a nivel funcional del organismo (distinta a la orgánica formal)
- Fuente de información estadística y de uso real de los sistemas: Dimensionamiento
- Incorpora información de género

JUNTA DE ANDALUCIA

Funcionalidad – Integración (1 de 3)

- Catálogo de servicios basados en estándares seguros
  - LDAPS (LDAP Seguro)
  - Servicios Web
  - API
- Pautas para la integración publicadas en MADEJA
- Varios entornos disponibles para todo el ciclo de vida del desarrollo de la integración
- Funcionalidad de virtual de directorio:
  - Oracle Virtual Directory (OVD)
  - Mostrar como propios datos de terceras fuentes
  - Enmascarar OpenLDAP – Active Directory

Funcionalidad – Integración (2 de 3)

- Ya implementadas:
  - SIRhUS: Fuente autoritativa de datos para personal interno.
  - @firma: Autenticación y cambio de contraseñas
  - Correo corporativo:
    - Alta de usuario desde GUIA (generación de uid por correo corporativo)
    - Sincronización bidireccional de contraseñas
    - Movimiento de cuentas entre organismos controlado por GUIA
  - NAOS: Datos de las identidades
  - AGATA: Gestión de grupos
  - SSOWeb
- Probadas
  - Controlador de dominio
    - Samba + OpenLDAP
    - Active Directory (sólo como prueba de concepto)
  - Acceso a datos de Séneca (Educación) mediante LDAP a través de virtualización de directorio con OVD
- Iniciadas (estado desconocido por el proyecto)
  - CRONO (Control horario)

Funcionalidad – Integración (3 de 3)

- Oracle Identity Manager (OIM) como núcleo de GUIA
  - Dispone de conectores nativos para sistemas específicos: SAP, Active Directory, RAC-F, ..
  - Dispone de conector genérico que permite hacer conectores a medida
  - Conectores sujetos a licencia
  - GUIA dispone de conectores para: Base de datos, RAC-F (sin usar) y LDAP (adaptado también para Active Directory)
- Otras integraciones a abordar
  - Active Directory de la CHAP: realizándose pruebas. Se requiere soporte para GUIA
  - SUR y Datamart SUR
  - GIRO: Múltiples limitaciones y decisiones de diseño hacen recomendable integrar la gestión de identidades con GIRO
    - Identificados varios escenarios posibles
      - Gestión de autorizaciones de acceso: Automatismo de la tramitación con alta final en SAP a mano
      - Login único: Buscando además resolver la limitación del tamaño del nombre de usuario
      - Aprovisionamiento: Requiere conector y es compatible con los dos anteriores. Es la evolución natural del sistema
    - Riesgos importantes:
      - Inexperiencia por parte del personal de la UTE de GIRO
      - Plazos: Son decisiones de arquitectura y diseño y ya se está en fases avanzadas.
  - GREHONTE: De forma muy similar a SIRhUS como fuente autoritativa de datos de RR.HH.

Funcionalidad – Acceso al puesto

- Login con tarjeta: opción de requerir PIN
  - IdOne para ordenadores Windows (requiere licencia adicional)
  - PasswordBank para ordenadores Linux
- Single Sign-on de escritorio: introduce las credenciales en las ventanas de login automáticamente
  - Oracle Enterprise Single Sign-on para windows
  - PasswordBank para linux
- Single Sign-on vía web: Basado en estándar SAMLv2
  - Se integra con el login de las aplicaciones
  - Las aplicaciones requieren sencilla adaptación
  - Escenarios de federación de identidades aportando seguridad
  - Integrados: Red profesional, Reserva de salas, Moodle, Redmine, Catálogo de Platina. Correo Corporativo está en proceso.
  - Opción en estudio para GIRO (SAP soporta SAMLv2)

Índice

- Funcionalidad
  - Ciclo de vida de la identidad
  - Directorio Corporativo
  - Integración
  - Acceso al puesto
- **Mejoras evolutivas**
  - Evolución de la gestión de autorizaciones de acceso
  - Conectores adicionales
  - Evolución de la plataforma base
  - Otras líneas de evolución
- Tareas operativas para puesta en marcha/mantenimiento
  - Incorporación del resto de organismos
  - Carga de personas externas
  - Administración funcional
- Dependencia con otros sistemas (NAOS)

Mejoras evolutivas

- Conectores adicionales
  - SAP para GIRO
  - Active Directory en entorno multidominio para la Consejería, el SAS y otros organismos
  - Se debe pedir presupuesto a Oracle
    - Expediente GUIA (2006) 312,74€ cada conector
- Evolución de plataforma de base
  - Productos instalados desde 2.011 que requieren actualización para seguir soportados
  - Requiere soporte de sistemas, de Oracle y del proveedor de GUIA
- Otras líneas de evolución
  - Administración delegada para Delegaciones Provinciales y Territoriales
  - Desacople entre el sistema de tramitación (NAOS-GUIA) y el aplicativo de GUIA (Aplicación de Gestión Operativa)

JUNTA DE ANDALUCIA

Mejoras evolutivas – Plataforma base

- Se requiere para poder sustituir al actual sistema de Júpiter:
  - GIRO
  - SUR
  - Datamart Sur
  - Carpetas de red de la Consejería (Active Directory)
- El flujo actual es muy sencillo y limitado
- No es imprescindible para la entrada en producción de GIRO
- Estimación aprox. 310.000 €

JUNTA DE ANDALUCIA

Índice

- Funcionalidad
  - Ciclo de vida de la identidad
  - Directorio Corporativo
  - Integración
  - Acceso al puesto
- Mejoras evolutivas
  - Evolución de la gestión de autorizaciones de acceso
  - Conectores adicionales
  - Evolución de la plataforma base
  - Otras líneas de evolución
- **Tareas operativas para puesta en marcha/mantenimiento**
  - Incorporación del resto de organismos
  - Carga de personas externas
  - Administración funcional
- Dependencia con otros sistemas (NAOS)

JUNTA DE ANDALUCIA

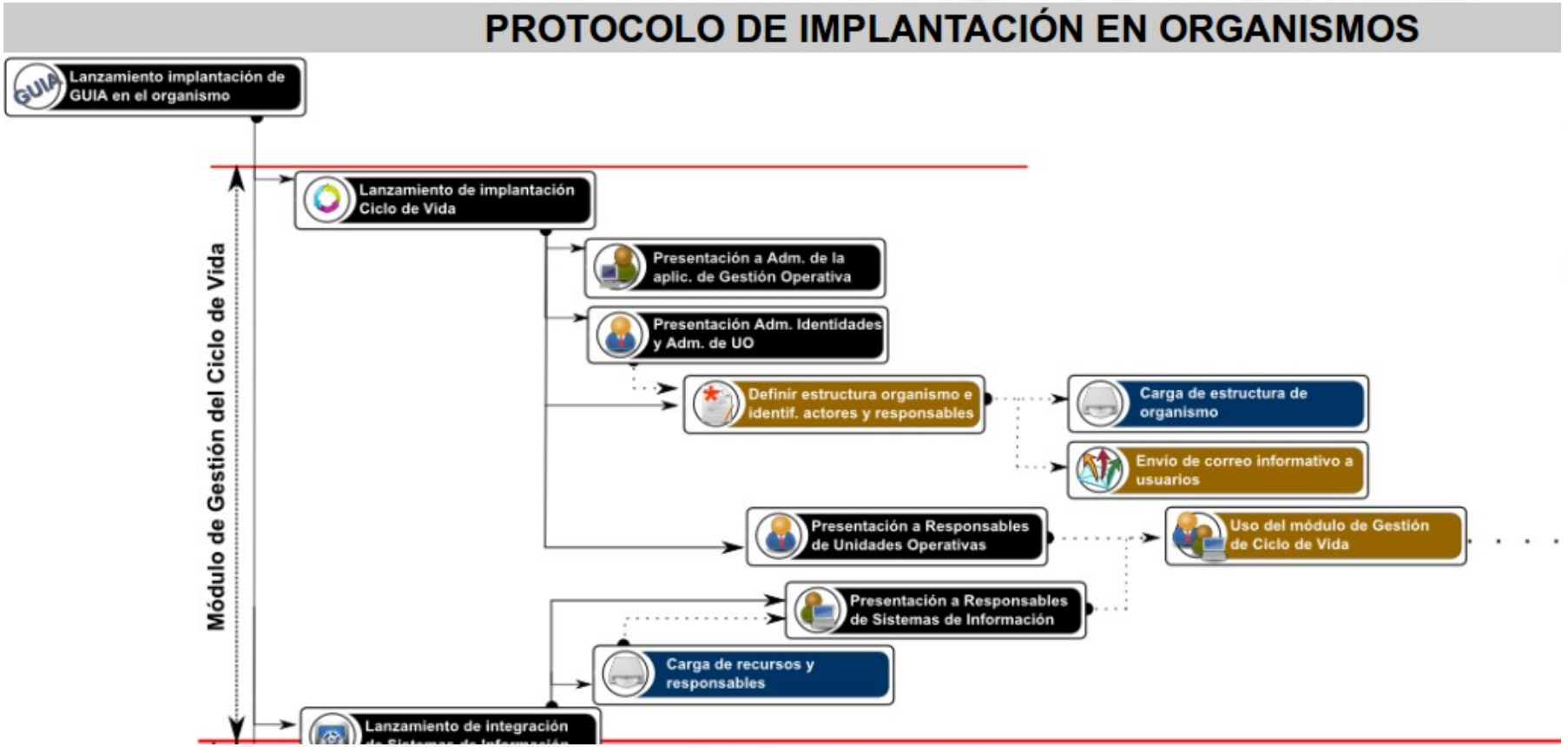
Tareas operativas para puesta en marcha/mantenimiento

- Carga completa
  - Disponible procedimiento, manuales, material para formación, etc.
  - Poblado del directorio
    1. Presentación del sistema a la Secretaría General Técnica y el Servicio de Personal
    2. Presentación al Servicio de Personal de la Aplicación de Gestión Operativa
    3. Carga de la estructura definida por la S.G.T.
    4. Presentación a las personas responsables de unidad (jefatura de servicio)
    5. Formación a la persona responsable técnico del organismo
    6. Asignación de personas a unidades

- Carga mínima:
  - Creación de una UO por cada responsable de usuarios actual en el organismo
    - Asignación del rol de administrador de UO a esa persona
    - Asignación a su UO de las identidades a las que deba gestionar acceso a GIRO
  - Requiere que la DGPD desempeñe el resto de roles
- Transición desde carga mínima a carga completa
  - De forma gradual
  - Comienza con la transferencia de los roles de administración de identidades, de unidades y responsable técnico
  - De forma autónoma por el organismo, con apoyo en seguimiento y formación por parte de la DGPD

JUNTA DE ANDALUCIA

Tareas operativas para puesta en marcha/mantenimiento



JUNTA DE ANDALUCIA

Tareas operativas para puesta en marcha/mantenimiento

- Gestión de autorizaciones de acceso
  - Implantado a posteriori gradualmente
- Incorporación de personas externas
  - Solicitud de autorregistro con certificado digital
  - Responsable de UO acepta/rechaza la solicitud

- Administración funcional
  - Durante fase de carga mínima: Completa
  - Posteriormente: Como acompañamiento
    - Soporte y asesoramiento
  - Englobada en la "**Administración de Sistemas Corporativos de la Dirección General de Política Digital**" de manera análoga a la función realizada por el **Servicio de Administración SIRhUS**

JUNTA DE ANDALUCIA

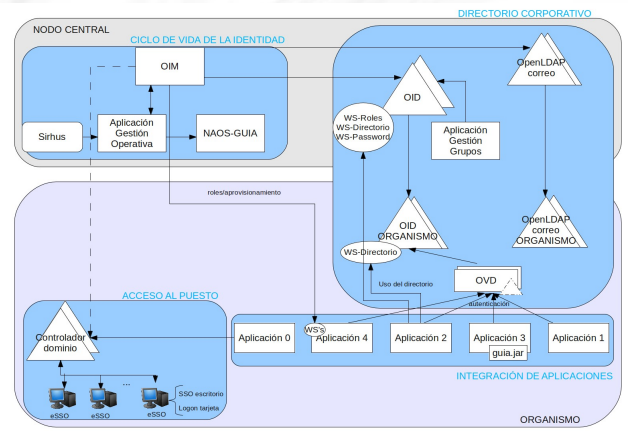
Índice

- Funcionalidad
  - Ciclo de vida de la identidad
  - Directorio Corporativo
  - Integración
  - Acceso al puesto
- Mejoras evolutivas
  - Evolución de la gestión de autorizaciones de acceso
  - Conectores adicionales
  - Evolución de la plataforma base
  - Otras líneas de evolución
- Tareas operativas para puesta en marcha/mantenimiento
  - Incorporación del resto de organismos
  - Carga de personas externas
  - Administración funcional
- **Dependencia con otros sistemas (NAOS)**

JUNTA DE ANDALUCIA

Dependencia con otros sistemas (NAOS)

- GUIA se compone de múltiples sistemas:
  - No es un conjunto de herramientas
  - Todas son GUIA
- Dependencia de proveedores externos
  - Oracle
    - Oracle Identity Manager
    - Oracle Internet Directory
    - Oracle Virtual Directory
- Dependencia de sistemas propios de la Junta de Andalucía
  - NAOS
    - Es el tramitador de flujos de ciclo de vida de identidad, incluido autorizaciones de acceso
    - Es una instancia de NAOS 2.4 diferenciada del resto
    - NAOS-GUIA
    - Identificada la necesidad de desacople: Objetivo posible sustitución por herramienta de cada organismo
      - Realizado el análisis (trabajos detenidos)



Dependencia con otros sistemas (NAOS)

- Licencias disponibles

Producto	Modalidad	Proveedor
Directory Services	Ciudadano Perpetua	Oracle
Identity Federation	Ciudadano Perpetua	Oracle
Identity Manager	Ciudadano Perpetua	Oracle
Identity Manager Connector – Database Applications Table	Ciudadano Perpetua	Oracle
Identity Manager Connector - Database User Management	Ciudadano Perpetua	Oracle
Identity Manager Connector - IBM RACF	Ciudadano Perpetua	Oracle
Oracle Enterprise Single Sign-On Suite	Ciudadano Perpetua	Oracle
idOne	Por puestos	SmartAccess

JUNTA DE ANDALUCIA


JUNTA DE ANDALUCIA