



GU

# Guía de estándares y procedimientos de desarrollo y adquisición de aplicaciones en la Amtega

Elaborado por Arquitecturas Tecnológicas



XUNTA  
DE GALICIA





CONTROL DE VERSIONES Y DISTRIBUCIÓN			
<b>NOMBRE DO DOCUMENTO:</b>	<b>Guía de estándares de desarrollo y procedimientos de desarrollo y adquisición de aplicaciones en la Amtega</b>	<b>VERSIÓN:</b>	01.02
<b>COD. DEL DOCUMENTO:</b>	AMTEGA_GU_estandaresProcedimientosDesarrolloAdquisicion_v.01.02_es		
<b>ELABORADO POR:</b>	Arquitecturas Tecnolóxicas	<b>FECHA:</b>	09/08/2018
<b>VALIDADO POR:</b>	Departamento de Seguridade e Calidade	<b>FECHA:</b>	04/09/2018
<b>APROBADO POR:</b>	Comité de Dirección Amtega	<b>FECHA:</b>	19/12/2018

REGISTRO DE CAMBIOS		
Versión	Causa de la nueva versión	Fecha de aprobación
01.00	Versión inicial	05/04/2017
01.01	<p>Modificación del nombre del documento.</p> <p>Se actualiza apartado 2 de plataforma tecnológica base corporativa a la última versión del documento de plataforma tecnológica Amtega (GLOBAL_AT_plataformaTecnologicaAmtega:v.01.05). El documento de plataforma se sustituirá por esta guía de estándares y procedimientos de desarrollo y adquisición de aplicaciones en Amtega.</p> <p>Se incluye versión de WSO2 El corporativa en el apartado SOA de plataforma tecnológica.</p> <p>Se añade versión CAS de plataforma SOA en apartado 2.9</p> <p>Se añaden los estándares de arquitecturas de aplicaciones, de desarrollo de aplicaciones general y de desarrollo de servicios web al apartado 4.2.1</p> <p>Se incluyen procedimiento avanzado y procedimiento de liberación y consumo de servicios SOA al apartado 4.2.4</p>	11/04/2018
01.02	Actualización del apartado 2.4 – servidores de aplicaciones con nueva versión IIS10 y Weblogic 12.2, así como el replanteamiento del uso de las plataformas Tomcat y Jboss.	19/12/2018

LISTA DE DISTRIBUCIÓN (opcional)		
Nombre	Número de copia	Área/Centro/Localización

**CLÁUSULA DE CONFIDENCIALIDAD**

Este documento es propiedad de la Amtega (Axencia para a Modernización Tecnolóxica de Galicia). Deberá emplear este material exclusivamente para los servicios que fueron acordados con la Amtega y que requieren necesariamente de su utilización. Está prohibida la reproducción parcial o total, por cualquier medio o método, de los contenidos de este documento para cualquier otro uso no acordado con la Amtega.

## Índice

1. Introducción.....	4
1.1. Ámbito de aplicación.....	4
2. Plataforma tecnológica corporativa.....	5
2.1. Puesto de usuario.....	6
2.2. Sistemas operativos de servidor.....	6
2.3. Servidores WEB.....	6
2.3.1. Balanceadores y proxys.....	6
2.3.2. Contenedor web para PHP.....	6
2.4. Servidores de aplicaciones.....	6
2.5. Generador de informes/documentos.....	7
2.6. Servidores de bases de datos.....	7
2.7. Gestores de contenidos (CMS).....	7
2.8. Sistemas de información geográfica (GIS).....	8
2.9. CAS	8
2.10. SOA8	
2.11. Blogs.....	8
2.12. Gestores documentales.....	8
2.13. Portales de colaboración.....	9
2.14. Teleformación.....	9
2.15. Virtualización.....	9
2.16. Soluciones de integración continua para el desarrollo.....	9
2.17. Gestión de tickets y Gestión de la configuración (CMDB).....	9
2.18. Virtualización.....	9
2.19. Correo.....	9
2.20. Vulnerabilidades.....	10
3. Herramientas corporativas disponibles.....	11
3.1. Repositorio de documentación y portales de colaboración.....	11
3.2. Gestión de proyectos.....	11
3.3. Procesos ITIL.....	11
3.4. Herramientas de soporte al desarrollo.....	11
4. Estándares y procedimientos.....	12
4.1. Calidad.....	12
4.1.1. Nomenclatura.....	12
4.1.2. Gestión de la documentación.....	12
4.1.3. Procedimiento de alta de proyectos.....	12
4.2. Desarrollo y adquisición de sistemas de información.....	12
4.2.1. Diseño y desarrollo.....	13
4.2.2. Integración continua.....	13
4.2.3. Plataforma	14
4.2.4. Procedimientos de desarrollo y auditoría técnicas.....	14
4.2.5. Procedimiento de publicación de aplicaciones.....	14
4.3. Seguridad.....	14
4.3.1. Gestión del personal.....	15
4.3.2. Entrega de compromisos de confidencialidad.....	15
4.3.3. Acceso a los sistemas de información y acceso físico.....	15
4.3.4. Seguridad en el desarrollo de aplicaciones y sistemas.....	15

## 1. Introducción

Este documento pretende servir como guía introductoria a los procedimientos y estándares definidos por la Axencia para a Modernización Tecnolóxica de Galicia (en adelante Amtega). Estos se deberán aplicar por defecto en los proyectos y servicios licitados por la Amtega y especialmente en los proyectos de desarrollo y adquisición de aplicaciones software.

Se indicará en primer lugar la plataforma tecnológica base corporativa. Posteriormente se enumeran los principales estándares y procedimientos existentes en la organización, que serán de aplicación a todos los proyectos, incluyendo los de desarrollo, mantenimiento y adquisición de aplicaciones de software.

La Amtega dispone de documentos específicos para cada estándar y procedimiento descrito que se pueden consultar en el portal XuntaTIC (<http://xuntatic.xunta.es>), portal de divulgación de estándares, normativa y cualquier otra información para el personal TIC de la Xunta de Galicia. Tienen acceso a dicho portal el personal interno y personal correspondiente a contrataciones vigentes de la Amtega que disponga de un usuario en el directorio activo corporativo.

### 1.1. Ámbito de aplicación

Los estándares descritos en este documento aplicarán por defecto en todos los proyectos y servicios licitados en Amtega y especialmente en los proyectos de desarrollo, mantenimiento y adquisición de software.

## 2. Plataforma tecnológica corporativa

Este apartado define la línea base de plataforma que será tomada como referencia en todos los proyectos en el ámbito de la Amtega. Se pretende reflejar una foto del conjunto de entornos corporativos existentes en Amtega y que no están basadas en entornos heredados. Se incluye, además, algún apunte sobre el entorno de cliente (PC del usuario).

Las versiones concretas de detalle de los productos identificados en este apartado, así como otras versiones de productos, drivers, librerías, etc directamente relacionadas con la plataforma tecnológica, se mantendrán actualizadas en la [WikiTIC](#), dejando este documento para identificar las versiones “mayor” de los productos que definen la plataforma tecnológica corporativa.

En las reuniones de arranque de los proyectos, a través de la tramitación de los procedimientos de auditoría técnica (desarrollo convencional, desarrollo ágil o adquisición), se debe seleccionar y acordar la plataforma idónea a aplicar. En dichas reuniones, se revisarán las versiones vigentes del software y middleware de interés para el proyecto.

De forma general, para todas las plataformas tecnológicas corporativas, se soporta un conjunto reducido de versiones por el coste de mantenimiento asociado a tener que mantener múltiples entornos de ciclo de vida, así como mayores garantías de una correcta gestión, disponibilidad, rendimiento, monitorización, etc. de dichos entornos, al poder contar con un alto nivel de especialización y conocimiento de los mismos al tratarse de un conjunto limitado de versiones.

En esta misma línea de limitar y homogeneizar los productos y versiones corporativos, la especialización y conocimiento de infraestructura por parte de los diferentes grupos, implica una mayor calidad y eficiencia en los servicios prestados, mejorando los procesos ITIL:

- Gestión de cambios, incidencias, problemas, peticiones y eventos: se consigue una mayor eficiencia en los equipos de administración al poder enfocarse en un número limitado de elementos de infraestructura.
- Gestión de capacidad, disponibilidad y continuidad negocio: mejoras en los procesos derivados de contar con un conjunto más acotado de soluciones tecnológicas.
- Gestión del conocimiento: permite tener una mayor profundidad de conocimiento en cada área, producto y solución tecnológica, al ser un conjunto reducido.
- Gestión de seguridad: mayor control de infraestructura, y facilidad de aplicar medidas proactivas en un conjunto más reducido de elementos.
- Gestión de pruebas y validación: permite procesos de prueba más estandarizados y depurados, que reducen los tiempos de prueba y mejoran la calidad de los mismos.

Estas mejoras en calidad y eficiencia en los diferentes procesos permiten además reducir los riesgos en la ejecución de los diferentes proyectos, tanto de implantación de nuevos servicios (o evolución de los actuales), como de proyectos de infraestructura (migraciones, etc.).”

Cualquier propuesta por parte de los equipos de proyecto de plataformas o versiones de productos diferentes a las indicadas en este apartado deberán ser argumentadas y consensuadas previamente con el grupo de Arquitecturas Tecnológicas en base a una valoración de las diferentes alternativas técnicas, las posibilidades de adaptación existentes, los riesgos asociados, etc. En el caso de que finalmente se autorice el despliegue en una plataforma o versión de producto diferente de la corporativa podrá implicar que el nivel de servicio que se podrá prestar sobre dicha plataforma será menor que el ofrecido sobre plataformas corporativas. En estos casos también se podrá valorar el desplegar dicho entorno en un modelo de administración delegada, sobre el que se está definiendo un estándar para su regulación, en el que no se dispondrá de todas las garantías de disponibilidad, rendimiento y mantenimiento de los entornos corporativos, y en el que podrían no estar disponibles todos los entornos de ciclo de vida. En cualquier caso, estos escenarios excepcionales deberán justificarse y autorizarse; se deberá consultar con el grupo de Arquitecturas Tecnológicas en caso de dudas sobre estos modelos de administración delegada mientras no esté publicado el estándar.

Este documento llevará asociado un procedimiento de revisión y actualización periódico, con el fin de revisar la actualización de versiones y productos. Esta actualización tendrá que ser motivada por necesidades de negocio o por necesidades tecnológicas como puede ser la falta de soporte, etc.. Habrá un plan de migración de versiones alineado con las aplicaciones y servicios que corren en las plataformas. Se crearán procedimientos para articularlo. En los próximos meses se irán incorporando a la plataforma corporativa nuevos elementos que obligarán a la actualización de este documento.

## 2.1. Puesto de usuario

El software que puede impactar en el funcionamiento de las aplicaciones de las maquina de PCs en Xunta es el siguiente:

- Sistema Operativo
- Navegador
- Máquina virtual de Java (JRE)
- AWP

Las versiones corporativas de este software pueden consultarse en el documento [GLOBAL\\_PCD\\_ConfigDefPostoTraballoCorporativo\\_v.xx.yy](#).

## 2.2. Sistemas operativos de servidor

- Plataforma Unix: **Red Hat 7.X / Centos 7.X**.
- Plataforma Windows: **Windows Server 2016**.

Nota: las versiones RHEL 6.x / CentOS 6.x y Windows 2012 R2 también son corporativas, si bien no son recomendadas para la instalación de nuevo software.

## 2.3. Servidores WEB

### 2.3.1. Balanceadores y proxys

- **Apache 2.2**  
Es el proxy web corporativo de referencia.
- **Microsoft Forefront Unified Access Gateway (UAG) 2010**  
Solo para plataforma Microsoft en las que se justifique su uso, al ser Apache el proxy web corporativo. El uso de UAG es exclusivamente para accesos externos: la publicación de forma autenticada de webs intranet en internet (los accesos en el ámbito de la intranet no irán por UAG).
- **Balanceadores hardware (A10)**  
Como solución generalizada se utilizan balanceadores HW para el reparto de peticiones con los proxys web.

### 2.3.2. Contenedor web para PHP

- **Apache 2**  
Es el contenedor web de referencia para aplicaciones PHP. Las versiones de PHP corporativas son 5.3.3 y 5.6.x.

## 2.4. Servidores de aplicaciones

- **Tomcat 8.5** con JRE 1.8, JSP 2.3 y Servlet 3.1. Entorno UNIX.

Su uso está orientado a aplicaciones web desarrolladas en Java (JSPs, Servlets...) que no requieren de las capacidades enterprise de JEE. En este escenario encajan gran parte de las aplicaciones desarrolladas en la Amtega, que son aplicaciones de criticidad medio baja, con arquitecturas sencillas, etc. Destacar que las garantías de nivel de servicio de esta plataforma son inferiores a la plataforma Weblogic, dado que no se cuenta con soporte de fabricante y las herramientas de gestión y monitorización son más limitadas. No obstante, dichas garantías serán suficientes para un conjunto de aplicaciones importante.

También encajan en este grupo las aplicaciones legacy que están corriendo en versiones de Tomcat más antiguas. Podrán migrar a la versión de Tomcat corporativa de manera más sencilla.

Nota: la plataforma Tomcat 8, con JRE 1.7 también es corporativa pero no se recomienda para nuevos desarrollos.

- **Weblogic 12.2** con JRE 1.8 – Compliant JEE7. Entorno UNIX.

Está orientado a albergar aplicaciones JEE más críticas, o de cierta criticidad, que requieren niveles de servicio más elevados. De igual modo, también está destinado a aplicaciones en donde



se requieran capacidades JEE que no están incluídas en un simple contenedor web. La selección de esta plataforma en lugar de la plataforma Tomcat para novos proyectos, se debe decidir en base a criterios como complejidad de la arquitectura, criticidad, afinidad de: negocio, tecnolóxica, de administración, de soporte, etc.

Nota: la plataforma Weblogic 12.1 (12c) con JRE 1.7 – Compliant JEE6 también es corporativa, pero no se recomienda para novos desarrollos.

- **JBOSS EAP 6** con JRE Java SE 1.7 (con soporte JEE 6). Entorno UNIX.  
Su uso quedará reducido a los entornos ya existentes y, de ser necesario, en proyectos en los que no encajen las soluciones estándar (Tomcat o Weblogic), su uso deberá ser correctamente argumentado y consensado con el equipo de Arquitecturas Tecnolóxicas. Esta plataforma seguirá manteniendo el soporte de fabricante.
- **IIS10**  
Para aplicaciones .NET bajo entorno Windows 2016 . Framework .NET 4.7 (con soporte a versiones inferiores).  
Su uso está reservado a proyectos existentes y nuevas aplicaciones que deban utilizar plataforma Windows: en estos casos, su uso deberá ser correctamente argumentado y consensado con el equipo de Arquitecturas Tecnolóxicas.  
Nota: la plataforma IIS 8.5 con Windows 2012 R2 también es corporativa, pero no se recomienda para novos desarrollos.

## 2.5. Generador de informes/documentos

- **JasperReports Server 6.3**  
Plataforma de reporting para la generación de informes (listados) en varios formatos de salida: pdf, html, xml, etc.
- **LibreOffice 4.x (Servidor)**  
Servidor para la generación de documentos y conversión de formatos, en base a plantillas, por parte de las aplicaciones. El acceso a este servidor debe ser a través de los servicios existentes para este propósito.

## 2.6. Servidores de bases de datos

- **Oracle 12C** (codificación AL32UTF8)  
Es la opción corporativa a utilizar en novos proyectos. Por defecto se utiliza el modo de clúster Oracle RAC. Si en alguna aplicación no encaja el uso de Oracle RAC por algún motivo, se podrán usar servicios SINGLETON para simular el comportamiento de una base de datos Single Instance. Este aspecto deberá ser argumentado y consensado con el equipo de Arquitecturas Tecnolóxicas.
- **Informix 11**  
La selección de esta plataforma en lugar de la de Oracle para novos proyectos, se debe decidir en base a criterios como la afinidad de negocio, tecnología, administración, soporte, etc., previa argumentación y consenso con el equipo de Arquitecturas Tecnolóxicas.  
Nota: está prevista una próxima instalación de la versión de Informix 12.
- **MySQL 5.7.x clúster (basado en scripts multimaestro MHA)**. Entorno UNIX.  
Orientado a aplicaciones simples (divulgación, etc), con un modelo de desarrollo LAMP, sin requerimientos altos de infraestructura.
- **SQL Server 2016**  
En proyectos en los que no encaje el uso del gestor corporativo Oracle, podrá ser evaluada la utilización de SQL Server, previa argumentación y consenso con el equipo de Arquitecturas Tecnolóxicas. La versión SQL Server 2012 también es corporativa, si bien su uso no está recomendada para novos desarrollos.

## 2.7. Gestores de contenidos (CMS)

- **Drupal v7**

Es la solución recomendada para la implementación de portales (con un modelo de desarrollo LAMP), con bajas necesidades de desarrollo y/o personalizaciones. El entorno de ejecución de la plataforma Drupal corporativa se indica en la [WikiTIC](#).

- **Liferay v6.2**  
Orientado a portales más complejos en donde la solución recomendada por defecto no aplique, con necesidades de personalización altas (desarrollos en JEE), para entornos multiportales con requisitos de integración importantes o con necesidades de infraestructura también más exigentes. Su uso debe estar correctamente justificado y validado con el equipo de Arquitecturas Tecnológicas por los problemas que presenta en cuanto a los recursos dedicados de infraestructura necesarios para su despliegue y mantenimiento.
- **OpenCMS v9**  
Su uso está orientado a portales integrados con Liferay. Su uso como CMS independiente debe estar correctamente justificado y validado con el equipo de Arquitecturas Tecnológicas, siempre que no encaje el uso de la solución Drupal.

## 2.8. Sistemas de información geográfica (GIS)

- **ArcGIS Server 10.5.**  
Entorno Windows. Plataforma corporativa para el despliegue de servicios GIS.  
Nota: La versión 10.4 también es corporativa, si bien no es de aplicación para nuevos proyectos.
- **Portal for ArcGIS 10.5.**  
Entorno Windows. Plataforma corporativa para el despliegue de mapas y visores GIS.

## 2.9. CAS

- **CAS v4.2.x.**  
Plataforma CAS/SSO en entorno de alta disponibilidad. Su uso está orientado a aplicaciones web en intranet.
- **CAS v5.x**  
CAS en alta disponibilidad, cuyo uso está reservado para las aplicaciones consumidoras de servicios y para los propios servicios de la plataforma SOA. Actúa como proveedor OpenID Connect 1.0, que es el protocolo de seguridad (autenticación) para la integración entre servicios, montado sobre el protocolo OAuth 2.0 (autorización).

## 2.10. SOA

- **WSO2 GREG v.5.x**  
Herramienta de gobierno SOA corporativa.
- **WSO2 EI v.6.x**  
Orientado a facilitar la interconectividad entre servicios y aplicaciones a nivel empresarial. Está formado por:
  - ✓ ESB (Enterprise Service Bus): establece una capa intermedia de interconexión y procesamiento de mensajes, así como proporciona capacidades de QoS (timeout, reintentos, control de flujo, seguridad y asincronismo).
  - ✓ DSS (Data Services Server): permite exponer diferentes fuentes de datos como servicios publicados en el ESB.
  - ✓ microDAS (Data Analytics Server): posibilita la monitorización y análisis del ESB (estadísticas y trazabilidad de mensajes).

## 2.11. Blogs

- **blogs.xunta.gal**
- **WordPress v4.x**  
El uso de WordPress está limitado a blogs que no encajen en la plataforma blogs.xunta.gal. Su uso debe estar correctamente justificado y validado con el equipo de Arquitecturas Tecnológicas y, en cualquier caso, no debe utilizarse para el desarrollo de portales web, donde la solución corporativa recomendada es Drupal.



## 2.12. Gestores documentales

- **Alfresco 4.2.x**  
Desplegado sobre máquinas Linux. Es la opción recomendada para la gestión documental en un proyecto para albergar documentación de expedientes vinculados a procesos de tramitación electrónica. El acceso a Alfresco deberá realizarse a través de la capa de servicios definida en el proyecto ARPAD. Para poder realizar accesos directos a Alfresco deberá justificarse y acordarse con el equipo de Arquitecturas Tecnológicas, en cuyo caso se deberá utilizar el componente transversal ya existente para acceso por CMIS.
- **SharePoint 2013**  
El uso de esta plataforma está orientado exclusivamente a aplicaciones que ya están integradas con Sharepoint.
- **Base de datos o Sistema de Ficheros**  
El uso de base de datos o sistema de ficheros para el almacenamiento masivo de documentos no está recomendado de forma general, pero para aquellos casos que no encajen en el resto de escenarios, podrá valorarse su uso previa justificación y autorización por parte del equipo de Arquitecturas Tecnológicas.

## 2.13. Portales de colaboración

- **SharePoint 2013**  
Su uso no está orientado al desarrollo de portales de negocio corporativos, sino únicamente para la generación de espacios de colaboración.

## 2.14. Teleformación

- **PLAFOR**  
Plataforma multisite de teleformación Amtega, basada en Moodle 3.0.x. Más información en [XuntaTIC](#).

## 2.15. Virtualización

- **RHEV v3**: Es la solución corporativa por defecto para la virtualización.
- **VMWare 5**: Es una solución disponible para ámbitos reducidos, por lo que su uso se debe argumentar y consensuar con el equipo de Arquitecturas Tecnológicas en cada caso.

## 2.16. Soluciones de integración continua para el desarrollo

- Control de código fuente: **Subversion 1.11.x**
- Gestión de proyectos: **Redmine 3.x**
- Repositorio de artefactos **Nexus 2.x**
- Gestor de pruebas **TestLink 1.9.x**
- Servidor de Integración Continua: **Jenkins 1.x**
- Medición de calidad del software: **Sonar 4.x**
- Pruebas de carga: **Jmeter 2.x / 3.x**

## 2.17. Gestión de tickets y Gestión de la configuración (CMDB).

- Gestión de la configuración: **OTRS 5.x**.

## 2.18. Virtualización

- **RHEV v4.x**
- **VMWare 5.x**

## 2.19. Correo

Servicio de correo en el ámbito Xunta basado en Microsoft:

- **MS Exchange 2013**
- **Symantec Enterprise Vault 11.x.** Servicio de archivado de correo para Exchange.

Servidor de correo actual en los ámbitos de Educación y Xustiza basado en:

- **Postfix 2.7.1 e Imaproxy 1.2.6**

## 2.20. Vulnerabilidades

- **Acunetix versión 10.x.** Para el análisis de vulnerabilidades en aplicaciones web.
- **Symantec Protection Engine for Cloud Services versión 7.x.** Servicio online en Amtega para la detección de virus.

### 3. Herramientas corporativas disponibles

La Amtega dispone, para los diferentes proyectos y servicios, de diversas herramientas corporativas de apoyo. A continuación se citan las herramientas principales.

#### 3.1. Repositorio de documentación y portales de colaboración

Toda la documentación de los proyectos se depositará en la herramienta de gestión de documentación de proyectos corporativa basada en **Sharepoint**. Esta plataforma se empleará asimismo para la generación de espacios de colaboración.

#### 3.2. Gestión de proyectos

La herramienta que se usa en la Amtega para el seguimiento y control de los proyectos es **Redmine**.

#### 3.3. Procesos ITIL

La herramienta **OTRS** soporta en la Amtega los procesos ITIL de gestión de incidencias, gestión de peticiones de servicio y gestión de configuración.

La gestión de accesos la herramienta de gestión de incidencias corporativa se detallan en la guía *GLOBAL\_GU\_proyectosDesenvolvementoAdquisicion\_v.xx.yy*.

Con el fin de gestionar, identificar y controlar los elementos de los proyectos se realiza el proceso de Gestión de la configuración recogido en el documento *GLOBAL\_BP\_xestionConfiguracion\_v.xx.yy*. Toda la información se almacena en la CMDB compartida por todos los procesos, asegurando por tanto que la gestión de activos e ITIL están alineados.

#### 3.4. Herramientas de soporte al desarrollo

Las herramientas disponibles en la Amtega para los proyectos de desarrollo y adquisición de software son:

- **Servidor de Integración Continua: Jenkins.** Se utiliza para la construcción, generación de artefactos, pruebas unitarias, revisión de la calidad del código y automatización de los procesos de despliegue en los servidores corporativos.
- **Medición de calidad del software: Sonar.** Gestiona la revisión automatizada de la calidad del código fuente de forma automatizada.
- **Gestor de pruebas: TestLink.** Se utiliza para llevar a cabo la gestión de pruebas funcionales y no funcionales en las aplicaciones, permitiendo llevar trazabilidad de los ciclos de prueba ejecutados en cada versión.
- **Repositorio de artefactos: Nexus.** Se utiliza para ubicar las releases Final y RC, principalmente, y también las revisiones anteriores necesarias (alphas y betas).
- **Control de código fuente: Subversion.** Cada proyecto contará con su propio repositorio de Subversion. Los principales usuarios del repositorio serán los desarrolladores, sin embargo, también lo utilizará el servidor de integración continua en los procesos de construcción automatizada del software, mediante la descarga de los fuentes de la versión de la aplicación que construye.
- **Gobierno de arquitectura SOA: WSO2 GReg.** Herramienta que permite publicar los servicios SOA transversales y departamentales existentes en Amtega, así como valorar y comentar aspectos de interés de cada servicio.
- **Monitorización de servicios en plataforma SOA: Cuadro de mando del DAS (Data Analytics Server).** Se utiliza para monitorizar los servicios expuestos por el ESB (número de peticiones, transacciones por segundo, tiempos de respuesta, payload completos de las peticiones y respuestas, etc).
- **Wiki de XuntaTIC** con FAQs, ejemplos de código y documentación, errores conocidos, componentes API transversales disponibles, y otros recursos de interés para el desarrollo.
- **Comité de arquitecturas:** Foro corporativo de debate técnico sobre estándares y procedimientos en el ámbito de la arquitectura de las aplicaciones.



## 4. Estándares y procedimientos

Para todos los proyectos y servicios licitados en Amtega es necesario cumplir con una serie de estándares y procedimientos. Toda la documentación relativa a estándares y procedimientos de la Amtega se encuentra publicada en el portal de colaboración XuntaTIC.

### 4.1. Calidad

Todos los proyectos de la Amtega deben respetar las normas de calidad establecidas para toda la organización en lo referente aspectos generales (estándares generales, nomenclatura, gestión documental, procesos TIC, etc.).

#### 4.1.1. Nomenclatura

La guía que establece la política de nombrado de elementos TIC en la Amtega es *GLOBAL\_GU\_nomenclaturaGeneral\_v.xx.yy*. Sirve como directorio de consulta de nombrado de cualquier elemento TIC, así como otros elementos relacionados con éstos que se gestionan en la agencia. Existen además otras guías específicas publicadas:

- **Nomenclatura unificada de elementos tecnológicos de la plataforma de sistemas** (*D\_S\_AT\_nomenclaturaUnificadaSistemas\_v.xx.yy*): Regula la nomenclatura a utilizar en los diversos elementos tecnológicos que forman parte de la plataforma gestionada por el Departamento de Sistemas. De este modo, las infraestructuras consolidadas nombrarán sus componentes de manera uniforme y autodescriptiva.
- **Nomenclatura unificada dos elementos da plataforma de bases de datos** (*D\_S\_AT\_nomenclaturaUnificadaObjetosBBDD\_v.xx.yy*): Regula la nomenclatura a utilizar en los diversos elementos de la plataforma de base de datos.

#### 4.1.2. Gestión de la documentación

Toda la documentación entregada por los proyectos deberá seguir la guía *GLOBAL\_GU\_modelosDocumentacionAmtega\_v.xx.yy* y utilizar obligatoriamente las plantillas corporativas basadas en **LibreOffice** que se encuentran publicadas en dicho portal.

#### 4.1.3. Procedimiento de alta de proyectos

Procedimiento obligatorio para todos los proyectos de desarrollo de la Amtega con el fin de integrar el nuevo proyecto en la infraestructura y los procesos TIC.

Todos los proyectos deben comenzar con el procedimiento de alta de proyecto publicado en XuntaTIC *GLOBAL\_PCD\_altaProyectos\_v.xx.yy*.

Este procedimiento deriva en el cumplimiento de otros procedimientos y/ estándares de la organización.

## 4.2. Desarrollo y adquisición de sistemas de información

Los principales **estándares de desarrollo aplicables en la Amtega** están recogidos en este documento, en el que se describen los principios básicos que deben tenerse en cuenta para el desarrollo o adquisición de aplicaciones en la Amtega, a destacar:

- 1 Para los nuevos desarrollos en plataforma corporativa es de obligado cumplimiento el uso del entorno de desarrollo
- 2 Las primeras versiones de aplicaciones que se han desarrollado en plataforma corporativa deben utilizar la plataforma de integración continua y los entornos de desarrollo, salvo motivo justificado, para aprovechar la ligereza y autonomía de los despliegues que dicha plataforma proporciona a los equipos de proyecto. También se recomienda para proporcionar autonomía a aquellas aplicaciones sujetas a un ciclo de vida muy activo, con requisitos de red despliegues muy frecuentes.
- 3 Las nuevas aplicaciones desarrolladas en Amtega deben seguir los arquetipos corporativos indicados en la [WikiTIC](#), salvo motivo justificado, para facilitar la integración con los diferentes servicios transversales, plataforma de integración continua, además de reducir posibles riesgos técnicos, problemas en despliegues, etc.



- 4 Las aplicaciones deben estar diseñadas respetando los principios básicos de arquitectura descritos en el Estándar de arquitectura de aplicaciones (GLOBAL\_ES\_EstandaresArquitecturaAplicaciones\_v.xx.yy)

Además de este estándar de desarrollo, la Amtega dispone de diversos estándares, procedimientos, modelos y guías aplicables también en los proyectos de desarrollo, todos ellos publicados en el portal XuntaTIC que se citan en los siguiente apartados.

### 4.2.1. Diseño y desarrollo

- **Estándar de arquitectura de aplicaciones** (GLOBAL\_ES\_EstandaresArquitecturaAplicaciones\_v.xx.yy):

El objetivo de este documento es facilitar la consolidación de la plataforma tecnológica y homogeneización de tecnologías en la Amtega. Describe los principios básicos de carácter general aplicables en la Amtega en base a las restricciones y requerimientos de la organización (seguridad, infraestructura, aspectos organizativos, etc), así como los estándares de arquitectura que deben cumplir en las aplicaciones desarrolladas e implantadas en la Amtega.

- **Estándar de desarrollo de aplicaciones** (GLOBAL\_ES\_EstandaresDesarrollo\_v.xx.yy):  
Conjunto mínimo de requerimientos, recomendaciones técnicas, marco tecnológico y terminología común necesarios para estandarizar los proyectos software de la Amtega.
- **Estándar de desarrollo de aplicaciones JEE** (GLOBAL\_ES\_EstandaresDesarrolloJEE\_v.xx.yy):  
Requerimientos y recomendaciones técnicas específicas para estandarizar los proyectos desarrollados en plataforma JEE de la Amtega.
- **Estándar de desarrollo de servicios web** (GLOBAL\_ES\_EstandaresDesarrolloWS\_v.xx.yy):  
Establece las pautas y recomendaciones a tener en cuenta para el desarrollo y consumo de servicios web en la Amtega, de modo que se facilite su reutilización en la organización.
- **Estándar de desarrollo de aplicaciones Drupal** (GLOBAL\_ES\_EstandaresDesenvolvemientoDrupal\_v.xx.yy)  
*Directrices y recomendaciones para desarrollos realizados con la distribución base Drupal para proyectos en la Amtega.*
- **Estándares y recomendaciones de diseño para bases de datos** (GLOBAL\_ES\_EstandaresBBDD\_v.xx.yy):  
*Recomendaciones importantes para manejar adecuadamente el acceso a los datos: secuencias, índices, segmentación, manejo de datos externos, etc.*
- **Guía de versionado y etiquetado de software** (GLOBAL\_GU\_versionadoEtiquetadoSW\_v.xx.yy):  
Describe los aspectos que relacionan el versionado de las entregas, con las etapas y entornos asociados a las distintas fases del ciclo de vida del software. También se detallan las convenciones de versionado de los diferentes elementos de una entrega, en función del momento del ciclo de vida donde se enmarca, procedimiento, entorno al que va dirigida y tipología.
- **Estándares de gestión de entregas** (GLOBAL\_ES\_gestionEntregas\_v.xx.yy):  
*Descripción del proceso operativo y convenciones necesarias para normalizar la gestión de la entregas de código fuente, documentación y artefactos de proyecto.*
- **Modelo de gobierno SOA** (GLOBAL\_ES\_ModeloGobiernoSOA\_v.xx.yy):  
Regula la implantación de esta arquitectura en la Amtega.

### 4.2.2. Integración continua

- **Modelo de integración continua** (GLOBAL\_ES\_ModeloIntegracionContinua\_v.xx.yy):  
Descripción del modelo de integración continua en su conjunto con las principales características de cada uno de los elementos que lo componen, así como su interrelación con otros componentes.
- **Plataforma unificada de Nexus** (D\_S\_AT\_plataformaUnificadaNexus\_v.xx.yy):  
Define y describe la arquitectura técnica estándar para la plataforma de integración continua nexus gestionada por el Departamento de Sistemas.

Además existen una serie de guías de apoyo al uso de las herramientas:

- **Manual de uso y arquitectura GU lógica de Nexus** (GLOBAL\_GU\_GuiaUsoNexus\_v.xx.yy).

- **Guía de uso de Jenkins** (*GLOBAL\_GU\_guiaUsoJenkins\_v.xx.yy*).
- **Manual de uso de Testlink** (*GLOBAL\_GU\_GuiaUsoTestlink\_v.xx.yy*).

### 4.2.3. Plataforma

- **Configuración unificada de servidores RHEL/CentOS** (*D\_S\_AT\_configuracionUnificadaRhelCentos\_v.xx.yy*): Estándar de configuración unificada para servidores con sistema operativo RHEL /CentOS.
- **Estructura unificada de entornos** (*D\_S\_AT\_estructuraUnificadaEntornos\_v.xx.yy*): Define un estándar de entornos que permite regular el ciclo de vida de un servicio TI a través de los sistemas gestionados por el Departamento de Sistemas.

### 4.2.4. Procedimientos de desarrollo y auditoría técnicas

Los nuevos proyectos de desarrollo o adquisición de aplicaciones software de negocio en la Amtega deben superar un procedimiento de auditoría como requisito para su implantación. Los procedimientos a seguir según el tipo de desarrollo son:

- **CONVENCIONAL** – *GLOBAL\_PCD\_convencionalDesarrolloAplicaciones\_v.xx.yy*. Aplicable en la mayoría de los proyectos de desarrollo de software aprobado por la Amtega
- **ÁGIL** - *GLOBAL\_PCD\_agilDesarrolloAplicaciones\_v.xx.yy*. Aplica a todo proyecto de desarrollo software aprobado por la Amtega, que por sus características funcionales o técnicas de baja complejidad, así como la ausencia de riesgos en cuanto a infraestructura o bien se desarrollen bajo metodologías ágiles no necesite completar el Procedimiento Convencional.
- **ADQUISICIÓN** – *GLOBAL\_PCD\_adquisicion\_v.xx.yy*. Aplica a todo proyecto o producto software desarrollado, cuya adquisición ha sido aprobada por la Amtega.
- **AVANZADO** – *GLOBAL\_PCD\_avanzado\_v.xx.yy*. Aplicable para proyectos de desarrollo y/o adquisición que por su complejidad a nivel de arquitectura (múltiples componentes, ecosistema de proyectos interrelacionados, etc.) requieran de una gestión y documentación global que abstraiga a la particular de cada pieza, subproyecto o proyecto individual (que seguirán su propio flujo de validación a través de los procedimientos ágil, convencional o adquisición).

Por otra parte, existen dos procedimientos complementarios:

- **Procedimiento de publicación de componentes API transversales** (*GLOBAL\_PCD\_publicacionComponentesApiTransversales\_v.xx.yy*) para la publicación de nuevas librerías/componentes API transversales que sean directamente reutilizables por otras aplicaciones o sistemas
- **Procedimiento de liberación y consumo de servicios SOA** (*GLOBAL\_PCD\_liberacionYConsumoServiciosSOA\_v.xx.yy*) para divulgar de forma transversal nuevos servicios SOA o actualización de aquellos existentes en la infraestructura de la Amtega, así como permitir el consumo de dichos servicios SOA transversales.

### 4.2.5. Procedimiento de publicación de aplicaciones

Una vez superadas las etapas correspondientes de los procedimientos de auditoría, se puede solicitar la publicación de la aplicación en el entorno que corresponda siguiendo el procedimiento *GLOBAL\_PCD\_publicacionAplicaciones\_v.xx.yy*.

Para la publicación de aplicaciones deben seguirse los estándares relacionados con los proyectos de desarrollo en XuntaTIC, siendo de especial interés en este punto el estándar de gestión de entregas *GLOBAL\_ES\_gestionEntregas\_v.xx.yy* y la guía de versionado y etiquetado de software *GLOBAL\_GU\_versionadoEtiquetadoSW\_v.xx.yy*.

## 4.3. Seguridad

Todo proyecto desarrollado en la Amtega, además de la legislación en materia de seguridad y protección de datos europea, estatal y autonómica, como son la Ley Orgánica 15/1999 de Protección de Datos o el Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad, deberá respetar lo establecido en el **Documento de Seguridad** (*GLOBAL\_DSE\_documentoSeguridadAmtega\_v.xx.yy*).

El objeto del documento de seguridad es establecer las medidas de índole técnica y organizativa necesarias para garantizar los niveles de seguridad que deben reunir los ficheros, los tratamientos, los

locales, los equipos, los sistemas, los programas y las personas que intervienen en el tratamiento de datos de carácter personal sujetos al régimen de la LOPD.

Además en la Amtega existen diferentes políticas, guías y estándares de seguridad de la información de obligado cumplimiento que se citan en los apartados siguientes.

### 4.3.1. Gestión del personal

- **Buenas prácticas en el uso de sistemas de información** (*Decreto 230/2008*): Regula las normas de utilización de los sistemas de información y de comunicaciones, fijos y móviles, de que dispone la Administración de la Comunidad Autónoma de Galicia, y establece los derechos y las obligaciones de las personas usuarias de estos sistemas en lo relativo a su seguridad y buen uso.
- **Buenas prácticas en el ámbito de la protección de datos** (*GLOBAL\_BP\_proteccionDatos\_v.xx.yy*): Mediante este documento se facilita a todas las personas usuarias de los sistemas de información de la Administración de la Comunidad Autónoma de Galicia, información suficiente para que conozcan las funciones y obligaciones que les correspondan en el marco de la protección de datos.
- **Documento de roles y responsabilidades:**  
(*GLOBAL\_PL\_FuncionsObrigasLOPDPersonalAmtega\_v.xx.yy*): Funciones y obligaciones que el personal debe llevar a cabo en relación con los ficheros que contengan datos de carácter personal, en función de las tareas que tengan encomendadas.

### 4.3.2. Entrega de compromisos de confidencialidad

- Deben entregar compromiso de confidencialidad -en formato pdf y firmado electrónicamente- siguiendo el procedimiento *GLOBAL\_PCD\_envioCompromisosConfidencialidade\_v.xx.yy* :
  - Las organizaciones ajenas a la administración autonómica que debido a su relación de colaboración con la Amtega accedan a información de el sector público autonómico.
  - Todo el personal ajeno a la administración autonómica que pueda tener acceso a la información del sector público autonómico, de forma intencionada o no, incluido el personal de entidades subcontratadas.

### 4.3.3. Acceso a los sistemas de información y acceso físico

- **Política de acceso lógico a los sistemas de información** (*GLOBAL\_PL\_AccesoLogicoSI\_v.xx.yy*): Establece un marco de actuación que garantiza un control adecuado del acceso de los usuarios a los sistemas de información de la Xunta de Galicia.
- **Política de control de acceso físico** (*GLOBAL\_PL\_ControlAccesoFisico\_v.xx.yy*): Conjunto de medidas de protección a aplicar en las instalaciones para la prevención de posibles accesos a Información por parte de personas no autorizadas, y para proporcionar evidencias necesarias cuando se produzca un acceso o intento de acceso.
- **Política de control de acceso a la red** (*GLOBAL\_PL\_AccesoRede\_v.xx.yy*): Marco de referencia para el acceso a la red corporativa de la Xunta de Galicia.
- **Política de seguridad de las redes sin hilos (WIFI)**  
(*GLOBAL\_PL\_SeguridadRedesSenFios\_v.xx.yy*): Marco para el uso de redes inalámbricas (WIFI) dentro de la Red Corporativa de la Xunta de Galicia.
- **Política de acceso remoto corporativo** (*GLOBAL\_PL\_AccesoRemotoCorporativo\_v.xx.yy*): Establece un marco para el acceso a la red interna y a los sistemas de información de la Xunta de Galicia accesibles desde la misma mediante acceso remoto corporativo y que permita garantizar su seguridad.
- **Política de contraseñas para el acceso a sistemas de información** (*GLOBAL\_PL\_PoliticaContrasinal\_v.xx.yy*): Establece una política de contraseñas común para los sistemas de información corporativos de la Xunta de Galicia que utilizan como método de autenticación un identificador y una contraseña.

#### 4.3.4. Seguridad en el desarrollo de aplicaciones y sistemas

- **Políticas de seguridad Web** (*GLOBAL\_PL\_PolíticaSeguridadeWeb\_v.xx.yy*): Políticas de seguridad a seguir por todos los portales y aplicaciones web de la Administración de la Comunidad Autónoma de Galicia.
- **Procedimiento de análisis de vulnerabilidades en aplicaciones y sistemas** (*GLOBAL\_PCD\_ProbasSeguridade\_v.xx.yy*): Regula las diferentes pruebas de seguridad que se realizan en la Amtega para el análisis de vulnerabilidades en aplicaciones web y sistemas.