SECRETARÍA DE ESTADO DE DEFENSA

DIRECCIÓN GENERAL DE
INFRAESTRUCTURA

SUBDIRECCIÓN GENERAL TIC

INSTRUCCIÓN TÉCNICA

GUÍA DE REQUISITOS DE INTEGRACIÓN EN LA PLATAFORMA SOA DEL MINISDEF

IT-01/SDGTIC/11/GRIPS/V.1

MARZO/2011

Documento

Título: *Guía de requisitos de Integración en la Plataforma SOA del MINISDEF*

Categoría: Instrucción Técnica Versión del Documento: *0.1* Fecha: *30/03/2011*

Departamento: *Subdirección General de Tecnologías de la Información y Comunicaciones*

Área: *Área de Tecnologías*

Control de Firmas

REDACTADO	REVISADO
Área de Tecnologías de la Subdirección General TIC	El Subdirector General de Tecnologías de la Información y Comunicaciones // El Jefe del Área de Tecnologías de la SDGTIC

APROBADO
La Directora General de Infraestructura // El Subdirector General de Tecnologías de la Información y Comunicaciones

Control de Cambios

VERSIÓN	REVISIÓN	FECHA	OBSERVACIONES
0	1	30/3/2011	1er. Borrador

ÍNDICE

1 INTRODUCCIÓN

1.1 *OBJETIVO*

El objetivo de este documento es proporcionar una guía para especificar los requisitos de una integración de sistemas en la Plataforma SOA del Ministerio de Defensa.

El documento resultado de completar esta guía es un documento de "requisitos de integración" que sirve para:

- Definir una solución de diseño de arquitectura específica para el sistema o sistemas a integrar.
- Fijar las condiciones de la puesta en servicio del sistema o sistemas en relación a los elementos de la Plataforma SOA y los compromisos adquiridos por las partes involucradas.

Se establecen los roles y responsabilidades para elaborar, validar y aprobar el documento de requisitos de integración del sistema con la Plataforma SOA, de modo que todas las partes implicadas estén debidamente informadas. Adicionalmente se establece el procedimiento de gestión de cambios una vez aprobada la integración.

Adicionalmente esta guía referencia los casos de uso de integración de sistemas y las tecnologías de servicios soportadas por la Plataforma SOA de modo que se disponga de una referencia para definir los requisitos.

Esta guía es un documento en evolución que recoge la experiencia práctica en los proyectos de integración realizados hasta ahora por el Área de Tecnología de la Subdirección General TIC, estando abierto a mejoras y correcciones provenientes de cualquier parte interesada. Sin embargo, el control de configuración del documento corresponde al Área de Tecnología de la Subdirección General TIC.

Organización de la guía:

Consta de varios capítulos que describen cada uno los apartados a completar para elaborar el documento de requisitos de integración. Se establecen directrices y recomendaciones para proporcionar la información correcta y necesaria.

El capítulo 2 especifica los requisitos de integración funcionales de alto nivel y el capítulo 3 los requisitos técnicos incidiendo en los servicios e interfaces .

El capítulo 4 establece roles y responsabilidades en la integración, el proceso de elaboración del documento de requisitos de integración y el procedimiento de gestión de cambios.

1.2 *ALCANCE*

Esta guía es de aplicación para todas las integraciones de sistemas que vayan a utilizar servicios de la Plataforma SOA, en cualquiera de los dominios de explotación de la WAN PG.

En el contexto de integración de sistemas, los servicios proporcionados por la Plataforma SOA son:

- Servicios seguridad. Autenticar/Autorizar el consumo de los servicios, cifrado a nivel de mensaje o transporte, auditoría de los servicios,…
- Servicios de mediación. Transformación y adaptación de servicios en cuanto a formatos de datos y protocolos de transporte de nivel de aplicación en los casos en los que se requiera.
- Servicios de Registro: Publicación y consulta de servicios disponibles en la red de modo que estén controlados y se evite la proliferación innecesaria de servicios.

Normalmente, los servicios finales serán desarrollados y mantenidos por los sistemas proveedores del mismo, pudiendo estar implementados sobre el bus de servicio de la Plataforma SOA o sobre otros entornos.

1.3 *AUDIENCIA*

Esta guía está dirigida a personal técnico implicado en el desarrollo, mantenimiento, despliegue y explotación de sistemas del Ministerio de Defensa que vayan a utilizar servicios de mediación y/o seguridad proporcionados por la Plataforma SOA:

- Directores técnicos de sistemas de información.
- Arquitectos y jefes de proyecto de desarrollo de software
- Responsables y técnicos de sistemas en producción.

1.4 *REFERENCIAS*

- [MSOA] "Modelo de Arquitectura Orientada a Servicios del MINISDEF", IGECIS, Versión 1.0, DIC 2009
- [GUIWS] "Guía de Implementación de Servicios Web en el Ministerio de Defensa"
- [WANPG2.0] "Especificación de Escenario Objetivo", Grupo de Trabajo de WAN PG 2.0 – IGECIS, Versión 1.0, Feb 2010
- [INET] Instrucción Técnica de IGECIS "Modelo de Arquitectura I*Net" – Mayo 2006

1.5 *PUNTO DE CONTACTO*

Para cualquier sugerencia o propuesta de cambio relativa a este documento, por favor diríjase a:

Ministerio de Defensa

Dirección General de Infraestructura

Subdirección General TIC

Área de Tecnologías

sdgtic@oc.mde.es

2 REQUISITOS DE INTEGRACIÓN FUNCIONALES

A continuación se describen cada uno de los apartados a completar con una breve explicación de su contenido.

2.1 *Necesidad de integración*

Contendrá una descripción de:

- por qué es necesario la integración entre las aplicaciones.
- tipo de información que es necesario intercambiar entre los sistemas.

2.2 *Sistemas y organismos/empresas(s)*

Contendrá una lista de los sistemas implicados, así como el organismo o empresa responsable del mismo.

Nombre	Empresa u organismo responsable

2.3 *Funcionalidad del sistema(s)*

Contendrá una descripción breve de la funcionalidad de cada uno de los sistemas implicados.

Nombre	**Descripción de la funcionalidad**

2.4 *Caso(s) de uso*

Se identificarán el/los caso(s) de uso que se ajusten a la necesidad de integración entre aplicaciones.

En el supuesto que la necesidad de integración no se ajuste a ninguno de los especificados en la tabla siguiente será necesario detallar y justificar la excepción.

A continuación se enumeran los posibles casos de usos contemplados en el contexto de integración de aplicaciones a través de la Plataforma SOA:

Nº	**Descripción**
1	Aplicación/Portal web en nodo de Servicios Web consume servicios de la Intranet
2	Sistema externo (en internet o red SARA[1]) consume un servicio del MINISDEF
3	Sistema expone un servicio para que sea consumido por otra aplicación de la intranet
4	Sistema en intranet consume un servicio publicado (en internet o red SARA[1]) por organismo externo al MINISDEF
5	Sistema en intranet consume un servicio publicado en el nodo de servicios Web
6	Aplicación web en nodo de Servicios Web consume un servicio publicado por

[1] O cualquier otra red externa al Ministerio de Defensa que se interconecte con el nodo extranet.

	organismo externo al MINISDEF (vía internet o red SARA[1])

Para mayor detalle de estos casos consultar el documento [MSOA] "Modelo de Arquitectura Orientada a Servicios del MINISDEF".

Estos casos de uso se adaptarán a las necesidades del nuevo modelo WAN 2.0, en el que desaparecen como tal el "nodo de servicios web", el "nodo extranet" y la "intranet". En WAN 2.0 existirán redes separadas correspondiendo a distintos dominios de seguridad tales como "uso oficial" y "uso público", apareciendo el concepto de nodo de interconexión ([WANPG2.0] "Especificación de Escenario Objetivo"). En este nuevo escenario las soluciones de arquitectura SOA adoptadas para el vigente modelo [INET] vigente serán muy similares, basándose en los mismos estándares y productos en los que se basa actualmente la Plataforma SOA.

2.5 *Perfil de la integración*

Se deberá especificar el perfil que más se adecua a la necesidad de integración.

A continuación se enumeran los perfiles de integración identificados en la Plataforma SOA:

- Un solo **sistema distribuido**. En este caso se trata de un único sistema que tiene distribuido distintos componentes de su aplicación por distintos dominios de seguridad (nodo servicios web, nodo extranet, intranet, internet, red SARA) y requiere del intercambio de información a través de sus componentes desplegados en diferentes dominios. En este caso la responsabilidad técnica de todos los componentes de la aplicación está bajo una misma autoridad independientemente de dónde se desplieguen.
- **Integración de** dos o más **sistemas**. En una arquitectura típica SOA se dan relaciones de uno o varios **proveedores** y uno o varios **consumidores**. En este caso la responsabilidad técnica de los componentes a desarrollar y/o adaptar corresponde a autoridades diferentes. Cuando se trate de este caso es necesario detallar qué sistemas asumen el rol de proveedor y cuáles el de consumidor.

2.6 *Disponibilidad*

Se tendrá que especificar la necesidad de disponibilidad de los servicios publicados en la Plataforma SOA, según las necesidades funcionales de la integración:

- 8x5
- 24x7
- Otras

Actualmente la Plataforma SOA tiene un soporte de 8x5 en los entornos de producción del CCEA.

2.7 *Diagrama de arquitectura de integración*

El diagrama contendrá:

- Los sistemas proveedores/consumidores y sus elementos implicados en la integración.
- Los elementos de la Plataforma SOA implicados
- Los flujos de información entre los elementos de la Plataforma SOA y los sistemas a integrar, así como sus posibles dependencias en tiempo de ejecución, como por ejemplo servidores ftp, ldap,…

A medida que se detalle el diseño de la solución, el diagrama contendrá adicionalmente la siguiente información:

- Las URLs proporcionadas por los distintos elementos implicados
- El transporte utilizado en cada una de las comunicaciones
- Los nombres de los servidores, IPs y puertos

En una fase posterior deberá completarse el diagrama con los elementos de infraestructura de red y de seguridad tales como firewalls, routers, etc.).

2.8 *Entornos*

La Plataforma SOA dispone de tres entornos: desarrollo, preproducción y producción. Se aconseja que los sistemas a integrar sigan esta misma filosofía.

El entorno de desarrollo de la plataforma SOA actualmente se encuentra disponible en la intranet.

El entorno de pre de la plataforma SOA para pruebas con componentes alojados en el nodo servicio web, en concreto los casos de uso 1, 5 y 6, solo está disponible en la intranet. Para el resto de casos en los que se requiera pruebas a través de red SARA o internet existe un entorno de pre tanto en el nodo extranet como en la intranet.

Por tanto, las pruebas de integración en estos entornos requieren que los sistemas a integrar tengan conectividad con la intranet o bien con el nodo extranet según corresponda.

En el caso de que alguno de los sistemas implicados en la integración no dispongan de alguno de los entornos (des, pre y pro) se deberá especificar en este punto.

Por otro lado también se detallará de acuerdo a la tabla más abajo los nombres de máquinas, IPs (y puertos cuando corresponda) en cada uno de los entornos. Esta tabla debe contener la información siguiente relativa tanto a proveedores y consumidores:

- Servidores alojados en internet y/o red externa al MINISDEF.

- Servidores alojados en Intranet del MINISDEF.
- Servidores alojados en nodo I*net del MINISDEF.

Aplicación/Sistema	Desarrollo	Preproducción	Producción
<nombre de la aplicación/sistema a integrar>	<Nombre cualificado de la máquina, IP, red en la que se encuentra, puertos>	<Nombre cualificado de la máquina, IP, red en la que se encuentra, puertos>	<Nombre cualificado de la máquina, IP, red en la que se encuentra, puertos>

2.9 *Cronograma estimado*

Se realizará un cronograma estimado incluyendo como mínimo las siguientes tareas:

- Desarrollo de los servicios/interfaces en cada uno de los sistemas/aplicaciones implicados
- Desarrollo y pruebas de las adaptaciones y configuraciones requeridas en la Plataforma SOA
- Identificación y gestión de recursos necesarios en elementos de infraestructura ajenos a la plataforma SOA como por ejemplo: altas de usuarios/roles en directorios corporativos, activación de puertos, certificados, etc.
- Despliegue en preproducción
- Pruebas de preproducción, incluyendo un hito final de aceptación para el paso a producción.
- Despliegue en producción y aceptación final.

En cada tarea se identificará un responsable, las partes implicadas, las dependencias y una estimación de tiempo.

Como resultado del cronograma estimado se obtendrá una fecha estimada de paso a producción.

3 REQUISITOS DE INTEGRACIÓN TÉCNICOS

A continuación se describen cada uno de los requisitos a completar con una explicación de su contenido.

3.1 *Rendimiento*

3.1.1 Número de servicios y operaciones

Se especificarán el número de servicios y el número de operaciones por cada uno de los servicios.

3.1.2 Carga estimada

Se especificará una estimación de la carga esperada, en cuanto a:

- Número de invocaciones por unidad de tiempo, invocaciones en paralelo, periodos pico media y valle.
- Volumen estimado de los mensajes intercambiados.
- En el caso de servicios que intercambian ficheros se detallará el número y volumen estimado de los ficheros.

3.2 *Seguridad*

3.2.1 Control de acceso

Se especificará si es necesario autenticar/autorizar los servicios tanto de los proveedores como de los consumidores.

En el caso que los servicios finales requieran mecanismos de autenticación, especificar cuáles son estos mecanismos y las credenciales necesarias (usuario/password, certificado digital,…). Esta autenticación se refiere a la identidad del sistema/aplicación no al usuario final.

Por otro lado especificar si es necesario autorizar a distintos consumidores a nivel de servicio y/o operación.

Además será necesario proporcionar las IPs tanto de entrada como de salida en caso que se trate de organismo externos que necesiten consumir un servicio/s del Minisdef o proveer un servicio/s al Minisdef.

3.2.2 Cifrado

El cifrado será requerido cuando se intercambien mensajes conteniendo datos con información sensible.

El cifrado de la información se podrá realizar de formas distintas:

- a nivel de transporte
- a nivel de mensaje
- una combinación de los anteriores

Se deberá especificar la opción propuesta indicando los elementos de la arquitectura responsables de cifrar y descifrar la información.

3.2.3 Auditoría

Se especificarán mecanismos para registrar la actividad de los servicios (logs), para su análisis cuando se requiera en las situaciones siguientes:

- Comportamientos no esperados en proveedores/consumidores de servicio que produzcan errores en la integración
- Contabilización de la actividad del sistema relacionada con el cumplimiento de acuerdos de nivel de servicio
- Comportamientos fraudulentos

Se deberá indicar por cada uno de los elementos de la arquitectura los requisitos de logs en lo referente a:

- Detalle de información requerido en cada invocación de servicio tales como contenido de los mensajes (petición/respuesta), tiempo de respuesta, identificación del origen de la petición,…
- Gestión de logs en línea según uno de los esquemas siguientes:
    - Periodo de retención por tiempo
    - Por tamaño máximo
- Gestión de logs en almacenamiento secundario: periodo de retención y tiempo requerido de recuperación y consulta

3.2.4 Propagación de identidad

En algunos casos será necesario propagar la identidad del consumidor del servicio al sistema/aplicación proveedor del servicio, por diferentes motivos tales como por ejemplo ajustar la lógica del servicio en función de quién es su usuario, debido a normas regulatorias, etc.

En este punto hay que distinguir dos casos:

- Se requiere la **identidad del usuario final** de aplicación, o en caso de no ser posible, algún mecanismo tal como un número de identificación único que, en caso necesario, permita al proveedor relacionar una invocación concreta de un servicio con el usuario final que la desencadenó.

- Se requiere la i**dentidad de la aplicación** consumidora del servicio de modo que la aplicación proveedora del servicio pueda distinguir cuál aplicación consume el servicio. Este caso solo aplica a aquellos servicios que sean consumidos por más de un sistema/aplicación.

De cualquier manera el proveedor del servicio debe confiar en la autenticación que realice el sistema/aplicación consumidor del servicio u otro elemento de la arquitectura de integración.

En caso de que se requiera propagar la identidad se especificará la tecnología a emplear: usernametoken, token SAML, …

3.2.5 Certificados digitales

Se especificarán los tipos de certificados requeridos indicando en cada caso:

- Propósito: para cliente o servidor, firma, cifrado, conexión SSL,…
- Qué CA lo emite: PKIDEF u otras soportadas por la infraestructura del MINISDEF

Para la emisión y uso de los certificados se seguirá la normativa vigente en el MINISDEF, supervisada por el Área de Seguridad teniendo en cuenta casos especiales en lo que se refiere a organismos ajenos al MINISDEF tales como el uso de certificados autofirmados o emitidos por otras CA's.

3.3 *Plataforma de desarrollo*

Se tendrá que especificar, tanto para consumidores como proveedores de los servicios, el entorno de desarrollo y plataforma con la que se implementan los servicios y las invocaciones. Así, se detallará en la medida de lo posible datos de los entornos implicados en la integración en lo referente a lenguajes de programación, productos, versiones, frameworks, toolkits, librerías, etc. tales como .Net, Axis, GSOAP, C++, C#, java, BIztalk, Entire-X.

3.4 *Interfaces de servicios*

3.4.1 Tecnología de servicios

Se especificará la tecnología a utilizar en la integración de las aplicaciones en lo referente a:

- Protocolo de transporte: http(s), JMS, SMTP, ftp, sftp, otros
- Protocolo de aplicación: SOAP
- Formato de los datos: XML, texto ASCII, binario…

En el caso de servicios web (SOAP sobre http(s)), la implementación de los servicios será de acuerdo a la referencia [GUIWS] "Guía de implementación de servicios Web del Minisdef".

3.4.2 *Intercambio de ficheros*

Se especificará si es necesario intercambiar ficheros entre las aplicaciones proveedoras y consumidoras del servicio.

En caso afirmativo se especificará la tecnología a utilizar: ftp, sftp, SOAP with Attachments, acceso a carpetas compartidas, …

Deberá especificarse el número y formato de los ficheros (pdf, xls, doc,..), así como el tamaño esperado y frecuencia.

3.4.3 *Tipología de mensajes*

En el caso de datos estructurados se indicará en caso necesario el formato y tamaño de los mensajes intercambiados, haciendo referencia en su caso a los documentos de especificación correspondientes.

3.5 *Plan de pruebas*

Deberá especificarse en este apartado un plan de pruebas a realizar teniendo en cuenta los siguientes aspectos:

- Lugar de ejecución de las diferentes pruebas, dependiendo de los recursos y personas implicadas. Por ejemplo: las pruebas iniciales en entorno de desarrollo podrán realizarse en ESPOL, CCOMSI, etc. sobre la intranet.
- Determinar los entornos necesarios de cada parte para hacer las pruebas como por ejemplo desarrollo, preproducción, certificación,… y la relación entre los diferentes entornos de cada una de las partes implicadas.
- Determinar en cada una de las pruebas las necesidades de conectividad: Intranet, SARA o redes de terceros, Internet,..
- Especificar el tipo de pruebas a realizar: de conectividad, de interfaz (entre dos elementos de la integración), funcionales considerando la operativa completa desde el usuario final hasta el/los sistemas proveedores, de carga.
- Especificar los datos que se van a utilizar en cada una de las prueba. En ciertos casos deberán utilizarse datos ficticios.

- Establecer los mecanismos de comunicación para coordinar la realización de las pruebas y, en particular, establecer las comunicaciones necesarias cuando alguno de los elementos de la arquitectura de integración no esté disponible, como por ejemplo: plataforma SOA, elementos de infraestructura del CCEA (ldap, conectividad en firewalls,…), servidores de aplicaciones a integrar, …
- Se deberá identificar el ciclo de pruebas para cada uno de los entornos y los hitos que irán asociados al finalizar las pruebas en cada caso. Por ejemplo: Las pruebas finalizadas satisfactoriamente en el entorno de preproducción dan lugar a la aceptación de la versión y su puesta en producción.
- Fechas estimadas para realizar las distintas pruebas, que deberán incluirse en el cronograma estimado.

Como recomendación los tipos de pruebas de interfaz a seguir en la Plataforma SOA con las aplicaciones a integrar son, en este orden:

1. Validación de la interfaz del proveedor desde un cliente genérico utilizado por Plataforma SOA como SOAPbox o SOAPUI.
2. Validación de la interfaz del proveedor provisionándolo en el elemento de la Plataforma SOA implicado (habitualmente “creación del proxy”)
3. Validación de la interfaz de la plataforma SOA desde el sistema/aplicación consumidora sin establecer políticas que afecten al interfaz como por ejemplo las de logging.
4. Validación de la interfaz de la plataforma SOA desde un cliente genérico una vez establecidas las políticas que afectan al interfaz, como por ejemplo la autenticación
5. Validación de la interfaz de la plataforma SOA desde el sistema/aplicación consumidora una vez establecidas todas las políticas del servicio.

3.6 *Monitorización de servicios*

Se especificarán mecanismos de monitorización técnica de los servicios, para hacer efectivo en su caso la vigilancia de acuerdos de nivel de servicio, tales como:

- Identificar mecanismos para detección de pérdida de servicio.
- Identificar mecanismos para detección de tiempos de respuesta que sobrepasen los umbrales acordados.

4 RESPONSABILIDADES Y GESTIÓN DE CAMBIOS

4.1 *Roles y responsabilidades*

Se deberán especificar los puntos de contacto de cada una de las partes implicadas, tanto responsables como técnicos.

Se distinguen los roles siguientes:

1. Responsable funcional: Responsable de la integración desde un punto de vista funcional, normalmente de un área de desarrollo y/o un departamento usuario del sistema.
2. Responsable de Arquitectura: Define la arquitectura en relación con los elementos de la Plataforma SOA.
3. Responsable de Explotación: Gestiona los recursos del CCEA en cualquiera de sus dominios de seguridad.
4. Responsable de Seguridad: Valida los requisitos de seguridad de la integración.
5. Responsable de sistema/aplicación a integrar (consumidor o proveedor). Gestiona recursos de desarrollo, configuración, pruebas,… en los sistemas a integrar. En una integración que participan varios sistemas deberá designarse al menos un responsable por cada sistema.
6. Coordinador con organismos. Se establece esta figura cuando el responsable funcional es de un organismo del MINISDEF ajeno a la SDGTIC.

A continuación se describen las responsabilidades de cada una los roles indicados:

1. Responsable funcional:
   - Gestionar los recursos de desarrollo y pruebas necesarios en cada una de los sistemas/aplicaciones a integrar en colaboración con los responsables de sistema/aplicación.
   - Velar porque los trabajos a realizar en los sistemas/aplicaciones a integrar cumplan con los requisitos y se ejecuten en tiempo.
   - Validar los resultados de las pruebas de integración.
   - Punto de contacto con las empresas u organismos ajenos al Minisdef implicados en la integración.
   - Solicitar a organismos ajenos al MINISDEF la información necesaria para la integración, además de comunicarles los requisitos tecnológicos y de seguridad del MINISDEF.

2. Responsable de Arquitectura:

- Definición de la arquitectura de integración.
- Planificación y seguimiento completo de la integración
- Asesoramiento técnico a responsables de sistema/aplicación y a responsable funcional sobre la solución adoptada.
- Gestionar el impacto y la relación que pueda tener la integración con la Plataforma SOA y otras integraciones (visión completa de las integraciones en curso).
- Validación técnica de los interfaces de servicio de los sistemas/aplicaciones a integrar y apoyo en su especificación cuando se requiera.
- Coordinar las pruebas en los distintos entornos.
- Gestión de la comunicación con las partes implicadas, como por ejemplo incidencias, retrasos sobre planificación, reporte del estado de los trabajos, etc.
- Aprobar cualquier cambio sobre la arquitectura de integración acordada en colaboración con el Responsable de Explotación.

3. Responsable de Explotación:

- Proporcionar una plataforma estable, tanto para pruebas en preproducción, como para el paso a explotación.
- Validar que los requisitos son compatibles con los elementos de infraestructura disponibles en el CCEA.
- Completar el diagrama de arquitectura de integración con los elementos de infraestructura de red y de seguridad tales como firewalls, routers, etc.
- Gestionar la configuración de los elementos de infraestructura de CCEA necesarios para la arquitectura de integración propuesta, como por ejemplo habilitar puertos, alta en ldap, etc.
- Durante la fase de pruebas, monitorizar los elementos de plataforma implicados y proporcionar a las partes implicadas los datos de monitorización requeridos para solucionar los problemas detectados.
- Proporcionar en caso requerido espacio y recursos (como mínimo un punto de acceso a la intranet) en las instalaciones del CCEA para pruebas en el entorno de preproducción.
- Realizar el paso a explotación apoyado por responsable de arquitectura y responsables de sistema.

4. Responsable de Seguridad:

- Validar que la Arquitectura propuesta cumple con la normativa de seguridad y en caso contrario recomendar alternativas.
- Asesoramiento técnico en tecnologías de seguridad implicadas en la solución.

- Apoyar en la gestión de los recursos requeridos de la PKI de Defensa y PSSDEF.

5. Responsable de sistema/aplicación:
   - Implementar los trabajos relativos a la integración de acuerdo a lo que se ha establecido en los requisitos de integración.
   - Comunicar a todas las partes cualquier problema o retraso relacionado con el desarrollo o adaptación de los servicios requeridos para la integración.
   - Comunicar a todas las partes cualquier cambio en el interfaz de los servicios o nuevos requisitos.
   - Realizar las pruebas y/o apoyar al responsable funcional en su ejecución.

6. Coordinador:
   - Coordinar los aspectos administrativos entre la SDGTIC y los organismos del MINISDEF ajenos a la SDGTIC.
   - En caso requerido redactar el acuerdo de nivel de servicio a suscribir por las partes implicadas.

Cada uno de los roles puede ser asumido por una o más personas, que deberán ser especificadas en una tabla del tipo:

Área/Sistema/ Organismo	Nombre y apellidos	e-mail	Tfno.	Rol en la integración	Responsabilidades

En caso necesario, en esta tabla se añadirán responsabilidades específicas de la integración no contempladas en esta guía.

4.2 *Documento de requisitos de integración*

Para la elaboración y aprobación del documento de requisitos de integración se seguirán las normas siguientes:

1. La **creación** del documento
   a. La edición del documento corresponde al Responsable de Arquitectura

b. El responsable funcional completará los apartados correspondientes a funcionalidad del sistema, necesidades de integración, disponibilidad, número de servicios y operaciones, carga estimada y plataforma de desarrollo. Adicionalmente, y en su ámbito de responsabilidad, deberá completar los apartados referidos a entornos, cronograma estimado, , plan de pruebas y tabla de POCs/ responsabilidades.

c. El responsable de Explotación completará en su ámbito de responsabilidad los apartados correspondientes a diagrama de arquitectura, cronograma estimado, plan de Pruebas, monitorización de servicios y tabla de POCs/responsabilidades.

d. El responsable de Seguridad completará en su ámbito de responsabilidad la tabla de POCs/responsabilidades.

e. Los responsables de sistema/aplicación aportarán la información necesaria a requerimiento del Responsable Funcional y el Responsable de Arquitectura.

2. La **aprobación** del documento de requisitos de integración corresponde a Responsable de Explotación, Responsable de Arquitectura, Responsable funcional y Responsable de Seguridad quienes la harán efectiva firmando digitalmente el documento en formato pdf.

3. El **control de versiones** corresponde al Responsable de Arquitectura

4. Para realizar **cambios** al documento una vez aprobada una versión se aplicará el procedimiento de gestión de cambios especificado en el apartado siguiente que afecta no sólo al documento sino a toda la integración.

5. Para la **comunicación** entre las partes interesadas se utilizará preferentemente el correo electrónico. No descartándose a futuro la utilización de otras herramientas colaborativas adaptadas.

4.3 *Procedimiento de gestión de cambios*

Una vez aprobada una versión inicial del documento de requisitos de integración, se seguirá el siguiente procedimiento para gestionar cambios en la integración:

1) Aparece una petición de cambio por parte de alguna de las partes implicadas. Ej: cambios en un interfaz de servicio, cambios en protocolos de transporte o puertos, necesidad de pruebas en un determinado entorno,…

2) Las peticiones de cambio se canalizan a través del Responsable de Arquitectura. Todas las peticiones se registrarán formalmente, y se evaluará su impacto a la vista de la arquitectura de integración y de las decisiones de diseño particulares de cada integración que se tomaron en su día.

3) Los cambios que afecten a la infraestructura desplegada en explotación serán evaluados y validados por el Responsable de Explotación. Por ejemplo: Instalar un elemento nuevo de infraestructura.

4) En la resolución se distinguen dos vías:

   a. Si el cambio es rechazado, el Responsable de Arquitectura informará a la parte interesada justificando la resolución.
   b. Si el cambio es aceptado, el Responsable de Arquitectura planificará la ejecución del cambio y coordinará a las partes interesadas. Asimismo, se valorará la edición de una nueva versión del documento de requisitos de integración que deberá ser aprobada.

5) En el seguimiento del cambio, distinguimos dos vías:

   a. Si el cambio afecta al entorno de explotación es su Responsable quien efectúa el seguimiento de la acción manteniendo informado al Responsable de Arquitectura y al originario de la petición de cambio.

   b. Si el cambio afecta a otro entorno es el responsable de dicho entorno quien efectúa el seguimiento manteniendo informado al originario de la petición de cambio y al Responsable de Arquitectura que valorará su comunicación a otras partes interesadas.

Una vez que los técnicos estén trabajando en la implementación de un cambio podrán comunicarse directamente, informando a sus responsables sólo de aquellos aspectos que modifiquen el cambio original. En este último caso se resolverá como una nueva petición de cambio.