# Pautas de Desarrollo de Integración

A continuación se describen las pautas para el desarrollo de los servicios que se deberán seguir para la correcta implementación de la arquitectura orientada a servicio que se quiere alcanzar en el SAS. Estas pautas pretenden aumentar el grado de interoperabilidad de los sistemas de información y la capacidad de atender de forma más eficiente los procesos de negocio, además de agilizar el desarrollo de nuevos servicios y el uso de los existentes.

## Tecnología de Comunicación

La mayoría de las implementaciones SOA están basadas en tecnologías de Servicios Web. Esta tecnología ha alcanzado un grado de madurez suficiente para que pueda ser considerado como elemento principal de comunicación en la estrategia de integración de la STIC. Teniendo en cuenta esta premisa, todas las especificaciones y normas se han definido para que sean lo más abiertas y transparentes posible a cualquier otro tipo de comunicación.

La Norma de la STIC se puede resumir en:

| Pautas | Carácter | Observaciones |
|---|---|---|
| Modelo SOA | Permitido | La OTI estudiará y determinará aquellas integraciones que deban de cumplir este modelo. |
| Modelo REST | Permitido | La OTI estudiará y determinará aquellas integraciones que deban de cumplir este modelo. |
| Modelo RPC | No Permitido | |
| Contract-first | Obligatorio | Se realiza primero la definición del servicio y luego se desarrolla. |
| Code-first | No Permitido | |
| Estilo document/literal | Permitido | |
| Estilo RPC/Encoded, RPC/literal | No Permitido | |

## Reglas de Codificación

En el siguiente apartado se describen un conjunto de reglas de codificación que deberán seguir el desarrollo de los servicios necesarios.

| Pautas | Carácter | Observaciones |
|---|---|---|
| Codificación con UTF-8 | Obligatorio | |
| Codificación de los namespaces | Obligatorio | Esto aplica a los servicios SOAP |

Todos los documentos asociados a la definición de un servicio (WSDLs, esquemas XSD (http://www.w3.org/XML/Schema), etc.) deberán estar codificados en UTF-8.

La definición de los namespaces dentro de los servicios es un tema muy importante a tener en cuenta. Una correcta definición de los mismos favorece la reutilización y catalogación de los servicios, da soporte a los procesos de versionado y posibilita la creación de cierto tipo de servicios horizontales de enrutación y mediación.

## Estándares de Mensajería

El uso de un estándar de mensajería nos permite disponer de una semántica común para el intercambio de datos entre los distintos sistemas. Por este motivo, nos ceñimos al estándar HL7 en su versión 2.5, tanto en formato XML como en formato plano ER7, HL7 FHIR Release 4 y HL7 CDA para las comunicaciones entre los distintos sistemas sanitarios.

Para negocios no contemplados por HL7 se estudiará si hay estándares aplicables y de lo contrario, la OTI realizará la definición que más se adecue a la necesidad.

En el caso de HL7 v2.5, se establece como prioritario el formato XML (http://www.w3.org/XML/) para toda la nueva mensajería que se defina para el catálogo de servicios. Se establecen los trabajos necesarios para pasar la mensajería creada hasta la fecha en texto plano, a formato XML, en coordinación con los sistemas de información impactados por estar enviando o recibiendo mensajería en formato texto plano. En próximas versiones de este documento se establecerá como único formato válido el XML, quedando prohibido a partir de ese momento el formato texto plano. El calendario de validez de la mensajería corporativa en formato texto plano vendrá marcada por la STIC y será anunciada convenientemente en este espacio.

En el caso de HL7 FHIR, se establece como prioritario el formato JSON para toda la nueva mensajería que se defina para el catálogo de servicios.

Para las invocaciones REST se debe respetar el protocolo HTTP donde el método (GET, POST, PUT, PATCH, DELETE) tiene un significado específico. Otros métodos que se utilizan son OPTIONS y HEAD. Una API debe proveer un mensaje de error útil en un formato conocido. La representación de un error debe no ser diferente a la representación de cualquier recurso, con su propio set de campos.

En cuanto al filtrado y la búsqueda de resultados, se debe mantener la URL base de recursos tan simple como sea posible. Se debe tener en cuenta lo siguiente:

- Un parámetro de búsqueda siempre debe estar contemplado en la definición del recurso como atributo.
- Los valores permitidos dentro de un filtro deben corresponderse con los establecidos en la definición.

## Trazabilidad de Mensajes

La identificación de los mensajes y *endpoints* involucrados en los procesos de comunicación, es un elemento esencial a la hora de realizar procesos de auditoría, monitorización, detección de duplicados, etc. Además, estos mismos elementos posibilitan la creación de un gran número de procesos de enrutamiento y mediación basados en los mismos.

De esta manera los mensajes utilizados en todos los puntos de comunicación vendrán provistos de una cabecera la cual incluirá un identificador único que garantizará una correlación entre todos los puntos por los que viaja el mensaje. Este campo, para el caso de la mensajería en HL7, es el MSH.10 del segmento de cabecera MSH.

## Control y Unicidad de Mensajes

En relación al control de unicidad de la mensajería, cada mensaje está identificado de manera única con un identificador de mensaje en un nodo de la cabecera. Independientemente de que el envío de un mensaje se intente un número de veces, ese identificador no debe variar en todos los intentos de entrega.

Este requerimiento no es trivial y debe ser tenido en cuenta por cada sistema participante en el circuito de envío y recepción de la mensajería, no solo por el ESB corporativo. Todos los sistemas susceptibles de reenviar un mensaje deben garantizar la unicidad del mismo, y todos los sistemas susceptibles de recibir un mensaje deben garantizar la unicidad de su procesamiento. Esto hace que el ESB deba garantizar ambas condiciones, pero también que todos los sistemas que interactúan con él deben garantizar una u otra condición en función de si son emisores o receptores de mensajería.

Un ejemplo de la casuística que puede darse es el de los timeouts en la entrega de un mensaje que, sin embargo, termina alcanzando el destino. Este caso implica un error previo en la definición del timeout, en su configuración, o en el rendimiento puntual de las comunicaciones. En cualquier caso, cuando el sistema emisor vuelva a intentar entregar ese mensaje, dado que se trata del mismo hecho de negocio, debe informar el mismo identificador de mensaje. De esta forma el ESB puede identificar si el mensaje que recibe en el segundo intento ya ha sido procesado previamente y puede descartarlo, evitando así que llegue dos veces a ningún destino, y evitando así provocar un error de integridad de datos. Del mismo modo un sistema que reciba mensajería del ESB debe tener en cuenta que puede darse una casuística similar, por lo que debe evitar procesar dos veces el mismo mensaje.

Se establecen las siguientes pautas de cumplimiento obligatorio para todos los sistemas en el consumo y publicación de servicios con el ESB corporativo:

- Todos los sistemas que envíen un mensaje al ESB deben garantizar que en caso de reenviar ese mensaje al ESB, el identificador del mensaje que se informa en la cabecera del mismo es único.
- El ESB garantiza que no procesará dos veces un mismo mensaje (es decir, no procesará un mensaje con un identificador de mensaje ya procesado).
- Todos los sistemas que reciban un mensaje desde el ESB deben garantizar que no procesan dos veces el mismo mensaje (es decir, que no procesará un mensaje con un identificador de mensaje ya procesado).
- Además, es obligatorio incluir en los planes de pruebas funcionales estos escenarios entre los casos de uso de error, para garantizar que de producirse esos timeouts en producción, ningún mensaje va a ser procesado más de una vez.

Por otro lado, para los servicios definidos sobre el estándar HL7 FHIR se debe realizar un control y gestión de versionado.

## Tiempos de respuesta de los servicios

Los tiempos de respuesta relacionados con los servicios deben cumplir con los siguientes requerimientos:

**Servicios SOAP:**

- Servicios **asíncronos**: Al tener que limitarse sólo a devolver el acuse de recepción del mensaje, deben de ofrecer una respuesta inferior a 500ms.
- Servicios **síncronos**: Debido a que los servicios de esta tipología requieren de un procesamiento, el destino debe responder en menos de un 1 segundo al 80% de los mensajes y en menos de 2 segundos en el 20% restante.

**Servicios REST:**

- Este modelo requiere que los tiempos de respuesta sean lo más óptimos posibles, ya que es habitual se puedan lanzar varias llamadas para obtener la información que requiere el origen. Por lo tanto, cada una de estas llamadas rest debe ser inferior a 300ms.

## Seguridad

La seguridad en las comunicaciones, es un elemento muy importante a tener en cuenta a la hora de diseñar un servicio. Los mecanismos de seguridad, además de garantizar la integridad, no repudio y confidencialidad de los mensajes, permiten habilitar mecanismos para la identificación y autorización de servicios y usuarios.

Este documento no fija que elementos de seguridad debe implementar un servicio, según que casos o escenarios, sólo da las guías y pautas a seguir para implementar y publicar estos elementos de seguridad dentro del SAS.

La siguiente tabla muestra un resumen de los elementos de seguridad esenciales y su recomendación dentro de la STIC.

| Elemento | Mecanismo Seguridad | Carácter | Comentario |
|---|---|---|---|
| Autenticación de Servicios | HTTP Basic Autentication | No recomendado | |
| | SSL X.509 Certificate | Recomendado | Permitido en entornos cerrados, con consumidores conocidos, siempre y cuando exista conexión directa entre todos los participantes. |
| | WS-Security Tokens | Recomendado | |
| Autenticación Usuarios | SAML | Recomendado | |
| Integridad | SSL | Recomendado | Permitido en entornos cerrados, siempre y cuando exista conexión directa entre todos los participantes. |
| | WS-Security (WS-Signature) | Recomendado | |
| Confidencialidad | SSL | Recomendado | Permitido en entornos cerrados, siempre y cuando exista conexión directa entre todos los participantes. |
| | WS-Security (WS-Encrypt) | Recomendado | |