

Procesado de Mensajería

- [Publicación de servicios:](#)
- [Envío de mensajería:](#)
 - [Envío Asíncrono:](#)
 - [Envío Síncrono:](#)
- [Recepción de mensajería:](#)
 - [Recepción Asíncrona:](#)
 - [1ª Fase: la respuesta de ACK/NACK:](#)
 - [2ª fase: el procesamiento del mensaje:](#)
 - [Recepción Síncrona:](#)
- [Validación del tique de Maco:](#)

A continuación se detallan, a nivel conceptual, los pasos a realizar por las aplicaciones para la correcta publicación y consumo de los servicios y el correcto procesado de la mensajería tanto que envían como que reciben.

Publicación de servicios:

Tal y como se especifica en la **Normativa de Seguridad publicada por la Unidad de Seguridad TIC (USTIC) al respecto de los requisitos de seguridad web** y que se puede encontrar en este [enlace](#):

- Para la comunicación entre el servicio web y el usuario hay que cifrar siempre los canales de comunicación mediante TLS, que es un protocolo criptográfico que permite cifrar los canales de comunicación. Este protocolo, aplica privacidad, autenticación e integridad de datos como propiedades del canal de comunicación. La versión mínima debe ser TLS 1.2 y además hay que evitar utilizar algoritmos y protocolos criptográficos que tengan debilidades significativas conocidas o que sean insuficientes para los requisitos de seguridad actuales.
- Para la comunicación con otras aplicaciones y/o servicios web, emplear una criptografía robusta como en el punto anterior, es decir, TLS 1.2 o superior con algoritmos y protocolos sin debilidades, sea cual sea el método o protocolo utilizado, por ejemplo, HTTPS o FTPS.

Es decir, todas las publicaciones de servicios de interoperabilidad independientemente del protocolo o estándar utilizado, deben emplear como mínimo TLS 1.2. Esto implica que **todos los servicios web tanto SOAP como REST** que utilizan el protocolo HTTP se deben publicar mediante **HTTPS**, siguiendo las directrices indicadas por la USTIC.

Envío de mensajería:

Envío Asíncrono:

1. Evento
2. Construcción del mensaje con tique de MACO incluido asegurando que la fecha del mensaje es posterior a la del tique
3. Mirar en la configuración a qué cola corresponde en función del tipo de mensaje (censo, demográfico, citas, ...) y el AH
4. Colocar el mensaje en la cola correspondiente
5. El proceso que va leyendo de la cola obtiene el primer elemento de la cola (el más antiguo), consulta la configuración para obtener la url a dónde enviarlo así como el tiempo que va a estar reintentando en caso de timeout y el intervalo de espera entre reintentos
6. Envía el mensaje a la url obtenida en el paso 5
7. Si no obtenemos ack/nack reintentamos durante el tiempo obtenido por configuración en el paso 5 esperando el intervalo correspondiente sin pasar al siguiente mensaje. Si se supera el tiempo que tiene que estar reintentando, se coloca el mensaje en la cola de histórico marcándolo con error sin respuesta. Estos mensajes que no se han podido entregar deben poder ser enviados de forma manual.
8. Cuando obtiene el ack/nack coloca el mensaje junto con el ack/nack en una cola jms para pasar a histórico a título de auditoría
9. El proceso que va leyendo de la cola pasa al siguiente elemento

Aconsejamos que el tiempo de intento de entrega para cada cola sea alto, de varias horas, incluso días, para no desordenar mensajes en caso de indisponibilidad. Eso no quiere decir que tarde todo ese tiempo en llegar los mensajes, sino que tenemos garantía de que en caso de problemas no van a descartarse mensajes hasta que se solucione la incidencia. En condiciones normales esa incidencia debe llegar por diferentes alertas entre otras la monitorización de esas colas y se debe detectar casi de inmediato y debe quedar resuelto en pocos minutos o pocas horas en función de la gravedad. Pero cuando se resuelva se tiene garantía que la mensajería se entrega en orden a todos los destinos incluidas las departamentales.

El tiempo real de procesamiento de mensajes en condiciones normales es tan bajo que no se introduce ningún retraso a pesar de que por cada cola se entreguen los mensajes secuencializados de 1 en 1 por colas en función del ámbito.

Aconsejamos que la separación se haga por contextos donde la mensajería sea dependiente y pueda paralelizarse con otras colas sin que importe el orden entre ambas, por ejemplo, para el caso hospitalario se podría hacer por ámbitos y áreas hospitalarias, es decir, Censo-VVVictoria, Citas-VVVictoria, G.Errores-VVVictoria, Censo-VRocio, Citas-VRocio, G.Errores-VRocio, ...

La distribución de las colas debe estar por configuración, permitiéndose parametrizar y poder ampliar o reducir el número de colas fácilmente.

Envío Síncrono:

1. Evento
2. Construcción del mensaje con tique de MACO incluido asegurando que la fecha del mensaje es posterior a la del tique
3. Se envía el mensaje sin usar colas y nos mantenemos a la espera de respuesta
4. Obtenemos la respuesta y la procesamos.
5. Colocamos el mensaje junto con la respuesta en una cola jms de forma asíncrona para pasar a histórico a título de auditoría

Recepción de mensajería:

Recepción Asíncrona:

Se divide en 2 fases:

1ª Fase: la respuesta de ACK/NACK:

1. Llega el mensaje
2. Validación sintáctica y [tique](#) (para comprobar la fecha del tique se hace contra la fecha del mensaje NUNC A contra la del sistema)
 - 2.1 Si NO OK se devuelve NACK
 - 2.2 Si OK intentamos poner el mensaje en la cola de procesamiento del ámbito correspondiente (censo, demográfico, citas, ...)
 - 2.2.1 Si OK se devuelve ACK al ESB
 - 2.2.2 Si NO OK (error interno o similar que no nos permita encolar el mensaje) se devuelve un SOAP Fault
3. Colocamos el mensaje junto con la respuesta en una cola jms de forma asíncrona para pasar a histórico a título de auditoría

Al igual que antes, aconsejamos que la separación se haga por contextos donde la mensajería sea dependiente y pueda paralelizarse con otras colas sin que importe el orden entre ambas, por ejemplo, para el caso hospitalario se podría hacer por ámbitos y áreas hospitalarias, es decir, Censo-VVictoria, Citas-VVictoria, G. Errores-VVictoria, Censo-VRocio, Citas-VRocio, G. Errores-VRocio, ...

La distribución de las colas debe estar por configuración, permitiéndose parametrizar y poder ampliar o reducir el número de colas fácilmente.

2ª fase: el procesamiento del mensaje:

4. Si hay elementos en la cola de procesamiento, cogemos el primer elemento
 - 4.1 Si el GUID ya está registrado como procesado no hacemos nada con él
 - 4.2 Si el GUID NO está registrado como procesado
 - 4.2.1 Procesar el mensaje
 - 4.2.2 Si se detecta un error de negocio, notificar el error por el S067 (ver proceso de envío asíncrono)
 - 4.2.3 Registrar el GUID como procesado
 - 4.3 volver al paso 4

Recepción Síncrona:

1. Llega el mensaje
2. Validación sintáctica y [tique](#)
 - 2.1 Si NO OK se devuelve error en el formato del servicio de respuesta síncrono concreto
 - 2.2 Si OK intentamos procesar el mensaje
 - 2.2.1 Si OK se devuelve la respuesta en el formato del servicio de respuesta síncrono concreto
 - 2.2.2 Si NO OK (error interno o similar) se devuelve error comprensible por el usuario en el formato del servicio de respuesta síncrono concreto.
3. Colocamos el mensaje junto con la respuesta en una cola jms de forma asíncrona para pasar a histórico a título de auditoría

En cualquiera de los casos, los detalles técnicos de la configuración de Weblogic y los servidores JMS se hará teniendo en cuenta el criterio de **Sistemas** y las directrices de **Arquitectura**.

Validación del tique de Maco:

La validación del ticket de MACO se realiza en los sistemas de destino de las transacciones. Esta validación del ticket de MACO implica tres acciones una vez se recibe el ticket en el sistema de destino:

1. Validar que el ticket y la firma son correctos.

El tique y firma que viaja en el mensaje se valida mediante un algoritmo en local, que se basa en generar un MD5 del tique, se decodifica la firma con la clave pública de Maco y se comparan ambos hashes, si coinciden el tique no ha sido modificado desde que lo creó Maco y podemos confiar en él. Esto se hace sin necesidad de invocar a sistemas externos.

2. Con la certeza de que el tique no ha sido alterado, pasamos a validar la fecha que se incluye en el ticket.

Dependiendo de la tipología del mensaje, la validación de la fecha se debe hacer con la fecha de creación del mensaje, para los servicios asíncronos, o con la fecha del sistema, para los servicios síncronos. En ambas casuísticas la diferencia entre las fechas con respecto a la del tique debe ser menor de 24 horas, siendo la fecha del tique siempre la más antigua.

3. Validar que el tique dispone de la operación permitida sobre el servicio al que se está invocando.

De esta forma validamos que el operador dispone de permisos para realizar la operacion sobre ese servicio.

En caso de incumplimiento de cualquiera de las validaciones indicadas en los puntos anteriores, el sistema destino, debe notificar al origen el error con una descripción precisa.