Junta de Andalucía

Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa
Agencia Digital de Andalucía

Dirección General de Estrategia Digital

Financiado por la Unión Europea

# Política de seguridad para interoperabilidad de servicios

Oficina Técnica de Interoperabilidad

## HOJA DE CONTROL DEL DOCUMENTO

| Información del Documento | | | |
|---|---|---|---|
| **Título** | Política de seguridad para interoperabilidad de servicios | | |
| **Asunto** | Oficina Técnica de Interoperabilidad | | |
| **Nombre del fichero** | DGED_SEG_Politica Seguridad de Servicios de Interoperabilidad_v01r05.odt | | |
| | | | |
| **Versión** | <v01r05> | **Fecha versión** | 12/09/2024 |
| | | **N.º Total Páginas** | 49 |

| Control de Versiones | | | |
|---|---|---|---|
| **Versión** | **Descripción de los cambios** | **Elaborado por** | **Fecha Elaboración** |
| v01r00 | Elaboración inicial del documento | OT-I | 29/03/17 |
| V01r01 | Revisión y ajuste de formato | OT-I | 18/11/20 |
| V01r02 | Ajuste de formato e inclusión de apartados: Objeto, alcance, normativas y buenas prácticas. | OT-I | 20/01/21 |
| V01r03 | Adaptación a la nueva plantilla | OT-I | 08/02/2021 |
| V01r04 | Adaptación del documento al ENS | OT-I | 01/12/2021 |
| V01r05 | Actualización encabezamiento y pie a la nueva versión | OT-I | 12/09/2024 |

| Lista de Distribución | |
|---|---|
| **Apellidos, Nombre** | **Cargo / Función** |
| | |
| | |
| | |
| | |
| | |

## ÍNDICE

# 1. INTRODUCCIÓN Y OBJETIVOS

El presente documento contiene información relativa a las políticas de seguridad de acuerdo al Esquema Nacional de Seguridad, en adelante ENS, en el que se fija el marco de actuación necesario con el objetivo de proteger la información y los recursos de información dispuestos y/o utilizados por la Consejería de Presidencia, Administración Pública e Interior de la Junta de Andalucía (CPAI en adelante), en concreto se definen:

- Los objetivos o misión de la organización.
- El marco legal y regulatorio en el que se desarrollarán las actividades.
- Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Además en concreto en la Oficina Técnica de Interoperabilidad, en adelante OT-I, para garantizar la calidad de los servicios de interoperabilidad, el presente documento describe cuáles son las políticas de seguridad que se deberán aplicar en el diseño e implementación de los servicios web para que sean conformes a las normas definidas.

Cuando utilizamos servicios web, la información que enviamos debe pasar por uno o más nodos intermedios, donde cada uno de ellos pueden leer y/o alterar la información que se envía. Debido a esto, es necesario evitar que alguien que no sea el destinatario deseado lea información confidencial, a fin de evitar la suplantación o que alguien que no sea el remitente deseado envíe mensajes.

Las especificaciones de servicios web no establecen cómo proteger los mensajes que se envían ni tampoco cómo proteger el canal por el que se realiza la comunicación. Esto implica que se requiera el uso de otros estándares o mecanismos que ayuden a preservar la integridad y confidencialidad de los mensajes.

De este modo, como objetivos básicos a cubrir por la seguridad de un servicio web, debemos tener en cuenta lo siguiente:

- Es necesario asegurar que existe una autenticación mutua entre el cliente que accede a los servicios web y el proveedor de dichos servicios.
- Se debe mantener una política de autorización del acceso a recursos y, más importante, a operaciones y procesos en un entorno en el que debe administrarse y controlarse el acceso de clientes, proveedores, vendedores, competidores y los posibles ataques que reciban de personal externo.
- Mantener al cliente identificado, de manera que se identifique una sola vez y pueda acceder a servicios en diversos sistemas, sin que resulte necesario identificarse nuevamente en cada uno de ellos.
- Controlar y asegurar la confidencialidad de los datos intercambiados, ya que por ejemplo SOAP no es capaz de cifrar la información, la cual viaja en claro a través de la red. Es necesario asegurar la comunicación con algún estándar que permita crear un canal seguro de comunicación. El estándar ya firmemente establecido de creación de canales seguros SSL y el cifrado de partes específicas de documentos mediante el cifrado XML son las direcciones que se están siguiendo en este terreno.
- Se debe asegurar la integridad de los datos, de manera que estén protegidos a los posibles ataques o a manipulaciones fortuitas. En este campo se está utilizando el estándar de firmas XMLDSIG, que permiten la firma de partes específicas del documento XML.
- Comprobar que no se repudian las operaciones, para lo cual es necesario mantener firmas en XML.

## 1.1. Alcance

Este procedimiento va dirigido a todo el personal con responsabilidades en la toma de decisiones dentro de cada ámbito de actuación que se defina en el documento.

- Directores de proyectos, que han de velar por el conocimiento y puesta en práctica de la normativa por parte de los equipos de desarrollo.
- Equipo de desarrollo, que ha de cumplir las normas aquí presentadas.

- Equipo de explotación, que ha de gestionar y administrar los componentes software objeto de este documento.
- Equipo de Interoperabilidad, responsable de la Plataforma y del gobierno de la interoperabilidad.

El **ámbito de aplicación es la Dirección General de Estrategia Digital de la Consejería de Presidencia, Administración Pública e Interior**, siendo una recomendación fuera de este contexto.

## 1.2. Condiciones de Uso

Las normas recogidas en esta guía son de **obligado cumplimiento**, dentro del alcance especificado. La OT-I de CPAI, se reserva el derecho a la modificación de la norma sin previo aviso, tras lo cual, notificará del cambio a los actores implicados para su adopción inmediata. La OT-I podrá estudiar los casos excepcionales, en el caso de que algún actor considere necesario el incumplimiento de alguna de las normas y/o recomendaciones, deberá aportar previamente la correspondiente justificación fehacientemente documentada de la solución alternativa propuesta, así como toda aquella documentación que le sea requerida para proceder a su validación técnica.

Tras el análisis de la información aportada, la OT-I informará de manera explícita sobre las conclusiones obtenidas para lograr encontrar una solución adaptada en la medida de lo posible a las directrices marcadas.

# 2. POLÍTICAS DE SEGURIDAD DE ACUERDO AL ENS

## 2.1. Marco legal y regulatorio en el se desempeñan las actividades

La política de seguridad es un concepto que abarca un conjunto de normas, que en muchas ocasiones de forma voluntaria, se adhiere a una organización con el fin de mejorar los procesos y garantizar un mayor nivel de protección, minimizando y conociendo los riesgos con los que se puede encontrar. El marco normativo en el que se desarrollan las actividades y, en particular, la prestación de los servicios electrónicos a los ciudadanos, está integrado por las siguientes normas:

### 2.1.1. Legislación aplicable

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD).
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Y su modificación en el Real Decreto 951/2015, de 23 de octubre.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD).

- Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.
- Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC.
- Resolución de 27 de septiembre 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía.
- Cualquier otra legislación de interés como las restantes normas aplicables a la Administración Electrónica derivadas de las anteriores y que puedan estar comprendidas dentro del ámbito de aplicación de esta Política de Seguridad, así como las referidas a la adopción de medidas para la protección de los activos TIC y de información que se rige, entre otras, por la siguiente normativa técnica:
  - Guías CCN-STIC y demás recomendaciones elaboradas por el Centro Criptológico Nacional.
  - La serie de normas ISO/IEC 27000, especialmente las normas ISO 27001 e ISO 27002.

## 2.2. Organización y gestión para la seguridad de los sistemas TIC

### 2.2.1. Estructura TIC del sistema

Las organizaciones, públicas o privadas, suelen diferenciar entre una Alta Dirección y una serie de Unidades Operativas o Departamentos. Cada Departamento tiene un responsable que informa a la Alta Dirección. Los Departamentos pueden disponer de recursos TIC propios, para sus usuarios, o limitarse a utilizar los servicios TIC horizontales, habitualmente encuadrados en su propio Departamento. Los servicios horizontales son también empleados por los diferentes usuarios. En la figura 1, se obserba un esquema con la estructura TIC del sistema:

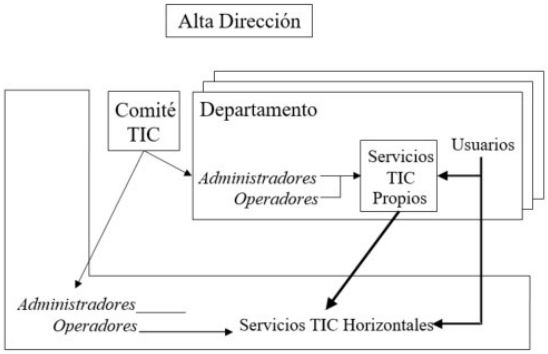


**Figura 1**. Estructura TIC del sistema, recuperado de GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-402)

#### 2.2.1.1. Comité TIC

Resulta conveniente coordinar las actividades TIC por medio de un Comité específico en el que:

- Se coordinan adquisiciones y desarrollos, decidiendo inversiones y controlando el gasto.
- Se coordinan servicios para evitar disfunciones y maximizar el uso.
- Este Comité no es técnico, pero recaba del personal técnico de los Departamentos la información pertinente para tomar decisiones.

El Comité TIC delega en una red de administradores y operadores TIC las tareas decididas:

- Los administradores se encargan de la instalación y configuración de aplicaciones, equipos y comunicaciones
- Los operadores se encargan de la operación continua de los servicios TIC.

### 2.2.2. Organización de seguridad

La Organización de la Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) está constituida por las autoridades responsables del establecimiento y aplicación de los procedimientos y normas STIC en el sistema.

Dentro de cada Organización STIC se establecen dos tipos fundamentales de estructuras:

- **Estructura de Operación STIC:** responsable de la implementación y mantenimiento de los requisitos de seguridad aprobados para el Sistema por la Alta Dirección. Está formada por:
  - Administradores STIC, son los responsables de la implantación, configuración y mantenimiento de los servicios de seguridad relacionados con las TIC.

  - Operadores STIC, son los responsables de la operación diaria de los servicios de seguridad relacionados con las TIC.
  - Usuarios de los sistemas, se relacionan con los servicios TIC para cumplir sus obligaciones laborales. Son el personal autorizado para acceder al Sistema utilizando las posibilidades que les ofrece el mismo. Juegan un papel fundamental en el mantenimiento de la seguridad del Sistema, por lo tanto, es fundamental su concienciación en la seguridad de las TIC ya que en la mayoría de los casos constituyen voluntariamente o involuntariamente la principal amenaza para el propio Sistema.

- **Estructura de Supervisión STIC:** responsable de establecer y aprobar los requisitos de seguridad para el Sistema además de verificar y supervisar la correcta implementación y mantenimiento de los mismos.

  Está formado por:

- Alta dirección,
  a) Responsable de que la Organización alcance sus objetivos a corto, medio y largo plazo.
  b) Respalda explícita y notoriamente las actividades STIC en la Organización.
  c) Expresa sus inquietudes al Comité de Seguridad Corporativa a través del Responsable de Seguridad Corporativa.
  d) Aprueba la Política de Seguridad de la Organización y los presupuestos presentados por el Comité de Seguridad Corporativa cuando sobrepasen una cantidad determinada.

- Comité se seguridad corporativa,

a) Coordina todas las funciones de seguridad de la Organización.

b) Vela por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.

c) Vela por el alineamiento de las actividades de seguridad y los objetivos de la Organización.

d) Es responsable de la elaboración de la Política de Seguridad Corporativa, que será aprobada por la Alta Dirección.

e) Aprueba las políticas de seguridad de las diferentes áreas, que serán presentadas por los correspondientes responsables de seguridad.

f) Coordina y aprueba las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad. Los presupuestos elevados serán transmitidos a la Alta Dirección para su aprobación. Los responsables de seguridad se encargarán de llevar a cabo un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.

g) Escucha las inquietudes de la Alta Dirección y las transmite a los Responsables de Seguridad pertinentes. De estos últimos recaba respuestas y soluciones que, una vez coordinadas, son notificadas a la Alta Dirección.

h) Recaba de los Responsables de Seguridad informes regulares del estado de seguridad de la Organización y de los posibles incidentes. Estos informes, se consolidan y resumen para la Alta Dirección.

i) Coordina y da respuesta a las inquietudes transmitidas a través de los Responsables de Seguridad.

j) Debe definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de tareas.

– Comité STIC,

a) Coordina todas las actividades relacionadas con la seguridad de las TIC.

b) Es responsable de la redacción de la Política de Seguridad de las TIC, que será presentada al Comité de Seguridad Corporativa para su aprobación.

c) Es responsable de la creación y aprobación de las normas que enmarcan el uso de los servicios TIC.

d) Aprobará los procedimientos de actuación en lo relativo al uso de los servicios TIC.

e) Aprobará los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.

f) El Comité STIC se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

– Responsable de seguridad corporativa,

a) Actúa como Secretario del Comité de Seguridad Corporativa.

b) Convoca al Comité de Seguridad Corporativa, recopilando la información pertinente.

c) Escucha las inquietudes de la Alta Dirección y de los responsables de seguridad y las incorpora al orden del día para su discusión en las reuniones del Comité de Seguridad Corporativa.

d) Es responsable, junto con los diferentes Responsables de Seguridad, de estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la Organización, debiendo informarse de las consecuencias para las actividades de la Organización, alertando al Comité de Seguridad Corporativo y proponiendo las medidas oportunas de adecuación al nuevo marco.

e) Es el responsable de la toma de decisiones día a día entre las reuniones del Comité de Seguridad Corporativa. Estas decisiones serán respuesta a propuestas de los responsables de seguridad, velando por la unidad de acción y la coordinación de actuaciones, en general y en especial en caso de incidencias que tengan repercusión fuera de la Organización y en caso de desastres.

f) En caso de desastre se incorporará al Comité de Crisis y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la Organización.

– Responsable STIC,

a) Actúa como Secretario del Comité STIC.

b) Es responsable de estar al tanto de cambios de la tecnología y/o del entorno en el que vive la Organización, tales que afecten a la Organización, debiendo informarse de las consecuencias para las actividades STIC, alertando al Comité de STIC y proponiendo las medidas oportunas de adecuación al nuevo marco. Así mismo trasladará al Comité de Seguridad Corporativa las decisiones adoptadas por el Comité STIC.

c) Es responsable de la redacción de los procedimientos de actuación el lo relativo al uso de los servicios TIC. Estos procedimientos se presentarán al Comité STIC para su aprobación. La redacción de los procedimientos puede delegarse en los Responsables STIC de Áreas.

d) Es responsable de la correcta ejecución de las instrucciones emanadas del Comité STIC, ejecución que materializará transmitiendo instrucciones a los administradores y operadores STIC, directamente o a través de los Responsables STIC de Áreas.

e) Es responsable de la presentación regular de informes sobre el estado de seguridad de los servicios TIC. Estos informes se presentarán al Comité STIC. Se elaborará así mismo un informe ejecutivo para ser presentado al Comité de Seguridad Corporativa.

f) Es responsable de la preparación de informes en caso de incidentes excepcionalmente graves y en caso de desastres. Se presentará un informe detallado al Comité STIC y un informe ejecutivo al Comité de Seguridad Corporativa.

g) Es responsable de la elaboración de un Análisis de Riesgos de los sistemas de las TIC, análisis que será presentado al Comité STIC para su aprobación. Este análisis deberá actualizarse regularmente (por ejemplo, cada 6 meses, aunque depende de la criticidad del sistema).

h) Es responsable de que se ejecuten regularmente verificaciones de seguridad según un plan predeterminado y aprobado por el Comité STIC. Los resultados de estas inspecciones se presentarán al Comité STIC para su conocimiento y aprobación. Si como resultado de la inspección aparecen incumplimientos, el Responsable STIC propondrá medidas correctoras que presentará al Comité STIC para su aprobación, responsabilizándose de que sean llevadas a cabo.

i) Es responsable de la elaboración y seguimiento del Plan de Seguridad. En la elaboración de este plan intervendrán los Responsables STIC de Áreas. Este plan será presentado al Comité STIC para su aprobación y al Comité de Seguridad Corporativo para su conocimiento y aprobación.

j) Elaborará para su aprobación por el Comité STIC los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.

k) Es responsable de la identificación de tareas de administración y operación que garanticen la satisfacción de los criterios y requisitos de segregación de tareas impuestos por el Comité de Seguridad Corporativa.

l) Es el interlocutor oficial en comunicaciones con otras Organizaciones, tarea que puede asumir personalmente o delegar según las circunstancias, pero nunca debe haber más de un interlocutor.

m) Es el responsable de coordinar la respuesta ante incidentes que desborden los casos previstos y procedimentados. Es el responsable de coordinar la investigación forense relacionada con incidentes que se consideren relevantes.

– Responsables STIC delegados,

En aquellos casos en que existan varios Sistemas que por su complejidad, diversidad, distribución, etc... requieran de una mayor dedicación, se podrán nombrar Responsables STIC Delegados cuyo ámbito de responsabilidad se limitará al área TIC para el que son designados. Estos responsables dependen funcionalmente del Responsable STIC que será, en última instancia, responsable de su adecuado desempeño.

a) Elaborarán procedimientos de actuación en el área que les compete, siguiendo las instrucciones recibidas del Responsable STIC.

b) Elaborarán informes regulares para el Responsable STIC sobre el estado de seguridad del área que les compete.

c) Elaborarán informes detallados para el Responsable STIC de incidencias no rutinarias en el área que les compete.

d) Se responsabilizarán de la adecuada competencia y formación continua de los administradores y operadores asignados a su área de competencia.

En resumen, los diferentes roles STIC se limitan a una jerarquía simple: el Comité STIC da instrucciones al Responsable STIC que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para la Organización.

El Comité STIC también escuchará las inquietudes de la Alta Dirección y del Comité TIC e informará a todos ellos del estado de seguridad de las TIC. En la siguiente figura se muestra la relación existente entre los difentes elementos de la organización:

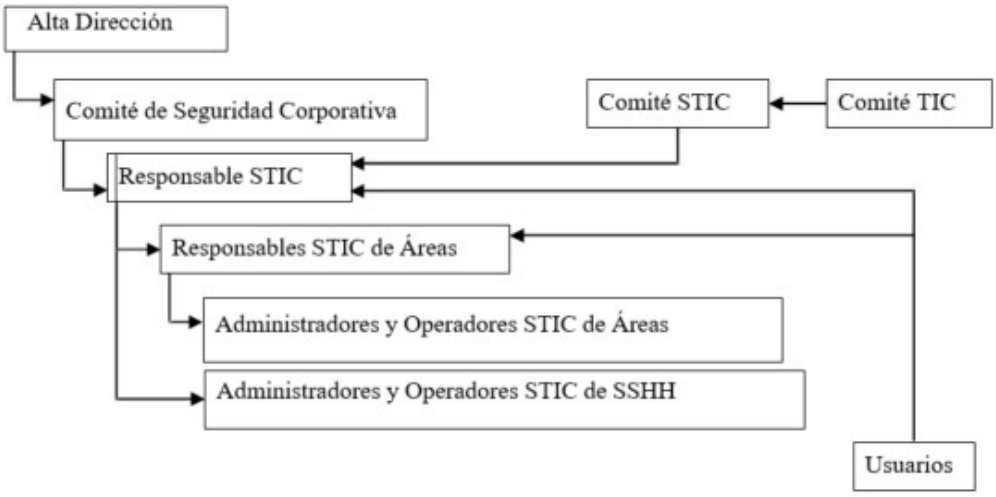


**Figura 2.** Relaciones entre las figuras que conforma STIC, recuperado de GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-402)

### 2.3. Responsabilidades y funciones

La Política de Seguridad, según requiere el Anexo II del ENS en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

Se establecen los siguientes roles en la organización relacionados con la Seguridad de la Información.

- Dirección de la Entidad del Sector Público: Máximo responsable de la implantación del ENS. Conformado por entidades del Sector Público del ámbito de aplicación del ENS, cuyo titular ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad, incluyendo las de seguridad de la información, de conformidad con lo dispuesto en la Ley 40/2015 y en el resto del ordenamiento jurídico.

- Responsable de la Información:

  Según el art.10 del ENS, las personas responsables de la información serán los que decidan sobre la finalidad, contenido y uso de la información y, por tanto, de su protección, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de la información constituye asimismo una actividad indelegable.

  Además, de acuerdo con el art.43 del ENS, son responsables últimos de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

  Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

a) Ayudar a determinar los requisitos de seguridad de la información, categorizando la información mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria al Responsable de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los Responsables de los Servicios y de las personas Responsables de los Sistemas.

c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

- Responsable del Servicio:

Según el art.10 del ENS, las personas Responsables de los Servicios serán los que decidan sobre las características de los servicios a prestar. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de los servicios constituye asimismo una actividad indelegable.

De acuerdo con el art.39 del ENS, las personas responsables de los servicios también deben decidir sobre las especificaciones en el ciclo de vida de los servicios, acompañados de los respectivos procedimientos de control.

Además, según el art.43 del ENS, se valorarán las consecuencias de un impacto negativo sobre la seguridad de los servicios. Para ello, se tendrá en cuenta la repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

a) Ayudar a determinar los requisitos de seguridad de los servicios a prestar, categorizando los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria al Responsable de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los Responsables de la Información y de los Responsables de los Sistemas.

c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

- Responsable de la Seguridad (STIC):

El Responsable de la Seguridad (de la información) es la persona designada por la Dirección de la entidad, según el procedimiento descrito en su Política de Seguridad de la Información y determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Además de ello, como hemos visto con anterioridad, en caso de servicios externalizados, la responsabilidad última la tiene siempre la Entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio (lo que sucede, por ejemplo, en la utilización de servicios en la nube).

Las dos funciones esenciales del Responsable de la Seguridad son:

a) Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización.

b) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. 43.

Además de ello, cuando la figura del Responsable de la Seguridad del ENS coincide con la Entidad Responsable de Seguridad de la Información derivada de la Directiva NIS, podrá desplegar las siguientes funciones:

c) Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.

d) Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.

e) Elaborar el documento de Declaración de Aplicabilidad.

f) Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

g) Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del RD-l 12/2018 y de su Reglamento de Desarrollo.

h) Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.

i) Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.

j) Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

k) Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

Considerando que las leyes 39/2015 y 40/2015 consagran el uso de los medios electrónicos en el desenvolvimiento cotidiano de las entidades del Sector Público, parece lógico suponer que la figura del Responsable de la Seguridad debe estar situada en una posición que le permita tener un acceso directo a los niveles directivos de la organización.

Por tanto, cuando se trate de organizaciones de la AGE, el Responsable de la Seguridad debería depender, en general, de la Secretaría General Técnica. En el caso de entidades locales (Diputaciones, Cabildos o Ayuntamientos), debería depender del Secretario General, tal como muestra la figura siguiente. En ambos casos, Secretaría General Técnica o Secretaría General liderarían los Comités de Seguridad de la Información.

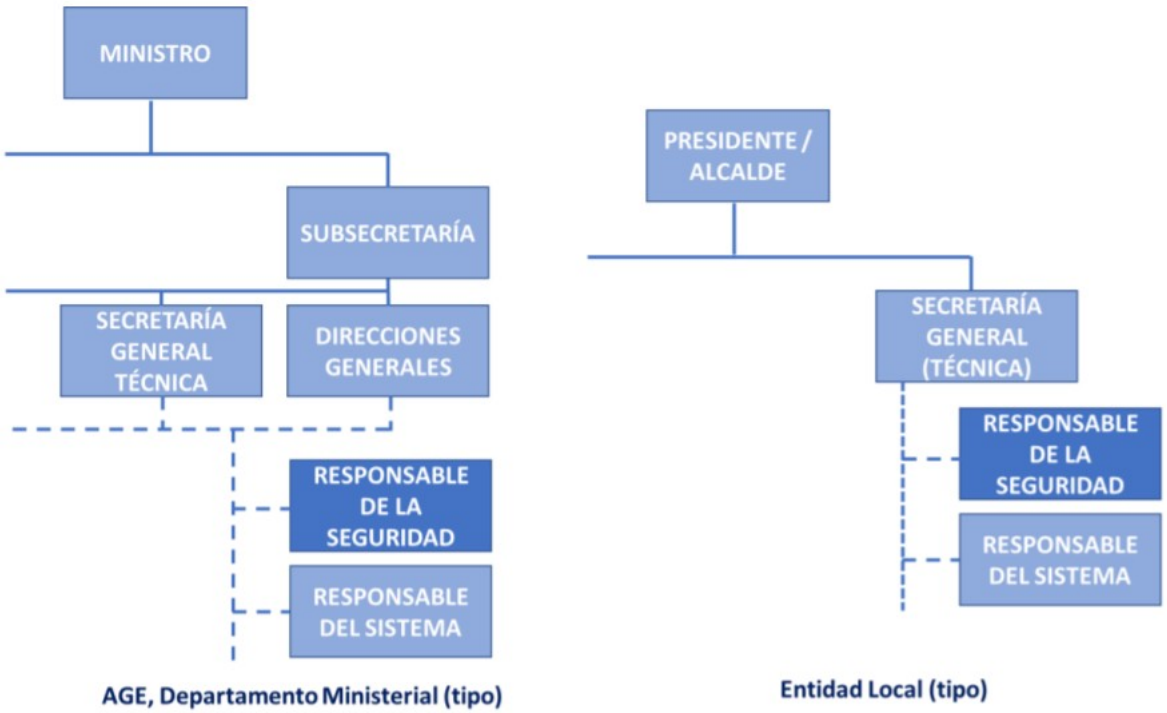


**Figura 3.** Responsable de la seguridad en las entidades existentes, recuperado de GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-402)

En el caso de las Comunidades Autónomas dependerá del tipo de organización elegido para la función de seguridad de la información: vertical (seguridad de la información localizada en cada Consejería) o transversal (seguridad de la información como actividad horizontal). Si se quiere imprimir una transversalidad a la seguridad, una solución frecuentemente utilizada es situar la Responsabilidad de la Seguridad en el ámbito competencial de la Consejería encargada de la Administración Electrónica, ubicando Responsables de Seguridad Delegados en cada una de las Consejerías restantes.

En aquellos sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, cada organización podrá designar Responsables de Seguridad Delegados. La designación corresponderá al Responsable de la Seguridad, que delegará funciones, no responsabilidad.

Los Responsables de Seguridad Delegados se harán cargo, en su ámbito competencial, de todas aquellas funciones delegadas por el Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos (departamentales, por ejemplo) o de sistemas de información horizontales.

Cada Responsable de la Seguridad Delegado mantendrá una dependencia funcional directa del Responsable de la Seguridad, a quien reportará.

- Responsable del Sistema (de información) (TIC):

Además de las tres figuras mencionadas en el art. 10 del ENS -Responsable de la Información, Responsable del Servicio y Responsable de la Seguridad-, cuyas competencias y responsabilidades pueden ser indelegables , las organizaciones suelen disponer también del denominado Responsable del Sistema (de información), cuya responsabilidad, según la ley la Ley 40/2015, puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.

Además, según lo art. 34.6 y 34.7 del ENS, los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

- Responsable del Tratamiento (Protección de Datos):

Según el art. 4.7) de RGPD y Título V de OPDGDD, el Responsable del Tratamiento se corresponde con la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

- Encargado del Tratamiento (Protección de Datos):

Según el art. 4.8) de RGPD y Título V de OPDGDD, se corresponde con la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable del Tratamiento

- Delegado de Protección de Datos:

El Delegado de Protección de Datos (DPD) puede ser interno o externo a la organización, pudiendo revestir asimismo la forma de un órgano colegiado (Comité Delegado de Protección de Datos), velando siempre por evitar conflicto de intereses en cualquiera de sus miembros. Además de ello, podrá designarse un único DPD para varias autoridades u organismos públicos, teniendo en consideración su estructura y tamaño.

Según el artículo 37, el Delegado de Protección de Datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39. Además, el Delegado de Protección de Datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

Las funciones del Delegado de Protección de Datos, según el art.39 serían:

a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

b) Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.

d) Cooperar con la autoridad de control.

e) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto. 2.

El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

El Responsable de Seguridad de la Información será propuesto por el Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante. El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política

## 2.4. Seguridad de la información

Aunque la seguridad de la información no es lo mismo que la seguridad de las TIC, la relación entre ambas es fuerte y crítica.
La clasificación de la información (como SECRETO, RESERVADO, CONFIDENCIAL o de DIFUSIÓN LIMITADA) no se decide por criterios TIC o STIC. Pero una vez determinada su clasificación, esta implica una serie de requisitos sobre su manipulación mediante servicios TIC.

### 2.4.1. Clasificación de la información

La información manejada por un sistema TIC es uno de los bienes críticos a proteger. Como tal, debe estar muy bien definido quién debe hacer qué con qué información. Como no toda la información requiere el mismo tratamiento, y el tratamiento puede ser laborioso y costoso, es muy conveniente establecer niveles de información en función de sus exigencias de seguridad. A esto se le denomina "clasificar la información" (o sea, establecer clases de información) y a la información cuya clase se conoce se la denomina "información clasificada".

La información clasificada requiere algunos procedimientos de control:

a. procedimiento para clasificar la información; que establece quién determina a qué clase pertenece y en base a qué criterios
b. procedimiento para cambiar la clasificación (incluida su desclasificación); que establece quién puede alterar la etiqueta de una información, en base a qué criterios y dejando qué registro
c. procedimientos para tratar la información en base a su nivel:
    i. ¿quién puede acceder a la información?, ¿en qué condiciones?,

       ¿dejando qué registros?
    ii. cifrado de los ficheros y gestión de claves,
    iii. realización de copias y gestión de copias,
    iv. etiquetado de soportes de información,
    v. impresión y gestión de información impresa,
    vi. transmisión (fax, redes, e-mail, ...),
    vii. acceso por terceras partes: autorización, obligaciones contraídas, etc.
    viii. copias de seguridad y gestión de copias,
    ix. destrucción de copias y soportes

La clasificación de la información tiene en cuenta las consecuencias que se derivarían de su conocimiento por personas que no deben tener acceso a ella

| Nivel | Características |
|---|---|
| Confidencial | Su revelación supondría un grave daño:<br>• supondría una ventaja comercial desproporcionada |

para la competencia
- supondría un grave quebranto económico
- podría quebrar la capacidad de operar de la Organización

supondría un serio daño a la imagen de la Organización

Difusión limitada

Su revelación causaría daños indeseables:
- supondría un ventaja comercial para la competencia
- supondría un quebranto económico
- dañaría significativamente a la capacidad de operar de la Organización
- supondría un cierto daño a la imagen de la Organización
- supondría un incumplimiento de las obligaciones de confidencialidad adquiridas por la Organización con respecto de terceros

supondría un incumplimiento de obligaciones legales Ejemplos: datos de carácter personal, salarios, acuerdos con clientes y proveedores,

Sin clasificar

En este capítulo se suele dejar la información interna que no es pública, y a la que pueden acceder todos los miembros de la Organización.
Su revelación no supondría un gran perjuicio, aunque pudiera ser embarazosa.

Ejemplos: listín telefónico, guías de procedimientos internos, borradores de documentos,

Cuando la información afecta a temas de Estado, suelen aparecer dos categorías superiores:

Secreto
- daños graves a la seguridad nacional
- incidentes graves internacionales

Reservado
- afectaría a la seguridad nacional
- afectaría al orden público
- causaría incidentes internacionales

Evidencia necesaria: Dentro de la política se indica cuál es el criterio para la calificación de la documentación, el procedimiento para su calificación, quién debe generarla y aprobarla, qué personas pueden acceder a ella, con qué frecuencia o bajo qué circunstancias debe revisarse, etc.

### 2.4.2. Calificación de la información

El proceso de calificación parte de la identificación y la valoración documental, y determina los valores de los documentos a lo largo de su ciclo de vida, sus plazos de conservación, las transferencias de custodia, la eliminación y las condiciones de acceso. En el ámbito de la Junta de Andalucía, la calificación es otorgada por la Comisión Andaluza de Valoración de Documentos (en adelante CAVD) como el órgano competente para dictaminar la conservación o eliminación de los documentos de titularidad pública relacionados en el Art. 9 de la Ley 7/2011.

Esta actividad calificadora de la CAVD se materializa en los instrumentos de calificación que son aprobados por la persona titular de la Consejería competente en materia de documentos, archivos y patrimonio documental, de acuerdo con la normativa que regula la Comisión.

Los criterios de calificación recogidos en ellos se incorporarán como parte de los metadatos de los documentos y expedientes electrónicos correspondientes. En los casos en los que la calificación decrete la eliminación, los metadatos correspondientes podrán ser explotados para la ejecución automática de la selección, sin perjuicio del procedimiento establecido por la CAVD para la autorización de la eliminación de documentos.

### 2.4.3. Acceso

Los valores y las características de los documentos varían con el paso del tiempo y su ciclo de vida, por lo que el uso de los metadatos es esencial en la automatización de la gestión del acceso a los documentos electrónicos.

El control de los permisos de acceso y las responsabilidades vinculadas a esas funciones es un proceso constante en los sistemas de gestión de documentos electrónicos, que los responsables de los mismos realizan de forma coordinada con los responsables de la gestión y conservación de los documentos.

El control de acceso garantizará:

- El acceso y uso restringido a los documentos por los agentes correspondientes en las formas autorizadas.
- La división en categorías de los documentos de acuerdo con el nivel de seguridad que les corresponda.

En ese contexto, al acceso a los documentos y expedientes electrónicos son aplicables las medidas de protección de la información previstas en el Anexo II del Esquema Nacional de Seguridad, normativa de acceso a los archivos, registros y a la información pública. En particular 'Datos de carácter personal' y 'Calificación de la información', sin perjuicio de otras medidas que puedan ser de aplicación a la luz de la categorización del sistema y de la calificación de la información, y de las medidas relativas al control de acceso. Para ello se atenderá tanto a lo dictado en la norma que regule el procedimiento que genera el documento o expediente, como a lo dictado por la Comisión Andaluza de Valoración de Documentos en relación a la serie documental a la que pertenecen.

En consecuencia, el acceso a los documentos y expedientes electrónicos estará sometido a un control en función de la calificación de la información y de los permisos y responsabilidades del actor en cuestión y contemplará la trazabilidad de las acciones que se realicen sobre cada uno de los documentos y expedientes electrónicos y sus metadatos asociados, de acuerdo con la normativa vigente.

# 3. NORMAS Y BUENAS PRÁCTICAS EN EL DESARROLLO DE WS

A continuación se presenta un resumen de las normas y buenas prácticas de aplicación en el contexto del uso de las políticas de seguridad en los desarrollos, los cuáles deberán seguir una serie de directrices según la red desde la que serán consumidos.

En el documento analizaremos los siguientes mecanismos de seguridad:

- WS-Security
- SAML
- HTTPS/SSL
- WS-Signature y WS-Addressing
- WS-Policy
- Oauth 2.0

Según desde donde sea consumido el WS, se establecen una serie de directrices:

- **WS Accesibles desde RCJA**

  Para todos los WS que sus accesos sean únicamente a través de la Red Corporativa de la Junta de Andalucía será obligatoria la autenticación mediante alguno de los siguientes mecanismos:

  - BasicAuth
  - WS-Security - UsernameToken (Recomendado para SOAP)
  - SAML
  - Mutual SSL
  - Oauth 2.0 (Recomendado para REST)

- **WS Accesibles desde Red SARA**

  Para aquellos WS que puedan ser accedidos a través de RCJA y también desde Red SARA, será obligatoria la autenticación mediante alguno de los siguientes mecanismos:

  - WS-Security - UsernameToken
  - SAML
  - Mutual SSL (Recomendado para SOAP)

- Oauth 2.0 (Recomendado para REST)

- **WS Accesibles desde Internet**

Para aquellos servicios que puedan ser accedidos a través de RCJA, Red SARA y también desde Internet, será obligatoria la autenticación mediante uno de los siguientes mecanismos:

- WS-Security - UsernameToken
- SAML
- Mutual SSL (Recomendado para SOAP)
- Oauth 2.0 (Recomendado para REST)

Además, será de carácter obligatorio la definición de la política de seguridad mediante la especificación WS-Policy para aquellos servicios que sean de tipo SOAP.

## 3.1. Servicios de seguridad básicos

La seguridad es un concepto más que junto con la transaccionalidad, fiabilidad y gestión / administración definen la Calidad del Servicio en los servicio Web.

Los servicios de seguridad básicos en los servicios web son la confidencialidad, integridad, autenticación, no repudio y autorización.

Los objetivos de seguridad que se describen tienen un ámbito de actuación en dos niveles:

- Seguridad a nivel de mensaje

  La seguridad de nivel de mensaje representa un enfoque según el cual toda la información relacionada con la seguridad está encapsulada en el mensaje en sí. La seguridad de nivel de mensaje implica protección con token de nombre de usuario, cifrado XML y firmas digitales. La especificación WS-Security ya establece una seguridad de nivel de mensaje. Por lo general, este tipo de seguridad se aplica en combinación con la seguridad de nivel de transporte.

- Seguridad a nivel de transporte

La seguridad de nivel de transporte es un mecanismo de seguridad punto a punto que se puede usar a efectos de identificación y autenticación de partes, integridad del mensaje y confidencialidad. HTTP es un protocolo intrínsecamente inseguro ya que toda la información es enviada en texto no cifrado entre pares no autenticados a través de una red insegura. Con la seguridad de nivel de transporte, la conexión entre un cliente y un servidor de aplicaciones suele estar asegurada con una Capa de sockets seguros (SSL), por medio de la cual el cliente y el servidor autentican la identidad del otro y se comunican con mensajes cifrados. Si se aplica la seguridad de nivel de transporte, toda la comunicación estará cifrada.

A continuación se explica brevemente cada uno de ellos:

### 3.2. Autenticación

Cada servicio web participante en una interacción podría requerir autenticación de la otra parte. Cuando cierto servicio A dirige una petición al servicio B, éste puede requerirle unas credenciales junto con una demostración de que le pertenecen como por ejemplo un par nombre de usuario (credencial)/password (demostración) o un certificado X.509v3 (credencial)/firma digital (demostración).

El principal problema de la autenticación, cuyo origen radica en la naturaleza heterogénea de los servicios Web, es conseguir un acuerdo en los protocolos y en los formatos de los datos de seguridad empleados. Otro punto a resolver es definir un modelo de autenticación Single Sign-On de forma que un servicio Web A que necesita interactuar con otros 6 servicios Web, para completar un proceso de negocio P en tiempo real, no necesite autenticarse más que una vez frente al primero de ellos para poder completar la operación bajo un tiempo de respuesta aceptable.

Así, **la autenticación es obligatoria** para mantener control y verificar la identidad de solicitantes y proveedores.

En función de la política de seguridad que se adopta, es necesario autenticar tanto al proveedor como al solicitante o simplemente a alguno de ellos. Se pueden emplear métodos basados en contraseñas, certificados, etc.. para formalizar la autenticación. Si se basan en contraseñas, es necesario aplicar una política que aporte robustez a las mismas.

Algunos mecanismos que se pueden llevar a cabo para los **servicios web de tipo SOAP** son:

- **Mecanismos basados en protocolos de transporte** como el HTTP Autentication y SSL/TLS X509 Certificate. Este mecanismo es válido cuando no se altera de forma intermedia el mensaje entre el consumidor y el proveedor final del servicio. Ya que si un mensaje SOAP viaja entre varios endpoints antes de llegar a su destino, es posible que las credenciales originales se pierdan en alguno de los puntos intermedios de tratamiento.
- **Mecanismos basados en tokens** que se incluye dentro del mensaje. El estándar WS-Security incorpora un gran número de tokens que pueden ser empleados en este caso; Username Token, X509 Certificate, SAML assertions, etc. Este mecanismo de autenticación no tiene los problemas de los mecanismos basados en el transporte, ya que las credenciales pueden viajar entre los distintos endpoints hasta llegar a su destino. Si usamos este mecanismo, es necesario que estos sean transmitidos de forma segura para evitar ataques de replay. Esto se consigue mediante la firma del token dentro del mensaje SOAP, junto a un TimeStamp o IDMessage, por lo que se recomienda incluir en la firma la cabecera de WS-Addressing. En entornos cerrados también se puede emplear SSL para transmitir los mensajes con Tokens de forma segura, aunque esta aproximación es menos segura que la anterior.

En el caso de los **servicios web REST:**

- Basada en la sesión, ya sea estableciendo un token de sesión a través de un llamada POST o utilizando una APIKey como argumento de una petición POST o de una cookie. Es el principio usado por SAML. Es muy importante indicar que los nombres de usuario, las contraseñas, los tokens de sesión y las claves API no deben aparecer en la URL, ya que estos podrían interceptarse.
- OAuth 2.0, protocolo de autorización que permite a terceros acceder a contenidos de la propiedad de un usuario, sin que este tenga que manejar ni conocer credenciales alguna.

## 3.3. Confidencialidad e integridad

Mantener de manera secreta la información crítica contenida en los mensajes intercambiados entre los servicios Web supone otra de las propiedades fundamentales que deben darse para que el canal de comunicación establecido se pueda considerar "seguro" . La confidencialidad se consigue mediante técnicas de cifrado ampliamente utilizadas y extendidas en otros campos de la computación. La confidencialidad no sólo afecta al canal que se utiliza para intercambiar los mensajes.

Especificaciones como el XMLSignature y el XMLEncrypt están diseñados para garantizar la confidencialidad (encriptación) e integridad (firma) de los mensajes dentro de una comunicación por Web Services. Estos dos estándares están recogidos a su vez, dentro de la especificación WS-Security.

Estos mecanismos de seguridad son independientes del transporte, por lo que son ideales en entornos por lo que la comunicación viaja por distintos tipos de transporte (https, jms, etc). Además, son mecanismos que garantizan una seguridad de extremo a extremo, es decir, abarcan comunicaciones de Servicios Webs por los que el mensaje circula por más de un endpoint.

Por último, permiten garantizar la integridad de los mensajes almacenados, por ejemplo cuando son encolados en colas JMS o guardados en ficheros, logs, BD, etc.

## 3.4. Autorización

Los servicios web deben disponer de mecanismos que les permitan controlar el acceso a sus servicios (recursos). Se debe poder determinar quién y cómo puede hacer a qué y cómo sobre sus recursos. La autorización concede permisos de ejecución de ciertos tipos de operaciones sobre ciertos recursos a ciertas identidades autenticadas. Normalmente ese conjunto de restricciones que gobiernan el acceso a los recursos se materializan en forma de políticas de seguridad de acceso. Mecanismos como SAML/XACML permiten a los servicios web establecer el control de autorizaciones sobre los recursos de un servicio.

## 3.5. No repudio

Cuando se realizan transacciones suele ser un requisito la capacidad de probar que una acción tuvo lugar y que fue realizada por cierto actor. En el caso de los servicios web, es necesario ser capaz de demostrar que un cliente utilizó un servicio pese a que éste lo niegue (no repudio del solicitante) así como demostrar que un servicio fue ejecutado (no repudio del receptor).

Para garantizar el no repudio dentro de las comunicaciones por Servicios Web, los mensajes SOAPs intercambiados deberán ser identificados de forma única mediante el uso de la especificación WS-Addressing.

Los mensajes SOAP junto a sus cabeceras "relevantes", deben ser firmadas según los procedimientos recogidos en la especificación WS-Security.

Por último, los mensajes deberán ser almacenados en ficheros de logs, para su posterior consulta. De forma esquemática se podría representar como WS-Addresing + WS-Security (WS-Signature) + logs.

# 4. MECANISMOS DE SEGURIDAD EN LA IMPLEMENTACIÓN DE WS

A continuación, se describen los diferentes mecanismos de seguridad que se pueden llevar a cabo durante la implementación de un servicio web para garantizar la seguridad del mismo.

## 4.1. WS-Security

Esta especificación es un estándar según OASIS y proporciona integridad, confidencialidad y opcionalmente no repudio a los mensajes SOAP intercambiados entre servicios Web.

El estándar WS-Security define una especificación que implementa una serie de mejoras al marco de trabajo de mensajería SOAP con el objetivo de mejorar la protección de los mensajes.

Para ello, se basa en dos mecanismos esenciales:

- La integridad y confidencialidad de los mensajes.
- Autenticación de un mensaje individual.

WS-Security especifica un procedimiento que permite indexar tokens de seguridad a los mensajes en los intercambios de información. Un token de seguridad está compuesto por varias declaraciones de seguridad. No se especifica ningún tipo de token de seguridad a aplicar con WS-Security dado el carácter extensible del estándar y soportar varios formatos actualmente.

En el estándar también encontramos como codificar tokens de seguridad binarios. Así mismo, se describen mecanismos que posibilitan realizar descripciones sobre las características de las credenciales que se encuentran incluidas dentro de un mensaje.

Aún siendo de gran ayuda, la especificación WS-Security no garantiza la seguridad, ni es capaz de proporcionar una solución de seguridad completa. WS-Security es un bloque de construcción que es utilizado conjuntamente con otros protocolos de servicios Web o específicos de aplicación para acomodar una amplia variedad de modelos de seguridad y tecnologías de cifrado. Implementar esta especificación no significa que una aplicación no pueda ser atacada o que la seguridad no pueda verse comprometida alguna vez.

WS-Security es flexible y su diseño constituye la base para la creación de modelos de seguridad más complejos incluyendo PKI, Kerberos y SSL. En particular, WS-Security proporciona soporte para múltiples tokens de seguridad, múltiples dominios de confianza, múltiples formatos de firma y múltiples tecnologías de cifrado.

Hay tres grandes problemas en la protección de intercambios de mensajes SOAP, y WS-Security brinda respuestas para todos ellos, aunque no directamente. Es, de hecho, una especificación que habla no sobre cómo proteger el mensaje, sino cómo hacer saber al destinatario que se ha protegido el mensaje. Para realizar la protección real, WS-Security referencia especificaciones adicionales:

- El primer problema es **identificar y autenticar al cliente**. Debido a que hay muchas maneras diferentes de crear tokens de seguridad, WS-Security no especifica ningún medio particular, sino que define cómo se deben transferir los token de seguridad dentro de los mensajes SOAP. En otras palabras, hace saber al destinatario cómo extraer tokens de seguridad del mensaje para su procesamiento.
- El segundo problema es **garantizar la integridad del mensaje**. WS-Security utiliza firmas digitales para eso, empleando la especificación de Firma XML en lugar de inventar algo nuevo. La Firma XML es una recomendación W3C que incluye un mecanismo para firmar documentos XML de manera digital.
- El tercer problema es **mantener el mensaje seguro contra la interceptación** mientras está en tránsito. Una vez más, WS-Security utiliza otro estándar W3C, esta vez Cifrado XML, que brinda un mecanismo para cifrar documentos XML.

## 4.2. SAML

Estándar XML para el intercambio de datos de autentificación y autorización entre dominios de seguridad, es decir, entre un proveedor de identidad (un productor de afirmaciones) y un proveedor de servicio (un consumidor de afirmaciones)

La información de seguridad se materializa en forma de afirmaciones hechas por una autoridad SAML sobre un sujeto. El sujeto de una afirmación es aquella entidad objeto de las afirmaciones realizadas por la autoridad SAML.

Las afirmaciones, contienen varios tipos de información. Pueden informar acerca de la autenticación, sobre atributo, o sobre decisiones de autorización. Analizando el tipo de declaraciones que pueden emitirse, pueden definirse tres tipos de autoridades como son:

- Autoridad de Autenticación. Afirmación para indicar que el usuario se autenticó en un momento dado contra el proveedor de identidad.
- Autoridad de Atributos. Afirmación para indicar que un sujeto se asocia con ciertos atributos, un atributo es simplemente un par clave-valor.
- Puntos de Decisión de Políticas. Decisión de autorización para determinar que un sujeto puede realizar una acción en un recurso.

Este estándar cobra especial importancia en sistemas bajo una arquitectura SSO y que tengan un control centralizado de políticas de autorización. En términos de servicios web, para aquellos casos en los que haya que orquestar llamadas entre servicios de distintos sistemas y no tener que negociar autenticación con cada uno de ellos.

## 4.3. HTTPS/SSL

HTTPS permite la autenticación del cliente y del servidor mediante certificados.

SSL es un protocolo que transmite las comunicaciones por Internet en formato cifrado. De esta manera se garantiza que la información se envíe sin cambios al servidor deseado. Es posible aplicar servicios web HTTPS a todos los tipos de clientes, incluidos los clientes Java EE y los clientes Java independientes.

En la actualidad, HTTPS con certificados del servidores constituye la configuración más habitual de la Web. En esta configuración, el servidor debe presentar su certificado al cliente para determinar la identidad del servidor. El cliente no necesita presentar su certificado al servidor para que este determine la identidad de aquel. En otras palabras, el cliente puede autenticar al servidor, pero el servidor no puede autenticar al cliente. Sin embargo, también es posible usar HTTPS junto con la autenticación básica, que permite al servidor autenticar al cliente o establecer un mecanismo de autenticación Mutual SSL donde hay un intercambio de certificados entre servidor y cliente.

## 4.4. WS-Signature y WS-Addressing

WS-Addressing es una especificación de mecanismos de transporte que permiten a los servicios web comunicar la información de direccionamiento.

Consiste básicamente en dos partes:

- Una estructura para la comunicación de una **referencia a un punto final** de un servicio web.
- Un conjunto de propiedades de direccionamiento de mensajes que asocian la **información de direccionamiento con un mensaje particular**.

Para garantizar el no repudio dentro de las comunicaciones por servicios webs, los mensajes SOAP intercambiados deberán ser identificados de forma única mediante el uso de la especificación WS-Addressing. Los mensajes SOAP junto a sus cabeceras "relevantes", deberán ser firmadas según los procedimientos recogidos en la especificación WS-Security. Por último, los mensajes deberán ser almacenados en ficheros de logs, para su posterior consulta. De forma esquemática se podría representar como WS-Addresing + WS-Security (WS-Signature) + logs.

A continuación se exponen las indicaciones descritas en la especificación WS-Adressing para la identificación de los mensajes SOAP que se intercambian:

- **Algoritmos fuertes**. Se deben utilizar algoritmos de cifrado lo más fuertes posible, como SHA-256 o SHA-512, para asegurar la integridad de las claves.
- **Irrevocabilidad**. Mediante la firma PKI se garantiza la irrevocabilidad de los mensajes enviados entre el emisor y el receptor, es decir, permite asegurar la identidad de los actores en la comunicación.
- **Repetición del mensaje**. Se debe impedir la reproducción de los mensajes de la aplicación utilizando, por ejemplo, la marca de hora (timestamp) en los mensajes o tecnologías como la secuenciación.

## 4.5. XMLEncrypt

Esta especificación define un proceso para cifrar datos asegurando así la confidencialidad de alguna o todas las partes de la información cifrada.

El resultado de cifrar un elemento se representa en formato XML EncryptedData el cual contiene o identifica (mediante una URI) los datos cifrados.

## 4.6. WS-Policy

Web Services Policy Framework, o WS-Policy, es una especificación que permite a un servicio web tener un conjunto de reglas que se deben cumplir, o consumir. Los autores de clientes que consumen servicios web deben estudiar la información de directivas para ver si pueden o no respetarlas. Por ende, no se puede escribir un cliente para que simplemente acceda a un servicio web que requiera que todos los mensajes sean cifrados o firmados de cierta manera. Un cliente tampoco accedería a un servicio web que tiene una directiva que requiere una marca de tiempo y enviar un mensaje que no la tenga. Y ese es el objetivo de WS-Policy: especificar información de directivas que deben respetar los consumidores del servicio web.

## 4.7. Oauth 2.0

OAuth2 es un protocolo de autorización que permite a terceros (clientes) acceder a contenidos propiedad de un usuario (alojados en aplicaciones de confianza, servidor de recursos) sin que éstos tengan que manejar ni conocer las credenciales del usuario. Es decir, aplicaciones de terceros pueden acceder a contenidos propiedad del usuario, pero estas aplicaciones no conocen las credenciales de autenticación.

Por tanto, en OAuth podemos identificar tres entidades:

- **Propietario de recursos**. Es una entidad capaz de dar acceso a recursos protegidos. Cuando es una persona nos referiremos a él como usuario final.
- **Cliente**. Es la aplicación hace peticiones a recursos protegidos en nombre de un propietario de recursos con la autorización del mismo.
- **Proveedor**
    - Servidor de recursos. Es la entidad que tiene los recursos protegidos. Es capaz de aceptar y responder peticiones usando un access token que debe venir en el cuerpo de la petición.
    - Servidor de autorización. En muchos casos el servidor de autenticación es el mismo que el Servidor de Recursos. En el caso de que se separen, el servidor de autenticación es el responsable de generar tokens de acceso y validar usuarios y credenciales.

OAuth2 tiene dos grandes ventajas, soluciona el problema de la confianza entre un usuario y aplicaciones de terceros, y a su vez permite a un proveedor de servicios/API facilitar a aplicaciones de terceros a que amplíen sus servicios con aplicaciones que hacen uso de los datos de sus usuarios de manera segura y dejando al usuario la decisión de cuando y a quien, revocar o facilitar acceso a sus datos, creando así un ecosistema de aplicaciones alrededor del proveedor de servicios/API. Esto es está directamente relacionado con el concepto de los API Manager.

# 5. MODELO DE SEGURIDAD PARA LOS SERVICIOS DE INTEROPERABILIDAD

La seguridad en las comunicaciones, es un elemento muy importante a tener en cuenta a la hora de diseñar o consumir un servicio de interoperabilidad y que todos los equipos de desarrollo deben tener en mente desde el primer minuto. 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.

A continuación, se darán las guías y pautas a seguir para implementar y publicar estos elementos de seguridad dentro de la OTI en función del ámbito de actuación de estos servicios.

Destacar, que las pautas que se describen a continuación se deberán aplicar de forma obligatoria a todos los nuevos servicios que se generen o consuman, no siendo de cumplimiento estrictamente obligatorio en aquellos servicios ya implementados.

La realidad actual es que los servicios pueden ser accesibles en tres niveles bien diferenciados:

- Seguridad desde RCJA.
- Seguridad desde Red SARA.
- Seguridad desde Internet.

Por cada nivel de accesibilidad se dan las siguientes directrices en cuanto a aseguramiento de la seguridad de los servicios.

## 5.1. Seguridad desde RCJA

En este bloque se deben encontrar aquellos servicios que sólo pueden ser consumidos por sistemas/usuarios que se encuentren conectados a RCJA. Estos servicios no podrán ser consumidos ni desde Red SARA ni por Internet. Los mecanismos de seguridad que se aplican en este caso deben tener en cuenta las limitaciones tecnológicas que puedan tener los sistemas que los proveen.

| Servicio | Carácter | Mecanismos de seguridad | Comentarios |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Autenticación | Obligatorio | BasicAuth | Opción menos recomendada por su fragilidad y no poder controlar el número de intentos de acceso. Esta opción sólo se deberá usar cuando el sistema proveedor tenga limitaciones técnicas para implementar otros mecanismos.<br>Aplicable tanto a servicios SOAP como REST. |
| | | WS-Security (UsernameToken) | Opción más segura que BasicAuth. Es de carácter obligatoria que la contraseña no vaya en abierto, usar por tanto Digest Access Authenticacion.<br>Aplicable a servicios SOAP.<br>**OPCIÓN RECOMENDADA SOAP.**<br>Amplia difusión en la comunidad de desarrollo. A día de hoy no hay plataforma de desarrollo que no se precie a poder configurar este mecanismo de seguridad de forma ágil. |
| | | SAML | Ideal sobre todo para entornos de SSO donde haya que orquestar llamadas a distintos servicios donde la ejecución de uno dependa del estado de otros.<br>Aplicable tanto a servicios SOAP como REST. |
| | | Mutual SSL | Permite restringir perfectamente los clientes |

| | | | |
|---|---|---|---|
| | | | consumidores de los servicios. Se trata de un mecanismo de seguridad basado en el intercambio de certificados entre servidor y clientes. |
| | | Oauth 2.0 | Para aquellos sistemas orientados a la definición de aplicaciones basadas en APIs. **OPCIÓN RECOMENDADA REST.** Amplia difusión en la comunidad de desarrollo. A día de hoy no hay plataforma de desarrollo que no se precie a poder configurar este mecanismo de seguridad de forma ágil. |
| Confidencialidad e Integridad | OPCIONAL | WS-Security (XMLEncrypt) | Técnica de cifrado del mensaje para asegurar confidencialidad y que sólo pueda ser interpretado por el destinatario final. |
| | | WS-Security (XMLSign) | Técnica de firma del mensaje para asegurar integridad. |
| Definición de políticas | OPCIONAL | WS-Policy | Especificación de políticas de uso de los servicios:<br>• TimeStamp: Marca de tiempo del momento en el que se hace la petición. Para evitar ataques por Reply Attack.<br>• Addressing: información del destinatario y emisor de los mensajes.<br>• Expired: duración establecida para la |

| | | | |
|---|---|---|---|
| | | | descartar un mensaje. |
| No repudio | OPCIONAL | WS-Addresing + WS-Security + logs | Para aquellos servicios que requieran confirmación de la recepción y trazabilidad de peticiones. |

### 5.2. Seguridad desde Red SARA

En este bloque se deben encontrar aquellos servicios que puedan ser consumidos desde RCJA y Red SARA. Estos servicios no podrán ser consumidos desde Internet. Los mecanismos de seguridad que se aplican en este caso deben tener en cuenta las limitaciones tecnológicas que puedan tener los sistemas que los proveen.

| Servicio | Carácter | Mecanismos de seguridad | Comentarios |
|---|---|---|---|
| Autenticación | Obligatorio | WS-Security (UsernameToken) | Opción más segura que BasicAuth. Es de carácter obligatoria que la contraseña no vaya en abierto, usar por tanto Digest Access Authenticacion.<br>Aplicable a servicios SOAP. |
| | | SAML | Ideal sobre todo para entornos de SSO donde haya que orquestar llamadas a distintos servicios donde la ejecución de uno dependa del estado de otros.<br>Aplicable tanto a servicios SOAP como REST. |
| | | Mutual SSL | Permite restringir perfectamente los clientes consumidores de los servicios. Se trata de un mecanismo de seguridad basado en el |

| | | | |
|---|---|---|---|
| | | | intercambio de certificados entre servidor y clientes.<br>**OPCIÓN RECOMENDADA SOAP.** |
| | | Oauth 2.0 | Para aquellos sistemas orientados a la definición de aplicaciones basadas en APIs.<br>**OPCIÓN RECOMENDADA REST.**<br>Amplia difusión en la comunidad de desarrollo. A día de hoy no hay plataforma de desarrollo que no se precie a poder configurar este mecanismo de seguridad de forma ágil. |
| Confidencialidad e Integridad | opcional | WS-Security (XMLEncrypt) | Técnica de cifrado del mensaje para asegurar confidencialidad y que sólo pueda ser interpretado por el destinatario final. |
| | | WS-Security (XMLSign) | Técnica de firma del mensaje para asegurar integridad. |
| Definición de políticas | opcional | WS-Policy | Especificación de políticas de uso de los servicios:<br>• TimeStamp: Marca de tiempo del momento en el que se hace la petición. Para evitar ataques por Reply Attack.<br>• Addressing: información del destinatario y emisor de los mensajes.<br>• Expired: duración establecida para la descartar un mensaje. |
| No repudio | opcional | WS-Addresing + WS- | Para aquellos servicios que |

| | | | |
|---|---|---|---|
| | | Security + logs | requieran confirmación de la recepción y trazabilidad de peticiones. |

## 5.3. Seguridad desde Internet

En este bloque se deben encontrar aquellos servicios puedan ser consumido desde RCJA, Red SARA o internet. Los mecanismos de seguridad que se aplican en este caso deben tener en cuenta las limitaciones tecnológicas que puedan tener los sistemas que los proveen. Es de vital importancia que se implemente políticas para limitar ataques por réplica.

| Servicio | Carácter | Mecanismos de seguridad | Comentarios |
|---|---|---|---|
| Autenticación | Obligatorio | WS-Security (UsernameToken) | Opción más segura que BasicAuth. Es de carácter obligatoria que la contraseña no vaya en abierto, usar por tanto Digest Access Authenticacion.<br>Aplicable a servicios SOAP. |
| | | SAML | Ideal sobre todo para entornos de SSO donde haya que orquestar llamadas a distintos servicios donde la ejecución de uno dependa del estado de otros.<br>Aplicable tanto a servicios SOAP como REST. |
| | | Mutual SSL | Permite restringir perfectamente los clientes consumidores de los servicios. Se trata de un mecanismo de seguridad basado en el intercambio de certificados |

| | | | |
|---|---|---|---|
| | | | entre servidor y clientes.<br>**OPCIÓN RECOMENDADA SOAP.** |
| | | Oauth 2.0 | Para aquellos sistemas orientados a la definición de aplicaciones basadas en APIs.<br>**OPCIÓN RECOMENDADA REST.**<br>Amplia difusión en la comunidad de desarrollo. A día de hoy no hay plataforma de desarrollo que no se precie a poder configurar este mecanismo de seguridad de forma ágil. |
| Confidencialidad e Integridad | opcional | WS-Security (XMLEncrypt) | Técnica de cifrado del mensaje para asegurar confidencialidad y que sólo pueda ser interpretado por el destinatario final. |
| | | WS-Security (XMLSign) | Técnica de firma del mensaje para asegurar integridad. |
| Definición de políticas | obligatorio | WS-Policy | Especificación de políticas de uso de los servicios:<br>• TimeStamp: Marca de tiempo del momento en el que se hace la petición. Para evitar ataques por Reply Attack.<br>• Addressing: información del destinatario y emisor de los mensajes.<br>• Expired: duración establecida para la descartarun mensaje.<br>**SOLO APLICABLE A SERVICIOS SOAP.** |

| | | | |
|---|---|---|---|
| No repudio | opcional | WS-Addresing + WS-Security + logs | Para aquellos servicios que requieran confirmación de la recepción y trazabilidad de peticiones. |

## 6. GLOSARIO

| Término | Definición |
|---|---|
| CPAI | Consejería de Presidencia, Administración Pública e Interior |
| OTI | Oficina Técnica de Interoperabilidad |
| ENS | Esquema Nacional de Seguridad |
| TIC | Tecnología de la Información y Comunicaciones. |
| STIC | Seguridad en la Tecnología de la Información y Comunicaciones |

# 7. ANEXO