

Catálogo de Estándares de Seguridad de Servicios de Interoperabilidad

Documento borrador

CTIC-IOP-P3-v.0.1



Abril de 2017

Índice de contenido

1. MARCO NORMATIVO REFERENCIAL.....	3
2. OBJETIVO.....	4
3. ALCANCE.....	4
4. DEFINICIONES.....	4
5.1. CARACTERÍSTICAS DE LOS SERVICIOS REST.....	5
5.2. CARACTERÍSTICAS DE LOS SERVICIOS SOA.....	6
6. CATÁLOGO DE ESTÁNDARES DE SEGURIDAD.....	7
7. REQUISITOS MÍNIMOS DE SEGURIDAD.....	9
8. REFERENCIAS.....	9

1. MARCO NORMATIVO REFERENCIAL

El Parágrafo II del Artículo 103 de la Constitución Política del Estado, establece que el Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.

Asimismo, el Parágrafo I del Artículo 85 de la Ley N° 031, de 19 de julio de 2010, Marco de Autonomías y Descentralización "Andrés Báñez", determina que dentro la competencias exclusivas del nivel central del Estado, se encuentra formular y aprobar el régimen general y las políticas de comunicaciones y telecomunicaciones del país, incluyendo el acceso al internet y demás Tecnologías de Información y Comunicaciones - TIC.

El Artículo 72 de la Ley N° 164, de 8 de agosto de 2011, de Telecomunicaciones, Tecnologías de Información y Comunicación, señala que las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las tecnologías de información, de manera prioritaria, haciendo énfasis en el área de gestión gubernamental, como mecanismo para atender la demanda social, facilitar el acceso y uso intensivo a nivel interno de cada unidad gubernamental, entre entidades gubernamentales, entre las ciudadanas y ciudadanos con las entidades gubernamentales, concordante con el Decreto Supremo N° 28168, de 17 de mayo de 2005, de Acceso a la Información, que dispone el derecho de acceso a la información a todas las personas, el cual sólo podrá ser negado de manera excepcional y motivada, únicamente respecto a aquella información que con anterioridad a la petición y de conformidad a leyes vigentes se encuentre clasificada como secreta, reservada o confidencial.

El Artículo 18 del Decreto Supremo N° 1793, de 13 de noviembre de 2013, Reglamento de la Ley N° 164, de 8 de abril de 2011, de Telecomunicaciones, Tecnologías de Información y Comunicación, señala que el Plan de Implementación del Gobierno Electrónico, deberá considerar minimamente los siguientes lineamientos: d) Proponer mecanismos para lograr eficiencia en el uso de los recursos tecnológicos de las entidades públicas, además de la interoperabilidad de los sistemas de información y de servicios gubernamentales desarrollados por cada una de ellas, a través de la aplicación y uso de estándares abiertos.

Finalmente, el Artículo 19 del Decreto Supremo N° 2514 de 9 de Septiembre de 2015, instituye a la AGETIC a coordinar con las entidades del sector público, la implementación de servicios de interoperabilidad de Gobierno Electrónico, así como los datos e información que deben estar disponibles, autorizando a las entidades públicas proporcionar a la AGETIC los datos e información que hubieran producido, recolectado o generado, por medios electrónicos o mecanismos de interoperabilidad, que ésta solicite mediante nota formal de su MAE, en el marco de la política general de Gobierno Electrónico, simplificación de trámites, transparencia, participación y control social y tecnologías de la información y comunicación; siendo el ente rector de Gobierno Electrónico, quien determinará la política general y normativa específica de interoperabilidad e intercambio de información y datos entre las entidades del sector público.

2. OBJETIVO

Conformar un catálogo de estándares recomendados para la seguridad de servicios de interoperabilidad en las instituciones del sector público.

3. ALCANCE

- Seguridad en servicios web.
- Se identifican normas y estándares nacionales e internacionales vigentes.

4. DEFINICIONES

Servicio de Interoperabilidad

Es una interfaz de software que describe un conjunto de operaciones a las cuales se puede acceder por la red.

Seguridad de Servicios de Interoperabilidad

Son mecanismos que garantizan la autenticación y la autorización del acceso a la información con la finalidad de preservar la integridad, disponibilidad y confidencialidad de la misma.

5. CARACTERÍSTICAS DE LOS SERVICIOS WEB

Integridad

Para lograr que los datos que se comparten a través de un servicio de interoperabilidad brinden el atributo de integridad entre los diferentes usuarios, se debe garantizar que los datos de origen y los de destino sean exactamente los mismos, para demostrar esta integridad de datos se utiliza un mecanismo de seguridad que permite a la entidad emisora añadir un hash o función matemática de resumen, que son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo) una salida alfanumérica de longitud fija que representa un resumen de toda la información, es decir que la entidad receptora a partir de los datos enviados por la entidad emisora crea una cadena única.

Confidencialidad

La confidencialidad permite mantener la información de forma exclusiva para los usuarios autorizados a manipularla, esto evita que alguien no autorizado pueda tener acceso a la información transferida, para ello se utilizan técnicas de cifrado o codificación de datos.

Disponibilidad

La disponibilidad es la capacidad de cumplir una función acordada (proveer el servicio) cuando es requerida.

Auditabilidad

Propiedad que asegura que cualquier acción sobre cualquier objeto parte de una infraestructura

tecnológica deje rastros o huellas de sus acciones a fin de establecer las responsabilidades reales de la operación.

Autenticación

Verificación de la identidad del usuario, proceso o servicio, como prerequisite para confiar el acceso a recursos en un sistema de información.

Autorización

Otorgar permisos para utilizar un recurso suministrado directa o indirectamente por una aplicación o el propietario de un sistema.

No repudiación

Asegurar que el emisor reciba prueba de envío y el receptor prueba de identidad del emisor, para que ninguno pueda negar tener la información y que esta sea correcta.

Criptografía

La solución adoptada para garantizar la seguridad en el uso de medios electrónicos está basada en la criptografía, es decir cifrar y descifrar información que hagan posible el intercambio de mensajes de manera que solo puedan ser leídos por las personas a quienes van dirigidos.

Firma digital

La firma digital es una herramienta que logra codificar los mensajes mediante un hash añadido a cada paquete de datos permite que el usuario final pueda verificar la integridad del mensaje.

5.1. CARACTERÍSTICAS DE LOS SERVICIOS REST

Validación

Validar todas las entradas en el servidor. Proteger su servidor contra ataques de inyección SQL o NoSQL.

Sesión de autenticación basada

Autenticación basada en sesión de uso para autenticar a un usuario cada vez que se realiza una solicitud a un método de servicio Web.

No hay datos sensibles en URL

Nunca usar nombre de usuario, contraseña o identificador de sesión en la URL, estos valores deben ser pasados al servicio web mediante el método POST.

Restricción de la ejecución del método

Permitir el uso restringido de métodos como GET, POST, DELETE. Método GET no debería ser capaz de eliminar datos.

Validar formato incorrecto en XML / JSON

Comprobar la entrada así formada se pasa a un método de servicio Web.

El tipo de mensajes de error genéricos

Un método de servicio web debe utilizar mensajes de error HTTP 403 como para mostrar el acceso prohibido.

5.2. CARACTERÍSTICAS DE LOS SERVICIOS SOA

WS Security

La especificación *WS-Security*, describe la forma de asegurar los servicios Web en el nivel de los mensajes, en lugar de en el nivel del protocolo de transferencia o en el de la conexión. Para ello, tiene como objetivo principal describir la forma de firmar y de cifrar mensajes de tipo SOAP. Las soluciones en el nivel de transporte actuales, como SSL/TLS, proporcionan un sólido cifrado y autenticación de datos punto a punto, aunque presentan limitaciones cuando un servicio intermedio debe procesar o examinar un mensaje. Por ejemplo, un gran número de organizaciones implementan un corta fuegos (firewall) que realiza un filtrado en el nivel de la aplicación para examinar el tráfico antes de pasarlo a una red interna.

Si un mensaje debe pasar a través de varios puntos para llegar a su destino, cada punto intermedio debe reenviarlo a través de una nueva conexión SSL. En este modelo, el mensaje original del cliente no está protegido mediante cifrado puesto que atraviesa servidores intermedios y para cada nueva conexión SSL que se establece se realizan operaciones de cifrado adicionales que requieren una gran cantidad de programación.

El estándar WS-Security se basa en estándares y certificaciones digitales para dotar a los mensajes SOAP de los criterios de seguridad necesarios. Se definen cabeceras y usa XML Signature para el manejo de firmas en el mensaje. El cifrado de la información la realiza mediante XML Encryption. Hace uso del intercambio de credenciales de los clientes.

WS-Policy

Es la especificación encargada de delimitar las diferentes políticas aplicables a los servicios Web. Es de vital importancia a la hora de integrar los servicios Web, ya que si presentan cierta complejidad, es muy necesario conocer los detalles del XML que lo define, además de otros requisitos o capacidades adicionales.

Si se produce un intento de integrar un servicio sin conocer los detalles de su implementación probablemente se este evocando al fracaso. Por lo tanto es muy necesario realizar un estándar que

defina las diferentes políticas a acordar. Sin él, los desarrolladores quedarían expuestos a realizar desarrollos sin integración y difícilmente escalables.

Un marco de trabajo de políticas permitiría a los desarrolladores expresar las políticas de los servicios de una forma procesable por las computadoras. La infraestructura de los servicios Web puede verse ser mejorada para entender ciertas políticas y forzar su uso en tiempo de ejecución.

WS-Trust

La especificación *WS-Trust* permite definir extensiones al estándar *WS-Security* con el objetivo claro de dotar a este de nuevos mecanismos de seguridad. En esta especificación se incluye el proceso de solicitud, emisión y control sobre *tokens* de seguridad y se permite la gestión de las relaciones de confianza entre los servicios.

WS-Security, realiza una definición amplia de los mecanismos básicos para proporcionar un entorno de trabajo seguro en el intercambio de mensajes. Esta especificación, partiendo de los mecanismos básicos, va añadiendo primitivas adicionales junto con extensiones para estandarizar el intercambio de tokens de seguridad. Con ello se busca optimizar la emisión y propagación de las credenciales de los servicios dentro de diferentes dominios de confianza.

WS-Federation

Con frecuencia se produce la situación de que participantes en el consumo y la prestación de un servicio pueden utilizar diferentes tecnologías de seguridad, por ejemplo, una de las partes podrá utilizar Kerberos y otro Certificados X.509, podría necesitarse una traducción de los datos que afectan a la seguridad entre las partes afectadas.

Una federación es una colección dominios de seguridad que han establecido relaciones en virtud del cual un proveedor de uno de los dominios puede proporcionar acceso autorizado a los recursos que gestiona sobre la base de la información de los participantes (como puede ser su identidad) la cual debe ser afirmada por un proveedor de identidad (Security Token Service).

WS-Federation es la especificación que describe la forma de llevar a cabo la intermediación entre los participantes. Esta especificación tiene como objetivo principal ayudar a la definición de los mecanismos de federación de dominios de seguridad, ya sean distintos o similares. Para ello, define, categoriza e intermedia con los niveles de confianza de las identidades, atributos, y autenticación de los servicios Web de todos los colaboradores.

En la especificación WS-Federation se definen perfiles asociados a las entidades que servirán para clasificar los solicitantes que pueden adaptarse al modelo. Es por tanto un objetivo prioritario de esta especificación habilitar la federación de la información de las identidades, atributos, autenticación y autorización.

WS-Addressing

WS-Addressing ofrece seguridad de extremo a extremo a la mensajería SOAP . Independientemente de los tipos de intermediarios como puertos, workstations, cortafuegos, etc. que sean atravesados por un

bloque en el camino al receptor, todo aquel que se encuentre por el camino sabrá:

- (Dirección postal) La dirección a donde se supone que va
- (Att) La persona o servicio específico en esa dirección que se supone va a recibirlo
- Dónde debería ir si no puede ser remitido como estaba previsto
- Todo esto lo incluye en la cabecera del mensaje SOAP

6. CATÁLOGO DE ESTÁNDARES DE SEGURIDAD

El catálogo de estándares de seguridad es presentado a continuación como un listado de los estándares en temas de seguridad utilizados que se recomienda utilizar en interoperabilidad:

CATEGORÍA	NOMBRE COMÚN	NOMBRE FORMAL	TIPO	VERSIÓN MINIMA	EXTENSIÓN
Autenticación Firma Digital	PKCS#7	PKCS #7: Cryptographic Message Syntax. Version 1.5	Abierto	RFC 2315	
Autenticación Firma Digital	XAdES	ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)	Abierto	1.2.2.	.xml .dsig .xsig
Autenticación Firma Digital	XML-DSig	XML Signature Syntax and Processing.	Abierto	Second Edition. 2008	.xml .dsig .xsig .sig
Firma digital	PKI	Internet X.509 Public Key Infrastructure	Abierto	RFC 3280, RFC 6187	
Autenticación - Política Firma Digital	ETSI TR 102 038	ETSI TR 102 038 TC Security - Electronic Signatures and Infrastructures (ESI);XML format for signature policies	Abierto	RFC 3125 1.1.1	
Autenticación - Política Firma Digital	ETSI TR 102 272	ETSI TR 102 272 Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies	Abierto	1.1.1.	

Cifrado	SSH	Secure Shell	Abierto	1.99 (SSH 2) RFC 4253
Cifrado	TLS	Transport Layer Security (TLS)	Abierto	RFC 5878, RFC 5746, RFC 5705, RFC 5489, RFC 5487, RFC 5469, RFC 5289, RFC 5288
Integridad	SHA	Secure Hash Algorithms	Abierto	RFC 4634, RFC 3874
Autenticación - Certificados	OCSP	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	Abierto	RFC 2560
Autenticación - Sellado de tiempo	ETSI TS 102 023	ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities	Abierto	RFC 3628
Autenticación	JWS	JSON Web Signature	Abierto	RFC 7515
Autenticación	JWT	JSON Web Token	Abierto	RFC 7519
Protocolos de comunicación e intercambio - Servicios Web	WS-Security	Web Services Security	Abierto	1.1

7. REQUISITOS MÍNIMOS DE SEGURIDAD

La entidad pública que provea un recurso o servicio web debe considerar en el mismo los siguientes aspectos (entre otros):

- Para consumir el servicio se debe requerir obligatoriamente la autenticación del usuario que lo consume, debiendo almacenar dicha información y otra (por ejemplo la dirección IP desde la cual se conecta, fecha y hora, entidad a la que corresponde el usuario o token, etc.) como pistas de auditoría para su consulta futura en caso de ser requerido.
- El mecanismo o procedimiento para otorgar accesos para el consumo de los servicios *web* es

responsabilidad de la entidad que publica el servicio, pero es necesario que se establezcan mecanismos robustos de seguridad que impidan el acceso a información relacionada cuentas de usuario, contraseñas o *tokens*.

- Se deben aplicar mecanismos que permitan a la entidad que consume el servicio la verificación de la integridad de la información provista por el mismo.
- Dependiendo de la clasificación de la información provista, corresponde a la entidad que publica el servicio establecer las medidas adicionales de seguridad, como ser cifrado, sellado de tiempo, firma digital, etc.

8. REFERENCIAS

W3C

La W3C nace con un objetivo claro, ser un foro de discusión abierto y fomentar la interoperabilidad en la evolución técnica que se produce en el mundo Web. En un periodo de tiempo menor a diez años, se han generado más de cincuenta especificaciones técnicas que están orientadas a la estandarización de la infraestructura Web.

Guía de aplicación de la Norma Técnica de Interoperabilidad

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiXydjPIpZTAhUI4SYKHXAuB6UQFggwMAE&url=https%3A%2F%2Fadministracionelectronica.gob.es%2Fpae_Home%2Fdms%2Fpae_Home%2Fdocumentos%2FEstrategias%2Fpae_Interoperabilidad_Inicio%2FNormas_tecnicas%2FGuia_de_aplicacion_NTI_catalogo_de_estandares_Publicacion_oficial_2012%2FGuia_aplicacion_Norma_Tecnica_Interoperabilidad_Catalogo_de_estandares.pdf&usg=AFQjCNEt2wnMPNvMyGNTiN4FYIXdcAoHNng&sig2=PuTZVz-b4AlBvdClcWqIMA

Norma para la Interoperabilidad entre los organismos del gobierno Dominicano

<http://optic.gob.do/nortic/images/documentos/normas/nortic-a4-1-2014.pdf>

Revista de seguridad web - El Cifrado Web (SSL/TLS)

<http://revista.seguridad.unam.mx/node/2157>

Autenticación y Autorización - Seguridad en servicios web. Autenticación y autorización.

<https://desarrolloweb.com/articulos/1640.php>

Seguridad en Servicios Web REST

http://www.es.w3eacademy.com/restful/restful_security.htm