UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA
Tecnología & Desarrollo
Vol. 14, Nº 1, Enero - Diciembre 2016, Pág.127-140

La cadena de seguridad y control en servicios web

Security and control in web services

Segundo Edwin Cieza Mostacero[1]

RESUMEN

El presente trabajo busca definir y explicar las diferentes perspectivas de la seguridad en la información de los Servicios Web, teniendo como base los conceptos, protocolos, servicios, normatividad y soluciones informáticas (basado en caso de estudio) en el año 2016 que permiten verificar la operatividad de un servicio web.

Palabras clave: Servicio web, Protocolo, Normatividad.

ABSTRACT

The present work seeks to define and explain the different perspectives of information security in the Web Services, based on the concepts, protocols, services, regulations and IT solutions (based on a case study) in 2016 that allow to verify the Operability of a web service.

.

Keywords: Web service, Protocol, Normativity.

Recepción: 18-08-2016 / **Aceptación:** 16-09-2016

[1] Universidad César Vallejo - Escuela de Ingeniería de Sistemas.
E-mail: sciezam88@ucvvirtual.edu.pe

1. INTRODUCCIÓN

Actualmente se define como servicio web a una interfaz modulable que permite que se invoque, se publique y se localice dentro de la red; intercambiando mensajes a través de XML estandarizados.

Los servicios web se utilizan desde hace mucho tiempo, sin embargo ¿qué nos garantiza que la información que trasmitimos y recibimos es segura o confiable?; es importante saber si dichos servicios web cumplen con los elementos de seguridad básicos en control de información tales como: Autenticación de servicios, autenticación de usuarios, integridad o confiden - cialidad. Actualmente, existen diferentes mecanismos de seguridad en servicios web tales como: http Autenticación, SSL X509 Certificate, SAML, SSL, WS-Signature o WS Encryption que se recomiendan verificar para garantizar los controles de la seguridad de la información en dichos servicios web.

1.1. Objetivo

El presente trabajo de investigación tiene como objetivo general determinar los conceptos generales de la seguridad y controles de la información en los servicios web, enfocándose en un marco teórico, elementos de seguridad, mecanismos de seguridad, normatividad y aplicaciones tecnológicas al año 2016.

1.2. Objetivos específicos

- Analizar las teorías relacionadas con la seguridad de los servicios web
- Determinar las instituciones que regulan la normatividad de seguridad y control de los servicios web en Perú.
- Conocer las amenazas de seguridad de los servicios web.
- Conocer los estándares sobre la seguridad en los servicios web.

2. LOS WEB SERVICES

Actualmente, se define a un servicio web como una interfaz modulable que permite que se invoque, se publique y se localice dentro de la red; intercambiando mensajes a través de XML estandarizados.
Los Servicios Web son capaces de ofrecer algunas ventajas características con respecto a los modelos tradicionales de arquitectura distribuidos como CORBA y EJB. Se pueden reseñar algunas representativas como:

- Permite la coexistencia a diferentes tecnologías.
- Comunicación entre aplicaciones que se han desarrollado mediante diferentes lenguajes de programación.
- Permite la transmisión mediante el protocolo HTTP
- Estandariza la localización de los servicios.

Los servicios web se basan en estándares[2] y protocolos abiertos. A continuación se describen los estándares de forma breve:

- Extensible Markup Language (XML): Basado en marcas y etiquetas, es muy frecuente el uso de este metalenguaje para crear otros lenguajes con entidad propia. Su simpleza, facilita su uso fundamentalmente en el intercambio de una gran variedad de datos.
- Simple Object Access Protocol (SOAP): Este protocolo permite realizar intercambios de información entre diversas aplicaciones situadas en entornos que están descentralizados y se encuentran distribuidas. Los diferentes mensajes, codificados en XML, se integran dentro de mensajes SOAP. Hay multitud de tipos de mensajes que se pueden integrar dentro de SOAP (respuestas tras el uso de un servicio, información de errores, estado del servicio, enlaces, datos distintos al formato XML (MIME). SOAP es independiente del sistema permitiéndole comunicar aplicaciones que se encuentren implementadas en diferentes lenguajes de programación. ¿También puede atravesar cortafuegos corporativos y ofrece la interoperabilidad de las aplicaciones. con la competitividad de las PYMES del sector calzado de la provincia de Trujillo en el año 2016?
- Universal Description Discovery and Integration (UDDI): Se encarga de la publicación, localización y enlazado de los Servicios Web. El principal objetivo que tiene UDDI es permitir, mediante el uso de unos criterios de selección para la búsqueda, el localizarse a las diferentes entidades de negocio
- Web Service Description Language (WSDL): Es el estándar que se utiliza para describir un Servicio Web. Está basado en XML y permite especificar cómo deben representarse los parámetros, tanto de entrada como de salida, en una invocación de tipo externo al servicio. Permite comprender cómo operar con el Servicio Web, a los diferentes clientes (Figura 1):
-

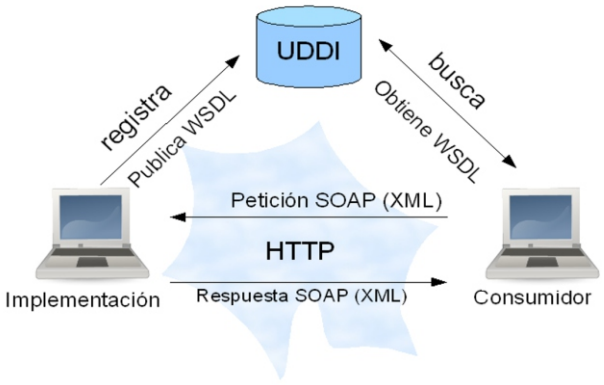

Figura 1: Implementación de un servicio web
Fuente: http://es.slideshare.net/maxt_15/presentacin-servicios-web

3. LA SEGURIDAD EN LOS SERVICIOS WEB

- Como objetivos básicos a cubrir por la seguridad de un servicio web:
- 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 SOAP (Simple Object Access Protocol) 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.

Los elementos de seguridad que debe de manejar los servicios web se pueden rescatar los siguientes:

- Autenticación de servicios.
- Autenticación de usuarios
- Integridad
- No repudio
- Confidencialidad

Para trabajar con los elementos de seguridad (antes mencionados), se tienen mecanismos de seguridad específicos para trabajar con los servicios, tales tenemos:

- Http autenticación
- SSL X509 Certifcate
- WS – Security Tokens
- SAML
- SSL
- WS-Signature
- WS-Policy

A continuación se ofrece una tabla resumen con los principales elementos de seguridad dentro de los servicios Web, así como las recomendaciones de maneja al respecto (Figura 2).

Elemento de seguridad	Mecanismo de seguridad	Carácter
Autenticación de servicios	Http autentication	No recomendado
	SSL X509 certificate	No recomendado
	WS-Security Tokens	Recomendado
Autenticación de usuarios	SAML	Recomendado
Integridad	SSL	Recomendado
	WS-Signature	
No repudio	WS-Signature WS-Adressing Logs	Recomendado
Confidencialidad	SSL	Recomendado
	WS-Encryption	
Política de seguridad	WS-Policy	Recomendado

Figura 2: Principales elementos de seguridad en servicios web
Fuente: http://es.slideshare.net/maxt_15/presentacin-servicios-web

4. ESTADO DEL ARTE: BASES TEÓRICAS

Permite conocer las teorías de la rama, interpretando y aplicando aquellas que propicien alcanzar el objetivo principal del presente trabajo. Asimismo permiten encaminar el proceso metodológico que se sigue para configurar de manera concreta el tema de investigación. Conforman la base teórica, referente a la Variable Independiente, las investigaciones de:

4.1 ONGEI 21/10/2011: Gobierno oficializa creación de la Plataforma de Interoperabilidad del Estado (PIDE)

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), es el Órgano Técnico Especializado que depende directamente del Despacho de la Presidencia del Consejo de Ministros (PCM).

ONGEI, en su calidad de ente rector del sistema nacional de informática, se encarga de liderar los proyectos, la normatividad, y las diversas actividades que en materia de

Gobierno Electrónico realiza el Estado. Entre sus actividades permanentes se encuentran las vinculadas a la normatividad informática, la seguridad de la información, el desarrollo de proyectos emblemáticos en Tecnologías de la Información y la Comunicación (TIC), brindar asesoría técnica e informática a las entidades públicas, así como, ofrecer capacitación y difusión en temas de Gobierno Electrónico y la modernización y descentralización del Estado.

En el 2011, El Poder Ejecutivo oficializó la creación de la Plataforma de Interoperabilidad del Estado (PIDE) que permitirá ofrecer servicios públicos y el intercambio electrónico de datos a través de internet y telefonía móvil, a favor de los ciudadanos.
Mediante decreto supremo 083-2011-PCM, queda establecido que la PIDE forma parte del proceso de modernización de la gestión del Estado y participarán de la plataforma todas las entidades integrantes de Sistema Nacional de Informática.

Servicios que brindan:

Nº	SERVICIOS WEB (UDDI)	DESCRIPCION
1.	Código único de operación - CUO	Es un código de 10 dígitos que permite tener la trazabilidad de los servicios públicos interoperables, a nivel de entidades públicas.
2.	Consulta de DNI	Permite tener los apellidos y nombres de los ciudadanos, dado el número de DNI.
3.	Servicio de mensajes de texto – SMS	Permite enviar mensajes SMS en forma automatizada a un grupo de números de teléfonos móviles, desde un sistema de información.
4.	Consulta de RUC	Dado el número de RUC, se obtiene el nombre del contribuyente, estado, dirección y otros datos.
5.	Generación de RUC	Es un servicio web elaborado para el Servicio de Constitución de Empresas en Línea, dado el envío de SUNARP, de los datos de la nueva empresa, genera el RUC en menos de 8 segundos, comparado a las 3 horas promedio por trámite tradicional.
6.	Envió de partes de embargos de inmuebles	Servicio que permite él envió de documentos electrónicos entre SUNAT (embargos inmuebles) y SUNARP.
7.	Consulta de placas vehiculares, conductores infractores (MTC).	Permite consultar licencias de conductor, papeletas y Sanciones.
8.	Convertidor de monedas	Dado un tipo de moneda origen y una destino se obtiene el tipo de cambio.
9.	Clima de ciudades	Dado el nombre de País y ciudad, se obtiene datos del clima en línea.
10.	Funcionarios de entidades publicas	Mediante el RUC como campo clave muestra la lista de funcionarios incluyendo cargos, resolución de designación, teléfono y correo institucional.
11.	Catálogo de servicios en línea	El servicio muestra por medio del ruc de entidad, el listado de Servicios en línea de la misma, registrados en el Portal de Servicios al Ciudadano y Empresas - PSCE
12.	Envío de partes notariales electrónico, consulta de partidas registrales	Servicio que permite el envío de documentos electrónicos entre Colegio de Notarios de Lima (Constitución de Empresas) , SUNAT (embargos) y SUNARP
13.	Ejecutoras por año	Consulta SNIP por unidades ejecutoras por año, usado en el aplicativo Sayhuite
14.	Fuentes por año	Consulta SNIP por fuentes presupuestales por año, usado en el aplicativo Sayhuite.
15.	Proyectos por año	Consulta de proyectos por año, usado en el aplicativo Sayhuite.
16.	Rubros por año	Consulta de rubros por año del SNIP, usado en el aplicativo Sayhuite.
17.	Sectores por año	Consulta de proyectos por sectores y año, usado en el aplicativo Sayhuite.
18.	Gasto PIP por año y nivel de gobierno	Consulta de gastos sobre Proyectos de Inversión, por niveles de gobierno, usado en el aplicativo Sayhuite.
19.	SNIP por código	Consulta de proyectos de Inversión Pública por Código, usado en el aplicativo Sayhuite.
20.	Licencia de funcionamiento municipal en línea / trámite	Integración del Sistema de Trámite Documentario de la Municipalidad con Sistema de Licencia de Funcionamiento Municipal en Linea - PCM.
21.	Licencia de funcionamiento municipal en línea / pago de servicio	Integración del Sistema de Caja (Pago) de la Municipalidad con el Sistema de Licencia de Funcionamiento Municipal en Linea- PCM.

22.	Integración del Sistema de Licencia de Funcionamiento de la Municipalidad con el Sistema de Licencia Funcionamiento	Integración del Sistema de Licencia de Funcionamiento de la Municipalidad con el Sistema de Licencia de Funcionamiento Municipal en Linea de PCM.
23.	Relación de Comisarías	Permite obtener el nombre, la dirección y los teléfonos de todas las comisarías de Lima y Callao.
24.	Establecimientos médicos	Permite obtener el nombre, la dirección y los teléfonos de todos los establecimientos médicos de Lima y Callao
25.	Funcionarios principales	Permite retornar la lista de funcionarios principales del Portal del Estado Peruano - PEP, de la entidad seleccionada
26.	Catálogo de servicios	Permite retornar la lista de servicios registrados en catálogo del Portal de Servicios al Ciudadano y Empresas - PSCE, de la entidad seleccionada
27.	Clasificador de trámites	Permite retornar el clasificador de trámites del Portal de Servicios al Ciudadano y Empresas - PSCE, de la entidad seleccionada
28.	Tipo de cambio / UIT	Permite retornar el tipo de cambio y el UIT del Portal del Estado Peruano - PEP

Tabla 1 : Servicios ONGEI - PIDE
Fuente: http://www.ongei.gob.pe/interoperabilidad/

Norma ISO 27001 - 2008:
La norma ISO 27001 se publicó en octubre de 2005, fundamentalmente la sustitución de la antigua norma BS7799-2. Es la especificación para un SGSI, un Sistema de Gestión de Seguridad de la Información. Sí BS7799 era una norma de larga data, publicado por primera vez en los años noventa como un código de prácticas. Como este maduró, una segunda parte surgió para cubrir los sistemas de gestión. Es esto en contra de la cual se otorga la certificación. Hoy en día más de mil certificados están en su lugar, en todo el mundo. El objetivo de la norma misma es "proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI)". En cuanto a su adopción, esto debería ser una decisión estratégica. Además, "El diseño y la aplicación de la información del sistema de gestión de seguridad de una organización están influenciados por las necesidades de la organización y los objetivos, requisitos de seguridad, los procesos organizativos utilizados y el tamaño y la estructura de la organización".
Se ofrece un repaso de las principales iniciativas, en forma de consorcios u organizaciones, que están implicadas en los servicios Web en general y en el aspecto de su seguridad en particular.

4.3 Consorcio World Wide Web (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[2,10].
Se definen como objetivos a largo plazo en W3C:
- Acceso Universal. Permitir que el acceso a la web sea para todos. Realizando un esfuerzo por las tecnologías que consideran las diferentes lenguas, culturas, capacidades, educación, recursos disponibles o las disminuciones físicas o psíquicas de cada uno.
- Web Semántica. Ofrecer y desarrollar avances en el mundo WEB que permitan a los usuarios disfrutar del mejor uso posible de los recursos disponibles en la web, adaptándolo a las necesidades de cada usuario.
- Web de Confianza. Crear un desarrollo web, que permita realizar desarrollo manteniendo unos criterios comerciales y sociales adecuados.

4.4 OASIS (Organization for the Advancement of Structured Information Standards)
OASIS, es un organismo global muy centrado en temas de comercio electrónico. Es un organismo sin ánimo de lucro. Oasis trata de establecer estándares de forma abierta y mediante procesos ligeros aplicados por sus miembros, tratando temas referentes a la seguridad, servicios Web, edición digital, tratamiento de XML, etc[5].

4.5 IBM/Microsoft/Verisign/RSA Security
Mediante un proceso de colaboración entre las principales compañías dentro del ámbito IT, siendo encabezadas por Microsoft e IBM, se han propuesto una serie de especificaciones acerca de cómo afrontar la seguridad en los servicios Web. Dentro de este conjunto de especificaciones se encuentra la especificación WS-Security estandarizada por OASIS[4].

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 encriptar mensajes de

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[3]. 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. La encriptación de la información la realiza mediante XML Encryption. Hace uso del intercambio de credenciales de los clientes.

WS-Addressing, desempeña un papel fundamental en la seguridad en el nivel de los mensajes puesto que proporciona los mecanismos para enviar los mensajes de un modo independiente del transporte. Esto permite enviar un mensaje seguro a través de cualquier transporte y enrutarlo con facilidad. La protección del mensaje en lugar del uso del protocolo de transporte ofrece varias ventajas[2]:

En primer lugar, resulta más flexible puesto que se pueden firmar o cifrar partes del mensaje en lugar del mensaje completo. De este modo, los intermediarios pueden ver las partes del mensaje destinadas a ellos. Un ejemplo de esto sería un servicio Web que en ruta mensajes SOAP y puede inspeccionar las partes no cifradas de los mismos para determinar a dónde enviarlos, mientras que otras partes permanecen cifradas.

En segundo lugar, los intermediarios pueden agregar sus propios encabezados al mensaje y firmarlos para llevar a cabo el registro de auditorías. Por último, esto implica que el mensaje protegido se puede enviar a través de diferentes protocolos, como SMTP, FTP y TCP, sin necesidad de basarse en el protocolo para la seguridad

Cómo funciona WS-Security
WS-Security define la forma de conseguir integridad, confidencialidad y autenticación en los mensajes SOAP.

Se realiza de la siguiente manera:

- La autenticación se ocupa de identificar al llamador.
- WS-Security utiliza tokens de seguridad para mantener esta información mediante un encabezado de seguridad del mensaje SOAP.
- La integridad del mensaje se consigue mediante firmas digitales XML, que permiten garantizar que no se han alterado partes del mensaje desde que lo firmó el originador.
- La confidencialidad del mensaje se basa en la especificación XML Encryption y garantiza que sólo el destinatario o los destinatarios a quien va destinado el mensaje podrán comprender las partes correspondientes.
- Se apoya en WS-Adressing para asegurar el no repudio.

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 esté 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.

Como funciona WS-Trust
Esta especificación da soporte a un modelo de confianza destinado a los servicios Web, se le denomina Web Services Trust Model. Para ello, define un proceso a través

del cual, un servicio, puede solicitar que cualquier petición que le llegue cumpla con una serie de reclamaciones. En la situación, que un solicitante no disponga de todos los requerimientos necesarios, los solicita al Servicio de tokens de seguridad (STS). Existe una relación de confianza entre el STS y el servicio
La especificación define varios mecanismos para verificar relaciones de confianza entre dos partes. Sin embargo, no se restringe solo a ellos, pudiendo un servicio verificar la relación de confianza con la otra parte como considere necesario. Los métodos que definen son los siguientes[8]:

- Fixed Trust Roots: El más simple. El servicio mantiene un conjunto fijo de relaciones de confianza.
- Trust hierarchies: El servicio confiara en los tokens siempre que vengan de una jerarquía de confianza que lleve a un trust root.
- Authentication Service: Es un servicio con el cual el servicio mantiene una relación de confianza. Cuando llega un security token, el servicio lo envía al Authentication Service el cuál enviará probablemente otro token que aprobará o no la autenticación

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.

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[7]:

- De donde viene.
- (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.
- Donde debería ir si no puede ser remitido como estaba previsto.
- Todo esto lo incluye en la cabecera del mensaje SOAP.

5. LA SEGURIDAD EN LA ARQUITECTURA DE REFERENCIA DE LOS SERVICIOS WEB

Siguiendo el modelo W3C, vamos a realizar un pequeño estudio sobre los requisitos de seguridad que se encuentran enumerados dentro de la arquitectura de referencia de los servicios web y señalando las diferentes tentativas de ataque que también aparecen dentro de la especificación. Se ofrecerán soluciones para las mismas[4].

5.1 Servicios de seguridad básicos
La seguridad es un concepto considerado clave dentro de los que comprenden el aseguramiento de calidad dentro del servicio Web. Si se realiza una catalogación básica de los servicios de seguridad son la confidencialidad, integridad, autenticidad de origen, no repudio y control de acceso. A continuación se explica brevemente cada uno de ellos[7]:
Autenticación de los participantes. Los servicios Web por definición tienen mucha heterogeneidad[3], lo que provoca que los sistemas de autenticación tengan que ser flexibles. Si imaginamos un servicio Web que necesita comunicarse con otro servicio, este podría solicitar al demandante credenciales junto a una demostración de que es el propietario de las mismas. Resulta necesario conseguir una estandarización de los protocolos y en los formatos a utilizar. Otro problema remanente es definir un modelo de autenticación Single Sign-On de forma que un servicio que necesita comunicarse con otros servicios Web,no tenga la necesidad de estar continuamente autenticándose y logre completar el proceso de negocio en un tiempo de respuesta aceptable.

Autorización. Con frecuencia, es necesario aplicar unos criterios que permitan controlar el acceso a los diferentes recursos. Es necesario definir los usuarios que pueden realizar diversas acciones sobre los diferentes recursos. En combinación con la autenticación, permite a las identidades conocidas realizar las acciones para las que tienen permisos. Con frecuencia se definen políticas de acceso en base a jerarquías.

Confidencialidad. Es necesario asegurar que el contenido incluido en los mensajes que se intercambian se mantiene como información.

Integridad. Esta propiedad garantiza que la información que se ha recibido, es exactamente la misma que se envió desde el cliente.

No repudio. En una comunicación que se realizan transacciones, es necesario registrar que las mismas se han producido y registrar el autor que lo ejecutó. En el caso de los servicios Web, trasladamos esta política al uso del servicio. Se comprueba que cierto cliente hizo uso de un servicio a pesar de que éste lo niegue (no repudio del solicitante) así como probar la ejecución se llevó a cabo (no repudio del receptor).

Disponibilidad. Uno de los ataques más frecuentes a las aplicaciones se basa en la denegación de servicios. Se lanzan múltiples solicitudes falsas para inundar el servicio y provocar su caída. Es necesario contemplar la disponibilidad, como punto muy importante en el diseño

de servicio web, ya que permiten cierta redundancia de los sistemas.

Auditabilidad. El registro de las acciones en los servicios Web permite mantener una traza de las mismas de manera que se puedan realizar análisis posteriores de los datos.

Seguridad extremo-a-extremo. Cuando se ejecuta un servicio es necesario garantizar la seguridad durante todo el recorrido que efectúan los mensajes.

5.2 Requisitos de seguridad

Si realizamos una abstracción sobre la problemática, el objetivo principal es conseguir un entorno para las transacciones y los procesos que sea seguro para todo el canal de comunicación. Obviamente, es necesario garantizar la seguridad durante el tránsito de la comunicación, ya sea con intermediarios o sin ellos durante la misma. Por otra parte, se necesita asegurar la seguridad de la información en los procesos de almacenamiento: A continuación se ofrece una revisión breve de los principales requisitos para asegurar la seguridad en la comunicación.

• Mecanismos de autenticación

La autenticación es obligatoria para mantener control y verificar la identidad de solicitantes y proveedores. En algunas ocasiones, resultará necesario realizar una autenticación tanto del solicitante como del proveedor, ya que puede producirse que los participantes no estén en conexión directa. Pueden existir intermediarios que retransmitan la comunicación

• Autorización

La autorización resulta necesaria para efectuar un control sobre el acceso a los recursos. Una vez se ha realizado la autenticación sobre el participante y se conoce su identidad, se utilizarán los mecanismos de autorización para realizar las comprobaciones pertinentes y asegurar el acceso adecuado al recurso por parte del participante.

• Integridad y confidencialidad de los datos

El proceso que mantiene la integridad de los datos, garantiza que la información que se ha enviada no ha sufrido ninguna transformación sin que se haya detectado. La confidencialidad, asegura los principios de intimidad de la información. Es decir, solo se permite el acceso a la información a aquellos participantes con permisos para hacerlo. Con frecuencia, se usan técnicas de cifrado para conceptos de confidencialidad y la firma digital para temas de integridad[1].

• No repudio

El objeto de las técnicas de no repudio ya se han comentado anteriormente, es registrar la participación y el grado de la misma de los diferentes interlocutores en una transacción para protegerlo de una posible denegación, posiblemente por parte de algún interlocutor de la misma, negando de que la transacción ocurrió o de su participación en la misma.

Las técnicas de no repudio permiten proporcionar evidencias sobre lo sucedido en la transacción, de manera que una tercera parte resuelve el desacuerdo producido.

Para garantizar el no repudio dentro de las comunicaciones por Servicios Webs, 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", deberán ser firmados según los procedimientos recogidos en la especificación WS-Security. Por último, los mensajes deberán ser almacenados en ficheros de logs, para su posterior consulta[11].

• Rastreabilidad

Es necesario ajustar trazas que aseguren poder conocer información del acceso una vez se haya producido este, y comprobar el comportamiento que ha tenido el usuario que ha realizado el acceso. Son de especial importancia para verificar la integridad del sistema.

• Aplicación distribuida de las políticas de seguridad

Si se han definido arquitecturas que están basadas en Servicios Web, están deben permitir la definición de políticas de seguridad y comprobar su cumplimiento en las diversas plataformas y con las diversas variaciones de acceso al servicio.

• Uso de políticas

Los mensajes que se envían en la comunicación de los servicios Web atraviesan los cortafuegos y pueden ser modificados a través de los diferentes puertos y protocolos existentes. Es necesario, para asegurar la calidad de seguridad en los servicios Web, crear políticas corporativas para integrarse con las diversas políticas de los proveedores y con la gestión de la confianza planificada.

• Políticas distribuidas

Con frecuencia, se asocian las políticas de seguridad a los proveedores o a los clientes o a un mecanismo de descubrimiento. Se utilizan para controlar y definir la metodología de acceso de las peticiones y las respuestas a las mismas, dadas por los involucrados en la comunicación.

• Políticas de confianza

Defiendo de manera simple una política de confianza como una política distribuida que asegura a dos entidades que afrontan una interacción sin conocerse previamente. Mediante el uso de credenciales, asumen el nivel de seguridad que pueden soportar.

• Mecanismo de descubrimiento seguro
El mecanismo de descubrimiento seguro controla las publicaciones y apariciones de un servicio. Cuando aparece un servicio, es necesario realizar una evaluación de las políticas de publicación del servicio, exceptuando las situaciones que supongan un servicio de descubrimiento entre nodos.

• Confianza y descubrimiento
Si imaginamos una situación donde un cliente descubre que existe un servicio Web muy necesario para él, y el proveedor del mismo, es una entidad desconocida hay que preguntarse qué nivel de confianza puede otorgar el solicitante a ese servicio.

• Privacidad
La privacidad se expresa mediante las diferentes políticas definidas por los diferentes propietarios de los datos. Con frecuencia, los propietarios son los usuarios de los servicios Web.

• Fiabilidad de los servicios Web
La aparición de errores es inevitable, especialmente si consideramos que el contexto engloba a multitud de servicios interconectados por una red global que pertenecen a todo tipo de personas y entidades. La eliminación de errores no puede ser completa, así que el objetivo principal es reducir la tasa de errores que aparecen al nivel máximo posible. especificación. Se ofrecerán soluciones para las mismas[4].

5.3 Amenazas de seguridad
Si analizamos el concepto de amenaza de seguridad, tendemos a asumir que existirá un intento de acceso y mal uso de los servicios. Por lo tanto hay que realizar un esfuerzo para controlar los accesos no permitidos. Si realizamos una clasificación de las principales amenazas, tenemos lo siguiente:

- Acceso no permitido llevado a cabo por entidades sin identificar. Es necesario poder identificar de forma confiable la identidad de proveedores, servicios, etc.
- Alteración de la información en el canal de comunicación. Es necesario garantizar la integridad de la información que se envía.
- Debe asegurarse el acceso a la información. Solo pueden acceder las partes deseadas.
- Debe de mantenerse una certeza del contenido y de que la comunicación tuvo lugar.
- Denegación de servicio. No debería ser posible que los clientes de los servicios no puedan acceder a él.

Tipos de ataques
Los tipos de ataques que se listan a continuación están extraídos de la especificación W3C.

Alteración de los mensajes
Es un tipo de ataque centrado sobre la integridad de los mensajes. Se busca modificar el contenido del mensaje (ya sea parcialmente o totalmente). En el caso que el atacante tuviera controlado un canal de comunicaciones entre servicios podría modificar los mismos, eliminarlos, capturarlos y reenviarlos[9].

Ataques a la confidencialidad
Centrados en la captación de la información contenida dentro de los mensajes. En ocasiones puede existir información muy sensible (datos médicos, datos económicos, etc...)

Hombre en el medio o 'man- in-the-middle.
Es la infiltración por parte de un atacante entre los participantes de una comunicación. Normalmente, intercepta la comunicación y suplanta a los participantes de manera que estos creen que se comunican entre sí cuando lo hacen con el atacante.
La posibilidad de un ataque de intermediario sigue siendo un problema potencial de seguridad serio, incluso para muchos sistemas criptográficos basados en clave pública.

Suplantación de identidad (Spoofing)
Es un ataque orientado a los niveles de confianza que se establecen en la comunicación. El atacante suplanta la identidad de uno de los participantes en una relación de confianza, usualmente trata de comprometer al destinatario de la comunicación. Es muy útil utilizar una robusta autenticación para fortalecer el servicio ante estos ataques.
Para evitar ataques de spoofing exitosos contra nuestros sistemas podemos tomar diferentes medidas preventivas; en primer lugar, parece evidente que una gran ayuda es reforzar la secuencia de predicción de números de secuencia TCP. Otra medida sencilla es eliminar las relaciones de confianza basadas en la dirección IP o el nombre de las máquinas, sustituyéndolas por relaciones basadas en claves criptográficas; el cifrado y el filtrado de las conexiones que pueden aceptar nuestras máquinas también son unas medidas de seguridad importantes de cara a evitar el spoofing[4].

Denegación de servicio
El objetivo es mantener un servicio activo para que los usuarios legítimos puedan acceder a él. Los ataques se centran en destruir la disponibilidad de un servicio. Su objetivo es interrumpir las operaciones de un servicio dejándolo desconectado.
Es necesario adaptar la configuración del servidor a las necesidades de autenticación, seguir recomendaciones con respecto al tamaño de mensajes aceptados, controlar la distribución de mensajes para minimizar este tipo de ataques[11].

6.ESTÁNDARES SOBRE LA SEGURIDAD EN SERVICIOS WEB

El esquema del que parte la estructura de los servicios Web, tiene unas características propias de acceso a la información, sobre el intercambio de la misma, sobre la autonomía de la información que difieren de lo establecido en los modelos de seguridad tradicionales. De hecho, esto provoca la necesidad y el desafío de modificar mecanismos que afectan a la integridad y confidencialidad de la información que es enviada por el canal del servicio Web. Si analizamos la estructura de los sistemas de seguridad perimetrales (cortafuegos, sistemas anti-intrusos) no están preparados para asegurar arquitecturas SOA. Estas arquitecturas son eminentemente dinámicas y son transmitidas a través de protocolos no asegurados como HTTP. Si aplicamos criterios que controlan la comunicación punto a punto (TLS, SSL), no son válidos para porque no aseguran la aplicación completa.

El procesamiento de SOA se basa en comunicaciones basadas en mensajes SOAP y documentos XML. Es necesario asegurar transmisiones a través de una infraestructura de conectividad. Los estándares que se están desarrollando por W3C y otros organismos, basados en XML, tratan de asegurar la confidencialidad, integridad y disponibilidad de los Servicios Web. Estas especificaciones dotan de mecanismos para cifrar, firmar digitalmente, autenticar y certificar documentos XML. A continuación vamos a ofrecer una breve descripción de los más significativos[16,17]:

6.1 XML Digital Signature

Establecido por W3C, tiene como objetivo crear una serie de mecanismos que permitan la creación y manejo de firmas digitales basadas en el lenguaje XML. XML Signature, es el estándar de firmado desarrollado para establecer un esquema que permite interpretar el resultado obtenido de las firmas digitales y aplicarlas sobre los datos. Dentro del esquema se contempla la integridad de los datos, el no repudio de las transacciones y criterios de autenticación sobre la transmisión

XML Signature permite firmar parcialmente el código XML y no obliga a que la firma se aplique a la totalidad de un documento, además permite firmar diferentes tipos de recursos dentro de estos fragmentos de código, como datos XHTML, datos en formatos binarios y datos en formatos en XML nativo. La validación de la firma requiere que el objeto que fue firmado sea accesible. La firma XML indica la localización del objeto original firmado, estas localizaciones pueden ser referenciadas por una URI[4] con la firma XML[10].

XML Encryption

Presenta un framework para cifrar documentos XML. En el siguiente ejemplo se muestra cómo usar este estándar con llaves simétricas. Un ejemplo de código sin firmar sería:

```
<?Xml version='1.0'?>
<Metodopago xmlns='http://madeja/ejemplo”>
 <Nombre>Desarrollador</Nombre>
  <CreditCard Limite='10000' Moneda='EU'>
   <Numero>222 111 333 444</Numero>
   <Issuer>BanJuntaAndalucia</Issuer>
  <Caducidad>10/10</Caducidad>
 </CreditCard>
</Metodopago>
```

XML Key Management

Está orientado a la obtención de información acerca de claves y certificados. Permite manejar los procesos de registro y revocación del servicio. Mediante el uso de este protocolo se puede intercambiar y registrar claves públicas. Está compuesto de dos elementos importantes: la información (X-KISS) y el registro (X-RKSS) de la clave pública. Se definen los dos estándares como:

- XML Key Information Service Specification (X-KISS). Tiene como objetivo crear protocolos para el procesamiento de la información asociada a las claves de una firma XML y el contenido de las claves, ya sean públicas o privadas, de los datos.

- XML Key Registration Service Specification (X-KRSS). Esta especificación está dirigida a registrar un conjunto de claves que permiten realizar gestiones sobre la arquitectura pública y privada. Su objetivo primordial, es ofrecer una gestión global de los procesos de intercambio de claves.

6.4 OASIS Security Service TC-SAML (Security Authorization Markup Language)

SAML es un derivado de XML que está diseñado para el intercambio de autenticación y autorización de datos. Este framework facilita infraestructuras de llave pública, que permiten realizar intercambios de autenticaciones y autorizaciones. Tiene como objetivo principal crear un conjunto de procesos que permitan realizar, de forma segura, un canje de los datos relacionados con la identidad y privilegios de los usuarios. 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, Autoridad de Atributos y Puntos de Decisión de Políticas[15].

6.5 XML Advanced Electronic Signatures (XAdES)

Es un estándar del W3C y propuesto por el ETSI europeo.

XADES define un estándar de firma de documentos basado en XML con[14]:

- Soporte a múltiples CA's.
- Soporte a múltiples documentos.
- Soporte a documentos complejos.
- Soporte a múltiples formatos de documentos.
- Soporte a múltiples firmas en tiempos distintos.

6.6 Platform for Privacy Preferences (P3P)

Es una especificación propuesta por el consorcio de W3C con el objetivo claro de indicar la política de privacidad de los participantes de manera estandarizada. En esta especificación se ha definido una forma de interpretar la información referente a la privacidad. En el sí incluye una recomendación para la creación de un conjunto de ficheros destinados al manejo de políticas[10,12].

Ventajas de P3P

P3P sirve para desarrollar herramientas y servicios que ofrezcan a los usuarios un mayor control sobre la información personal que se maneja en Internet y, al mismo tiempo, aumentar la confianza entre los servicios Web y los usuarios.

P3P mejora el control del usuario al colocar políticas de privacidad donde los usuarios pueden encontrarlas, en un formato en el que los usuarios pueden entender y, lo más importante, con la posibilidad de que el usuario actúe sobre lo que ven.

En conclusión, P3P proporciona a los usuarios Web facilidad y regularidad a la hora de decidir si quieren o no, y bajo qué circunstancia, revelar información personal.

Como funciona P3P

P3P[5] permite a los sitios Web trasladar sus prácticas de privacidad a un formato estandarizado y procesable por dispositivos (basado en XML) que puede ser recuperado de forma automática y que además puede ser interpretado fácilmente por los navegadores de los usuarios.

Una vez completada una simple configuración del servidor, el sitio Web informará automáticamente a los visitantes de la página que ese sitio Web es compatible con P3P. En el lado del usuario, P3P automáticamente busca y lee las políticas de privacidad del sitio Web. Un navegador equipado para utilizar P3P puede comprobar una política de privacidad de un sitio Web e informar al usuario sobre las prácticas de información de ese sitio. El navegador puede entonces comparar automáticamente la declaración con las preferencias de privacidad del usuario, pautas reguladoras u otra variedad de estándares legales desde todo el mundo[12].

XACML (eXtensible Authorization Markup Language)

Se define XACML como un estándar basado en la especificación XML, que tiene como objetivo principal la definición de un lenguaje que facilite la definición de la autorización. Es decir, un lenguaje que pueda realizar especificaciones y definiciones sobre políticas de acceso. XACML, es el encargado de crear un modelo para el intercambio de información de autorización, así como de almacenar y estructurar el citado almacenamiento de dicha información[13].

Ventajas del uso de XACML

- Un lenguaje unificado puede reemplazar varios lenguajes propietarios, simplificando la administración de políticas y control de acceso.
- No es necesario capacitarse en distintas herramientas o lenguajes.
- Cuando se implementa un nuevo sistema de autorización, los diseñadores no necesitarán pensar desde cero un lenguaje nuevo e implementar herramientas de configuración: pueden reutilizar código existente.
- XACML es lo suficientemente flexible para resolver las necesidades más comunes de información de autorización.
- Los mecanismos de extensibilidad de XACML permiten acomodar nuevas necesidades a medida que sean necesarias, con impacto mínimo en los sistemas ya implementados.
- XACML permite utilizar escenarios centralizados o descentralizados.
- En un escenario centralizado, un conjunto de políticas único se utiliza para referirse al control de acceso sobre distintos tipos de recursos.

7. IMPLANTACIÓN DE SERVICIOS WEB PARA LA INTEOPERABILIDAD EN EL ESTADO PERUANO – ONGEI

Según ONGEI, la interoperabilidad es la capacidad de los sistemas de información y de los procedimientos, para compartir datos y posibilitar el intercambio de información y conocimiento; y en el estado Peruano se maneja dicho término asociado a la Gobernanza de la Interoperabilidad que se refiere a los acuerdos y forma de alcanzarlos entre Gobiernos y actores que participan en los procesos de interoperabilidad, así como a los espacios de diálogo donde se definen dichos acuerdos[19]. La interoperabilidad tiene los siguientes beneficios:

- Cooperación entre instituciones de la administración pública, sin distinción del nivel de desarrollo tecnológico de estas.
- Simplificación de la actividad administrativa y de los procesos de negocio de las instituciones.
- Permite utilizar más fácilmente estándares abiertos y aplicaciones tecnológicas de distinta generación.
- La reutilización de datos y funcionalidades que puede redundar en una disminución de los costos.

- La mejora de la toma de decisiones.
- Mayor facilidad en la realización de trámites por el ciudadano o usuario.
- Mejora de la capacidad de promover la transparencia y la rendición de cuentas.

7.1 Plataforma de inteoperabilidad del Estado –PIDE

Mediante la Resolución Ministerial N° 381-2008-PCM, se establecen los lineamientos, mecanismos y estándares para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado.

La Plataforma de Interoperabilidad del Estado - PIDE, está a disposición de las entidades públicas, integrantes del Sistema Nacional de Informática, que implementen servicios públicos en línea por medios electrónicos y/o el intercambio electrónico de datos, que requieran de la participación de una o más entidades del Estado.

El uso de la Plataforma de Interoperabilidad del Estado PIDE, es gratuito.

Simplificación de la actividad administrativa y de los procesos de negocio de las instituciones.

El acceso a los servicios públicos por medios electrónicos a través de la Plataforma de Interoperabilidad del Estado - PIDE, no demandará costo adicional al administrado o ciudadano.

La Plataforma de Interoperabilidad del Estado Peruano (PIDE), es una infraestructura tecnológica que permite la implementación de servicios públicos en línea, por medios electrónicos y el intercambio electrónico de datos entre entidades del Estado a través de internet, telefonía móvil y otros medios tecnológicos disponibles[20].

7.2 Aspectos tecnológicos de la plataforma de interoperabilidad del estado peruano

La plataforma de interoperabilidad, ha sido implementada utilizando los siguientes componentes tecnológicos:

Software

- Módulo SOA: JBOSS SOA, SOA Software
- Server Web JBOSS
- Base de datos: PostgreSQL, MySQL
- Sistema operativo: Red Hat Enterprise Linux

Hardware

Servidores, balanceadores de carga, firewalls, sistemas de almacenamiento SAN[6], librerías robot, entre otros. La Arquitectura de la PIDE funciona en alta disponibilidad, 24 x 7 x 365.

Periodo de ejecución

Aproximadamente S/12´500,000.00.

Es un Proyecto de Inversión Pública, con Código SNIP[7], 46272, APROBADO: ABRIL 2007, CIERRE: FEBRERO 2013. Actualmente en producción y administrado por la Presidencia del Consejo de Ministros – PCM a través de la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI[19].

7.3Normatividad

- Resolución Ministerial Nº. 381-2008-PCM - Aprueban lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado
- Decreto Supremo N° 081-2013-PCM - Se aprueba la Política Nacional de Gobierno Electrónico 2013 - 2017
- Decreto Supremo No. 083-2011-PCM - Crean la Plataforma de Interoperabilidad del Estado - PIDE.
- Decreto Supremo No. 133-2013-PCM - Se establece el acceso e intercambio de información espacial entre entidades de la Administración Pública[19].

7.4 Caso de implantación de servicios web - Gobierno Regional de la Libertad

En el Gobierno Regional de la Libertad es un organismo público descentralizado que, en forma concertada, promueve el desarrollo Integral y sostenible de la región. Como organización, mantenemos una cultura ética, basada en el fomento y la práctica de los valores de honestidad, equidad, transparencia y Solidaridad. Utilizamos los recursos y las competencias asignadas con eficiencia y eficacia. A través de la Subgerencia de tecnologías de la Información se realizó las siguientes actividades:

- La Subgerencia de Tecnologías de la Información (SGTI) del Gobierno Regional de la Libertad identificó la necesidad de implementar los servicios web de "Consulta de DNI" y "Consulta RUC".
- La SGTI envía un oficio al Director de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), solicitando el acceso y anexando los formatos de solicitud debidamente completados (una solicitud por cada servicio web).
- Los formatos son de Solicitud de Consumo de Servicio de la PIDE – Para cualquier solicitud de servicio excepto mensajería de texto SMS.
- LA SGTI completa los datos señalados en el formato de solicitud.
- ONGEI recibe y valida las solicitudes, luego nos envía a SGTI un documento guía de implementación (contrato) para cada servicio web solicitado, conteniendo las indicaciones técnicas para su puesta en operación. (Confidencial).
- Se facilita una IP pública del Gobierno Regional a ONGEI para que nos habiliten el uso de los servicios web
- Se realiza el testeo de los web services con un software SoapUI (recomendado por ONGEI) que permite crear y ejecutar pruebas funcionales, de regresión, de cumplimiento y de carga automatizadas con facilidad y rapidez[21].
- Se desarrolla una solución web que consume los servicios web del DNI y RUC.

- Se publica (implementa) la solución web que consume los Web services.

Figura 3. Logo SOAPUI
Fuente: http://www.soapui.org/

Figura4.Consulta de Personas por DNI
Fuente:http://www.regionlalibertad.gob.pe/grllservicios/dni/

8. CONCLUSIONES

Los resultados obtenidos indican que existe el marco teórico básico sobre la seguridad de los servicios web que respaldan la forma de implementación en las instituciones.
Cabe señalar que se determinó las instituciones que regulan la normatividad de seguridad y control de los servicios web en Perú, como es ONGEI, la cual ofrece un sin número de servicios web integrados en su plataforma de Interoperabilidad del Estado PIDE.

Además se conoció las amenazas y los estándares de seguridad sobre los servicios web, rescatando que tenemos WS security que mejora el servicio de mensajes vía SOAP.
Los servicios web, no son del todo confiables, aunque exista métodos de encriptación, existe maneras de evadir eso y poder acceder a la información que se quiere llegar; sin embargo los beneficios de la implementación en el caso del Gobierno Regional de la Libertad se pueden mencionar:

- Cooperación entre instituciones de la administración pública.
- Simplificación de la actividad administrativa (consulta de información validada por RENIEC.)
- Permite utilizar más fácilmente estándares abiertos y aplicaciones tecnológicas de distinta generación.

9. AGRADECIMIENTO

El autor agradece a la Universidad César Vallejo y al Gobierno Regional de la Libertad por el apoyo con la información necesaria para la realización de este trabajo de investigación.

10. BIBLIOGRAFÍA

[1] https://books.google.com.pe/books?id=JBIMAAAACAAJ&dq=servicios+web&hl=es&sa=X&ved=0CD4Q6AEwBmoVChMIl6CNmt33xgIVQZANCh2XvQBy

[2] http://www.ibm.com/developerworks/ssa/webservices/newto/service.html

[3] http://es.slideshare.net/jselman/seguridad-para-servicios-web-presentation

[4] http://www.ibm.com/developerworks/ssa/library/ws-best11/

[5] http://www.safenet-inc.es/data-protection/web-services-security/

[6] https://books.google.com.pe/books?id=ibSu6896I_YC&pg=PA343&dq=seguridad+de+la+informacion+en+los+servicios+web&hl=es&sa=X&ved=0CBsQ6AEwAGoVChMIktaTp9H3xgIVjJENCh00EAJ#v=onepage&q&f=false

[7] http://desarrollosoa.blogspot.com/2013/05/la-seguridad-en-los-servicios-web_21.html

[8] http://www.slideshare.net/luas0_1/seguridad-en-servicios-web-net

[9] https://books.google.com.pe/books?id=xKkYBgAAQBAJ&pg=PA112&dq=seguridad+de+la+informacion+en+los+servicios+web&hl=es&sa=X&ved=0CCEQ6AEwAWoVChMIqtLmgt33xgIVi9WACh1eXQVp#v=onepage&q=seguridad%20de%20la%20informacion%20en%20los%20servicios%20web&f=false

[10] W3C World Wide Web Consortium, "Services Web"

[11] http://www.w3c.es/Divulgacion/GuiasBreves/ServiciosWeb

[12] http://www.w3.org/P3P/

[13] http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html#_Toc 325047090

[14] http://www.mundolinux.info/que-es-xml.htm

[15] https://books.google.com.pe/books?id=DemCZwEACAAJ&dq=Security+Authorization+Markup+Language&hl=es419&sa=X&ved=0CBsQ6AEwAGoVChMIy5vyhquDxwIVyryACh2_1QtM

[16] https://msdn.microsoft.com/eses/library/vstudio/ba0z6a33(v=vs.100).aspx

[17] http://desarrolloweb.dlsi.ua.es/cursos/2012/nuevos-estandares-desarrollo-sitios-web/desarrollo-web-actual

[18] http://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/

[19] http://www.ongei.gob.pe/

[20] http://www.ongei.gob.pe/interoperabilidad/

[21] http://www.regionlalibertad.gob.pe/

[22] http://www.soapui.org/