Revista Industrial Data 21(1): 123-132 (2018)
DOI: http://dx.doi.org/10.15381/idata.v21i1.14927

ISSN: 1560-9146 (Impreso) / ISSN: 1810-9993 (Electrónico)
Facultad de Ingeniería Industrial - UNMSM

Modelo de evaluación de seguridad para transmitir datos usando Web Services

EDGAR GÓMEZ ENCISO [1]
EFRAÍN E. PORRAS FLORES [2]

RECIBIDO: 4/10/2017 ACEPTADO: 04/06/2018

RESUMEN

Los Web Services actuales ofrecen una variedad de soluciones de software basadas en estándares para integrar aplicaciones y automatizar procesos de transferencia de información confidencial. Por lo tanto, la seguridad del Web Service se considera una característica muy importante para una entidad que tiene como objetivo ofrecer un mejor servicio al usuario, proporcionando una infraestructura completa que permite el intercambio de información de forma segura.

El modelo de evaluación propuesto responde a la necesidad de disponer de una herramienta válida y confiable para estimar la seguridad del Web Service durante la transferencia de datos; detallándose de manera específica los procedimientos necesarios para realizar una evaluación, usando criterios de evaluación que no han sido considerados por otros investigadores. Los resultados sirven para identificar con claridad las vulnerabilidades de seguridad que existen en los Web Services.

Palabras-claves: Evaluación; seguridad; métrica; servicio web.

SECURITY EVALUATION MODEL TO TRANSMIT DATA USING WEB SERVICES

ABSTRACT

The current Web Services offer a variety of software solutions based on standards to integrate applications, automatize processes and transfer confidential information. Therefore, the security of Web Service is considered a very important characteristic for an entity that aims at offering a better service to the user, providing a complete infrastructure that allows the exchange of information reliably.

The proposed evaluation model responds to the need to have a valid and reliable tool to estimate the security during the transfer of data; specifying in detail the procedures necessary to carry out an evaluation, using evaluation criteria that have not been considered by other researchers. The results serve to clearly identify the security vulnerabilities that exist in Web Services.

Keywords: Assessment; security; metric; web service.

1. INTRODUCCIÓN

La falta de implementación de las medidas de seguridad en los Web Services y el incremento de ataques cada vez más especializados y organizados, hace importante y fundamental un método para evaluar la seguridad de los Web Services durante transmisión de datos, que existen actualmente en las empresas e instituciones del sector gobierno (Luna, Garcia, y Romero, 2009). El incremento de los riesgos a la seguridad y las vulnerabilidades de seguridad, hacen necesaria la tarea de protección y vigilancia de los datos de una empresa.

La investigación propone un método para evaluar el grado de seguridad del Web Service, usando las cinco fases y los 17 procesos del modelo de evaluación propuesto, obtenidos a partir de los estudios revisados en la tabla 1. Las métricas utilizadas para realizar la medición de las cinco características de seguridad estudiadas en esta investigación, detallan de manera específica los procedimientos para realizar una medición precisa, los cuales son consideradas importantes, al tener en cuenta los aspectos mínimos de seguridad que requiere un Web Service (WS).

Para verificar la aplicabilidad del modelo de evaluación, se ha aplicado a un caso de estudio práctico; para medir la validez y consistencia interna del método, se ha utilizado una herramienta para hacer encuestas y evaluado por juicios expertos. Los resultados confirman que el mismo es adecuado, completo y preciso.

2. ANTECEDENTES

2.1 Protocolos del Web Service

La familia de protocolos del Web Service, es una colección de estándares que son utilizados para implementar y hacer que un Web Service interactúe con otro sistema. Los protocolos más estudiados son el XML Encryption, el XML Digital Signature y el WS-Security (Saravanaguru y Krishnakumar, 2013). En los últimos años se ha dado mayor impulso al estudio de las especificaciones de la familia de WS-Security.

1 Ingeniero Informático – UNSCH, Responsable TIC Centro de Atención al Ciudadano, PCM, e-mail: egomez@pcm.gob.pe.
2 MSc. Ingeniería de Sistemas – Universidad Nacional de Ingeniería, Docente Principal UNSCH, e-mail: efrain.porras@unsch.edu.pe.

2.2 Arquitectura de seguridad del Web Service

Según el Instituto Nacional de Estándares y Tecnología (NIST), el Web Service es una arquitectura por capas que consiste en: (1) la capa de Web Services, (2) la capa del framework del Web Service y (3) la Capa Web Server. Según Mokbel y Jiajin (2008), el objetivo de diseñar la arquitectura de seguridad es resumir los detalles de seguridad a nivel del mensaje de la lógica de negocios.

La ISO-WSP (Web Services Platforms) es una arquitectura de flujo de información que descompone la WSP en dos partes y que se ejecuta en dominios de protección diferentes: (1) el T-WSP: maneja la seguridad de datos confidenciales y (2) el U-WSP: que contiene amplio código que proporciona la normal funcionalidad del WS (Singaravelu, Wei y Pu, 2008).

2.3 Estándares de seguridad del Web Service

La seguridad del WS es un campo que ha tenido una prolífica actividad investigadora, son escasas las aportaciones que se han hecho sobre la seguridad de un software. Entre los estándares estudiados tenemos:

a. ISO/IEC 25040:2011
b. NTP ISO/IEC 27001:2014
c. NIST 800-95. Guide to Segure Web Services

2.4 Estudios sobre el modelo evaluación propuesto

Para el desarrollo del modelo de evaluación propuesto, se ha realizado una revisión a los diferentes estudios referentes a los tipos de seguridad de información del WS. Se han seleccionado los estudios luego se ha clasificado en cada fase por el tipo de estudio realizado en el modelo de evaluación propuesto (tabla 1).

3. PRESENTACIÓN DEL MODELO DE EVALUACIÓN DEL WEB SERVICE PROPUESTO

Las 5 fases del modelo de evaluación propuesto que se muestran en la Figura 1, se ha obtenido a partir de los estudios de las normas: ISO/IEC 25040:2011 y NTP ISO/IEC 14598-2:2004; que sirven como base para el desarrollo de los 17 procesos del modelo de avaluación propuesto, obtenidos a partir de los estudios revisados en la tabla 1.

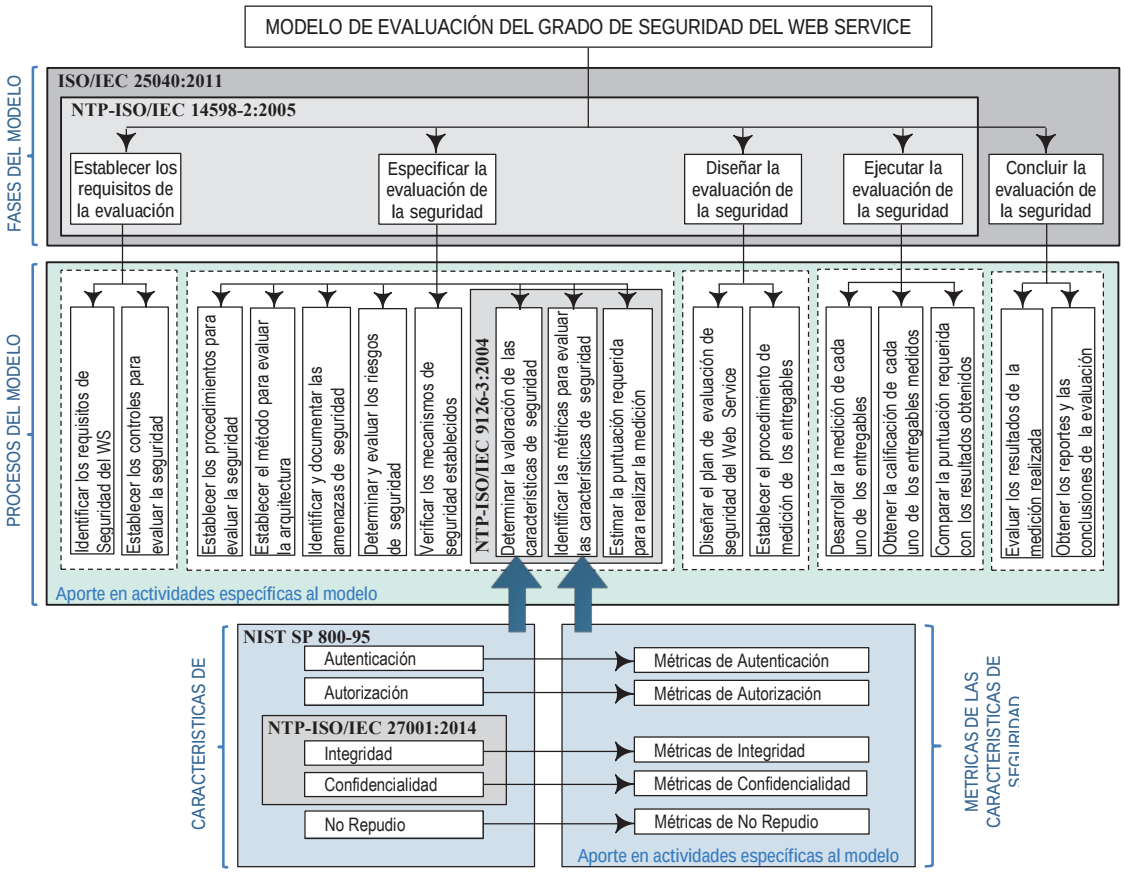

Figura 1. Modelo de evaluación propuesto para medir el grado de seguridad del Web Service

Fuente: Elaboración propia

Tabla 1. *Resúmen de las investigaciones estudiadas para el desarrollo del modelo de evaluación propuesto*

Título de Investigación	Descripción de la Investigación
A Performance Evaluation of Security Mechanisms for Web services	Revisión y evaluación de las pruebas de performance de varios mecanismos de seguridad aplicados a los mensajes de Web Services, obteniéndose diferentes resultados (Alrouh y Ghinea, 2009).
Estimating Web Service interface quality through conventional object oriented metrics	Presenta un conjunto de métricas para estimar la calidad de los artefactos de la interfaz del Web Service (WSDL), presenta un análisis estadístico correlacional con los atributos más relevantes de la calidad (Ordiales, Crasso y Mateos, 2013).
Using Web Security Scanners to Detect Vulnerabilities in Web Services.	Realiza una evaluación experimental de las vulnerabilidades de seguridad de los Web Services, los resultados muestran las diferentes vulnerabilidades de seguridad (Vieira, Antunes y Madeira, 2009).
Measuring Security of Web Services in Requirement Engineering Phase.	Realiza un estudio para evaluar la seguridad del Web Service a partir de las métricas y los requisitos de seguridad a través de un proceso de gestión de riesgos de seguridad del Web Service (Mougouei, Wan y Moein, 2012).
A Survey of Patterns for Web Services Security and Reliability Standards.	Luego de realizar un estudio presenta las inconsistencias que existen entre los patrones y estándares de seguridad del Web Service para el control de acceso a los servicios (Fernandez, Ajaj, Buckley y Delessy, 2012).
Web Services Security Assessment: An Authentication-focused Approach	Desarrolla un estudio sobre las amenazas y ataques a la autenticación de usuarios del Web Service. Realiza una evaluación al mecanismo de autenticación de los Web Services (Soupionis y Kandias, 2012).

Fuente: Elaboración propia.

4. PROCESOS PARA EVALUAR EL GRADO LA SEGURIDAD DEL WEB SERVICE

Los procesos del modelo de evaluación propuesto en la tabla 2, se han desarrollado a partir de los estudios revisados de la tabla 1. La clasificación de los estudios ha servido para identificar mejor los controles de seguridad y describir cada uno de los procesos de las 5 fases del modelo de evaluación.

4.2 Establecer los requisitos de la evaluación

Para realizar el análisis de requisitos se establecen los controles de seguridad a partir de las necesidades del usuario, los documentos elaborados de casos de prueba y los estándares de seguridad, para obtener una definición clara de lo que se quiere evaluar. Los procesos de evauación para esta fase son:

a. Identificar los requisitos de seguridad del WS
Para realizar un análisis detallado de los requisitos de seguridad del WS, se identifica y se documenta los requisitos funcionales y no funcionales, luego se evalúa según el tipo de seguridad que interviene durante la transmisión de datos.

Tabla 2. *Procesos del modelo de evaluación propuesto para medir el grado de seguridad de un Web Service*

Fases	Procesos
1. Establecer los requisitos de la evaluación	1.1 Identificar los requisitos de seguridad del Web Service
	1.2 Establecer los controles para evaluar la seguridad
2. Especificar la evaluación de la seguridad	2.1 Establecer los procedimientos para evaluar la seguridad
	2.2 Establecer el método para evaluar la arquitectura
	2.3 Identificar y documentar las amenazas de seguridad
	2.4 Determinar y evaluar los riesgos de seguridad
	2.5 Verificar los mecanismos de seguridad establecidos
	2.6 Determinar la valoración de las característica de seguridad
	2.7 Identificar métricas para evaluar las característica de seguridad
	2.8 Estimar la puntuación requerida para la medición
3. Diseñar la evaluación de la seguridad	3.1 Diseñar el plan de evaluación de seguridad del Web Service
	3.2 Establecer el procedimiento de medición de los entregables
4. Ejecutar la evaluación de la seguridad	4.1 Desarrollar la medición de cada uno de los entregables
	4.2 Obtener la calificación de cada uno de los entregables medidos
	4.3 Comparar la puntuación requerida con los resultados obtenidos
5. Concluir la evaluación de la seguridad	5.1 Evaluar los resultados de la medición realizada
	5.2 Obtener los reportes y las conclusiones de la evaluación

Fuente: Elaboración propia.

b. Establecer los controles para evaluar la seguridad
El modelo de evaluación propuesto presenta una lista de controles de seguridad que se ha establecido a partir de los requisitos de seguridad del Web Service. La tabla 3 muestra cada uno de los controles para garantizar el cumplimiento de los requisitos de seguridad.

4.2 Especificar la evaluación de la seguridad

Consiste en realizar un análisis minucioso a las especificaciones de seguridad del WS, las métricas utilizadas para la medición y los artefactos obtenidos al efectuar la evaluación de cada uno de los entregables. Los procesos propuestos para esta fase son:

a. Establecer los procedimientos para evaluar la seguridad
Consiste en identificar y desarrollar los procesos para realizar una evaluación del Web Service de manera correcta.

b. Establecer el método para evaluar la arquitectura
Evaluar los controles de seguridad de la arquitectura del Web Service empieza el día en que se modelan los requisitos del negocio y no termina hasta que la última copia de aplicación es retirada del servicio.

c. Identificar y documentar las amenazas de seguridad
Durante el diseño de la evaluación es importante identificar y documentar las amenazas de seguridad más comunes, para luego evaluar los controles de seguridad a fin de reducir el impacto que puede ocacionar una amenaza.

d. Determinar y evaluar los riesgos de seguridad
Se identifican los riesgos de seguridad para capturar las evidencias y neutralizar los posibles ataques a la seguridad que se presenten, con esto se busca que el impacto sea mínimo cuando ocurra un incidente. En la columna 2 de la tabla 4 se muestran los riesgos de seguridad identificados para cada catarterística.

e. Verificar los mecanismos de seguridad establecidos
Los WS poseen mecanismos de seguridad que deben ser evaluados, con el objeto de mitigar los riesgos de seguridad y reducir al mínimo el impacto presentado. La columna 3 de la tabla 4, muestran los mecanismos de seguridad para cada característica de seguridad.

f. Determinar la valoración de las característica de seguridad
La valoración de cada característica de seguridad, se realiza a partir de los artefactos obtenidos durante el análisis de requisitos. Una técnica de evaluación es asignando valores porcentuales a las características de seguridad que se han establecido para su evaluación.

g. Identificar las métricas para evaluar las características de seguridad
Identificar y seleccionar las métricas para realizar las mediciones de seguridad, los resulta-

Tabla 3. *Lista de controles para evaluar el cumplimiento de los requisitos de seguridad*

Características	Controles	Objetivos
Autenticidad	Los protocolos de transporte requieren nuevos métodos para la identificación de los clientes.	Garantizar que las transacciones se realicen sólo por las partes de confianza (envío y recepción)
Autorización	Las transacciones son invisibles para los mecanismos de filtrado y de control de acceso	Asegurar que sólo se realicen transacciones autorizadas en el sistema
Integridad	La información posee mínimas posibilidades de tener vulnerabilidades de integridad de datos	Garantizar que las transacciones no sean manipuladas
Confidencialidad	Las interfaces autodescriptivos posibilitan que no todos pueda ver las transacciones en texto (anónimo y privado)	Asegurar la privacidad de las transacciones (cumplimiento sobre los datos confidencia-les de los usuarios)
No Repudio	Las transacciones requieren métodos detallados que aseguren resultados correctos de extremo a extremo	Asegurar que habrá controles apropiados para garantizar los resultados de una transacción realizada

Fuente: Elaboración propia.

Tabla 4. *Riesgos y mecanismos de seguridad identificados*

Características	Riesgos de Seguridad	Mecanismos de seguridad
Autenticación	Acceso no autorizado al Web Service	Proporcionar la auten-ticación e identificación del usuario
Autorización	Permitir acciones del usuario no acorde con sus privilegios	Proporcionar el control de acceso y el flujo de información
Integridad	Modificación de datos no autorizados	Garantizar la integridad de datos
Confidencialidad	Acceso a información confidencial	Garantizar el cifrado de los datos confidenciales
No repudio	Negación de una acción realizada	Garantizar el no repu_ dio de la firma digital

Fuente: Elaboración propia.

dos determinan si es necesario implementar más controles seguridad en el WS o si algún mecanismo de seguridad en particular no es comprendido con claridad durante el desarrollo. Las métricas se muestran en la columna 2 de la tabla 5.

h. Estimar la puntuación requerida para realizar la medición

Luego de identificar las métricas de cada característica de seguridad (tabla 5), se realiza la estimación porcentual a los entregables en función de cada métrica, esta evaluación sirve para

Tabla 5. *Lista de métricas y su método de aplicación para evaluar los entregables*

Car.	Métricas	Entregables a evaluarse
Autenticación	Autenticación de credenciales del usuario de punto a punto	Reporte de pruebas de validación de las credenciales de los usuarios. Reporte de especificaciones de accesos al WS y autorizaciones a los usuarios.
	Verifica-ción de autenticidad del usua-rio en la capa de transporte	Verificar que los controles de auten-ticación del usuario se haya realizado con WS-Security o con SSL Especificaciones de las pruebas de autenticación de usuarios punto-punto
	Verificación de autenticidad del origen de datos del usuario	Casos de prueba de implementación para autenticar los datos del usuario. Reporte de pruebas de autenticación de usuarios en la capa de transporte (SSL/TLS).
	Utilización de Tokens para la autenticación del usuario	Casos de prueba de los tokens rea-lizados de autenticación de usuarios Reporte de operaciones ilegales no permitidas por los tokens del WS.
	Capacidad de detectar operación ilegal de acceso	Casos de prueba de la validación de controles de acceso con pool de dato Reporte de pruebas con operaciones ilegales detectadas por los controles.
Autorización	Responsabilidad de acceso al Web Service	Detalles de los accesos autorizados. Reporte de documentos de autoriza-ción de accesos. Documento de responsabilidad de los accesos al WS.
	Capacidad de administrar el control de acceso	Especificaciones de los accesos autorizados por el usuario respons. Reporte de documentos que autorizan de accesos al WS
	Conformidad de registro de revi-siones de control de acces	Documento de especificaciones de los accesos de los usuarios. Reporte de pruebas a las validacio-nes de acceso al WS.
	Capacidad de detectar autori-zaciones ilegales de control de acceso	Especificaciones de casos de prueba del control de acceso. Reporte de pruebas de acceso realizadas con pool de operaciones. Reporte de operación ilegales de acceso al WS detectadas.
Integridad	Verificación de cobertura de envío de datos	Casos de prueba de envío de mensajes realizados . Reporte de pruebas de envío de mensajes realizados a los usuarios.
	Conformidad de integridad del cifrado de mensajes	Reporte de pruebas de autenticación de mensajes implementados con WS-SSL. Reporte de pruebas del correcto cifrado de mensajes punto a punto.
	Integridad de mensajes con firmas digitales	Reporte de pruebas de autenticación de mensajes implementados con WS-Security. Reporte pruebas deverificación de integridad del mensaje punto a punto
Confidencialid	Confidencialidad del men saje en la capa de transporte	Casos de prueba del establecimiento de sesiones SSL/TLS. Reporte de pruebas del estableci-miento de sesiones SSL/TLS.
	Utilización de Tokens para la con-fidencialidad de mensajes	Reporte de pruebas de envío de mensajes con tokens WS-Security y WS-Trust. Reporte de pruebas de tokens de seguridad de confidencialidad de los mensajes con X.509.
	Utilización de certificado X.509 para encriptar y desencriptar mensajes	Casos de prueba y los resultados de los certificados implementados para los mensajes. Reporte de pruebas de mensajes encriptados y desencriptados por el certificado X.509.
	Validación de envío de mensajes en la estructura y contenido del XML	Casos de pruebas de validación de datos implementados para los men-sajes. Reporte de pruebas de validación de mensajes definidos e implementados.
No Repudio	Verificación del no repudio del emisor	Reporte pruebas de conformidad de acuse de recibo del archivo recibido Reporte de pruebas al historial de archivos enviados.
	Verificación del no repudio del receptor	Reporte de pruebas al acuse de recibo de archivos enviados. Reporte de pruebas al historial de archivos recibidos.

Fuente: Elaboración propia.

comparar el nivel de seguridad mínimo obtenido durante la transmición de datos en función de lo estimado. La puntuación asignada para la evaluación es de 0% a 100%.

4.3 Diseñar la evaluación de la seguridad

Desarrollar un buen diseño de evaluación ayuda a medir el cumplimiento de la seguridad del WS, identificar las necesidades de cada entidad y los requisitos mínimos que debe tener el producto. Se debe mostrar todo el monitoreo y las pruebas de evaluación que se realizan sobre el flujo de información para determinar la seguridad de accesibilidad a la información del Web Service.

a. Diseñar el plan de evaluación de seguridad del Web Service
El incluir un plan de evaluación en la programación, demuestra que la organización toma en serio los objetivos programados y que ha establecido un sistema para medir y entender el progreso de sus objetivos. El plan de evaluación debe expresar claramente los principales ejes que se propone desarrollar.

b. Establecer el procedimiento de medición de los entregables
Se ha establecido el procedimiento de medición de cada entregable, en función del cumplimiento de las necesidades de seguridad requeridas. La medición se realiza con la valoración de la métrica correspondiente.

4.4 Ejecutar la evaluación de la seguridad

El procedimiento utilizado para evaluar la seguridad del Web Service, indica la calidad del producto obtenido. Para una mejor apreciación de las etapas del proceso de evaluación, se ha desarrollado un caso práctico para evaluar la Seguridad del Web Service, como se detalla a continuación.

a. Desarrollar la medición de cada uno de los entregables
La medición de cada uno de los entregables, se realiza utilizando las métricas identificadas en la tabla 5. Para que una evaluación sea satisfactoria, el resultado obtenido debe ser superior al peso estimado requerido inicialmente. La diferencia de pesos da lugar a la calificación de cada métrica de seguridad, tal como se observa en la tabla 6.

b. Obtener la calificación de cada uno de los entregables medidos

La Figura 2 muestra la comparación de los pesos luego de realizar la evaluación de los entregables, la figura muestra que algunos de los entregables evaluados no cumplen con el peso requerido para obtener una calificación aceptable, 3 de los resultados de las 18 métricas utilizadas en la evaluación dan un valor negativo, mostrando que existen riesgos de seguridad que aún faltan implementarse en el Web Service.

Tabla 6. *Puntuación y calificación de la evaluación realizada a un Web Service*

Característica	Métrica	Peso requerido	Peso obtenido	Diferencia	Calificación
Autenticación		98.00%	98.50%	0.50%	Aceptable
		97.00%	97.65%	0.65%	Aceptable
		98.00%	98.75%	0.75%	Aceptable
		97.00%	98.30%	1.30%	Aceptable
		98.00%	98.70%	0.70%	Aceptable
Autorización		98.00%	97.20%	-0.80%	No Aceptable
		97.00%	97.50%	0.50%	Aceptable
		98.00%	98.90%	0.90%	Aceptable
		99.00%	99.10%	0.10%	Aceptable
Integridad		98.00%	98.80%	0.80%	Aceptable
		99.00%	98.55%	-0.45%	No Aceptable
		98.00%	99.55%	1.55%	Aceptable
Confidencialidad		99.00%	99.60%	0.60%	Aceptable
		99.00%	98.80%	-0.20%	No Aceptable
		97.00%	97.20%	0.20%	Aceptable
		97.00%	98.40%	1.40%	Aceptable
No repudio		96.00%	97.80%	1.80%	Aceptable
		97.50%	98.10%	0.60%	Aceptable

Fuente: Elaboración propia.

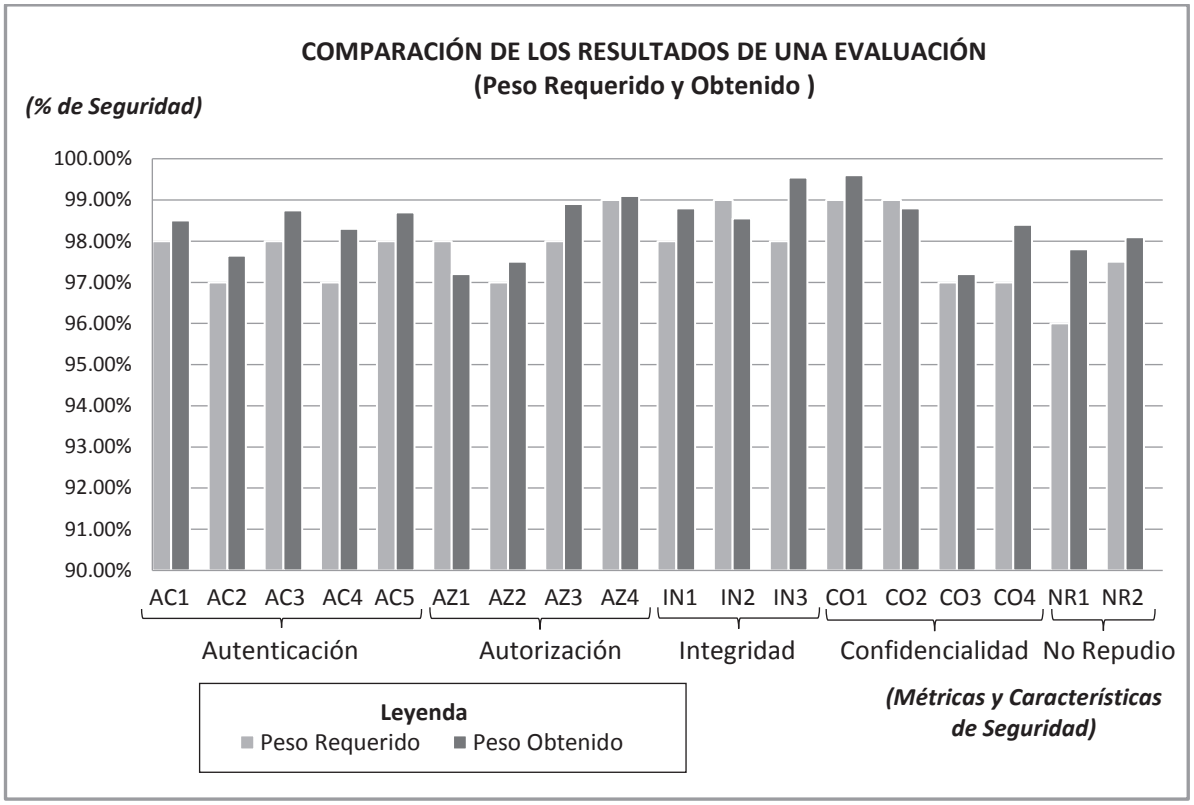

Figura2. Comparación de los resultados de una evaluación
Fuente: Elaboración propia.

c. Comparar la puntuación requerida con los resultados obtenidos

El criterio que se ha utilizado para evaluar los resultados de una evaluación es comparar los resultados de las características de seguridad del WS. Para que una calificación sea satisfactoria, el peso obtenido de cada característica debe ser superior al peso estimado inicialmente, ver la tabla 7.

Tabla 7. *Comparación de las características de seguridad*

Característica	Peso estimado	Peso obtenido	Nivel obtenido	Resultado
Autenticación	97.60%	98.38%	Múltiple	Cumple
Autorización	98.00%	98.18%	Alto	Cumple
Integridad	98.33%	98.97%	Integral	Cumple
Confidencialidad	98.00%	98.50%	Absoluto	Cumple
No repudio	96.75%	97.95%	Completo	Cumple

Fuente: Elaboración propia.

4.5 Concluir la evaluación de la seguridad

Las conclusiones son el resultado final de un proceso de evaluación, aquí se detallan todas las observaciones de los resultados obtenidos. Este es el paso final al culminar un proceso de evaluación.

a. Evaluar los resultados de la medición realizada

Los resultados de la evaluación son importantes para tomar decisiones sobre la seguridad del WS y obtener las conclusiones finales.

b. Obtener los reportes y las conclusiones de la evaluación

Consiste en evaluar los reportes estadísticos como resultado de la evaluación realizada, para elaborar el informe con las conclusiones y recomendaciones.

5. RESULTADOS DE APLICAR EL MODELO DE EVALUACIÓN

Los resultados obtenidos sirven para analizar y emitir las conclusiones y recomendaciones de la evaluación, que luego serán implementados. La tabla 7 concluye que los resultados obtenidos son aceptables y cumplen con los requisitos de seguridad mínimos establecidos para la evaluación.

6. VALIDACIÓN DEL MODELO SEGÚN JUICIOS DE EXPERTOS

Para que el modelo de evaluación propuesto tenga validéz, se ha desarrollado un instrumendo, el cual fué consultado a diez (10) jueces expertos, brindando su conclusión satisfactoria para que esta técnica de evaluación de la seguridad propuesto cumpla con los estándares de seguridad requeridos. Las opiniones y sugerencias recogidas de los expertos han servido para mejorar los procesos del modelo evaluación propuesto.

6.1 Medición de Coeficiente de Fiabilidad con Escala Alfa de Cronbach

Para verificar la fiabilidad del instrumento de evaluación, se ha desarrollado un cuestionario (tabla 8) que fue presentado a diez (10) Jueces Expertos, cuyo resultado se muestran en la tabla 9. Para la evaluación del instrumento se ha asignado la siguiente puntuación:

(1). Totalmente en desacuerdo

(2). En desacuerdo

(3). Ni de acuerdo ni en desacuerdo

(4). De acuerdo

(5). Totalmente de acuerdo

La tabla 10 muestra los resultados de la evaluación procesada utilizando la Escala de Alfa de Cronbach, cuyo resultado obtenido es α = 0.802 de coeficiente de fiabilidad del instrumento. El resultado indica que el instrumento utilizado para la recolección de datos tiene un alto grado de confiabilidad y consistencia.

Tabla 8. *Instrumento utilizado para medir la confiabilidad y la validez del modelo*

Definición conceptual del cuestionario	Puntuación				
	(1)	(2)	(3)	(4)	(5)
¿El modelo de evaluación mide los artefactos que se quieren evaluar?				X	
¿El modelo de evaluación abarca todas las variables que se desea evaluar?					X
¿El modelo de evaluación posee facilidad de aprendizaje?					X
¿El encuestado entiende el modelo de evaluación?				X	
¿Todas las métricas de evaluación de seguridad poseen posibles respuestas?				X	
¿El modelo de evaluación considera la mayoría de procesos de una evaluación?				X	
¿Los resultados de la evaluación crean una impresión positiva, que motiva a las personas aplicarlas?					X
¿El instrumento se adecúa al entorno de trabajo?				X	
¿El instrumento de evaluación es eficiente en tiempo y recursos?					X
¿Los resultados confirman los supuestos e ideas iniciales de la investigación?				X	
¿Los resultados obtenidos de la evaluación satisfacen los objetivos de la investigación?			X		
¿Los resultados obtenidos del instrumento de evaluación son interpretativos?				X	

Fuente: Elaboración propia.

Tabla 9. *Resultados de las encuestas realizadas a Jueces Expertos*

		Ítems (Nro. de preguntas)												Σt
		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	
Nro. de entrevistados (Juicios Expertos)	E1	4	5	5	4	4	4	5	4	5	4	3	4	51
	E2	2	2	5	3	3	2	2	3	4	5	3	3	37
	E3	2	4	4	5	3	5	3	4	4	3	4	5	46
	E4	5	3	4	5	5	4	5	5	5	4	5	4	54
	E5	4	3	3	5	4	5	3	5	3	5	5	4	49
	E6	4	5	5	4	5	4	5	3	4	4	5	5	53
	E7	5	4	3	5	4	3	4	4	3	4	4	4	47
	E8	3	5	5	4	5	4	5	4	5	3	5	5	53
	E9	3	3	3	2	3	5	4	2	2	5	3	2	37
	E10	5	5	4	4	5	4	5	5	4	5	4	5	55

Fuente: Elaboración propia.

Tabla 9. *Resultados de la evaluación realizada utilizando Alfa de Cronbach*

Suma (Σt)	37	39	41	41	41	40	41	39	39	42	41	41	**482**
Promedio	3.7	3.9	4.1	4.1	4.1	4	4.1	3.9	3.9	4.2	4.1	4.1	**48.2**
D. estándar	1.10	1.04	0.83	0.94	0.83	0.89	1.04	0.94	0.94	0.75	0.83	0.94	**6.258**

VARP : (Varianza de la población)	**1.21**	**1.09**	**0.69**	**0.89**	**0.69**	**0.8**	**1.09**	**0.89**	**0.89**	**0.56**	**0.69**	**0.89**	**S_T^2:**	**39.16**
											ΣSi²:	**10.38**		

Fuente: Elaboración propia.

6.2 Medición de la Validez del Coeficiente de Fiabilidad

Para medir la Validez del Coeficiente de Fiabilidad, se ha utilizado el procedimiento de la fórmula de Pearson (índice de correlación), para lo cual se ha procesado los resultados obtenidos en la tabla 9. Según la escala de Spearman-Brown (tabla 11), se obtiene la muestra R = 0.759 grado de validez, el resultado es ligeramente superior al mínimo aceptable de 0.6, considerado en el estudio.

Tabla 11. *Resultados de la evaluación utilizando la fórmula de Pearson y Spearman-Brown*

	A	B	AB	A^2	B^2
Σ E1	26	25	650	676	625
Σ E2	19	18	342	361	324
Σ E3	20	26	520	400	676
Σ E4	29	25	725	841	625
Σ E5	22	27	594	484	729
Σ E6	28	25	700	784	625
Σ E7	23	24	552	529	576
Σ E8	28	25	700	784	625
Σ E9	18	19	342	324	361
Σ E10	27	28	756	729	784
	240	**242**	**5881**	**5912**	**5950**

$N = 10$

$n(\Sigma AB) = 58{,}810$

$(\Sigma A)(\Sigma B) = 58{,}080$

$n(\Sigma A^2) = 59{,}120$ $\quad n(\Sigma A^2) - (\Sigma A)^2 = 1520$

$(\Sigma A)^2 = 57{,}600$

$n(\Sigma B^2) = 59{,}500$ $\quad n(\Sigma B^2) - (\Sigma B)^2 = 936$

$(\Sigma B)^2 = 58{,}564$

- Índice de correlación de Pearson (r) = 0.612
- Corrección según Spearman-Brown (R) = 0.759

6.3 Medición de la Satisfacción de los Resultados con Escala de Likert

Para medir la satisfacción de los resultados obtenidos con el instrumento de evaluación (tabla 8), se ha utilizado la escala de Likert. Como resultado del análisis de la evaluación, se ha concluido que:

- El concepto es pertinente
- La redacción es adecuada y apropiada
- Es factible de obtener una opinión

7. CONCLUSIONES

El modelo de evaluación propuesto es una herramienta metódica que en base a criterios y el uso de técnicas de evaluación, mide el grado de seguridad, analiza los procesos y valora los artefactos; con el fin de generar conocimiento útil para la toma de decisiones y el cumplimiento de los objetivos de seguridad de un WS.

Los resultados demuestran que el modelo de evaluación propuesto fue conveniente desarrollarlo porque es completo en cuanto a la especificación, adecuado en el contexto y preciso en el resultado alcanzado.

8. REFERENCIAS BIBLIOGRÁFICAS

[1] Alrouh, B. y Ghinea, G. (2009). A Performance Evaluation of Security Mechanisms for Web services. *2009 Fifth International Conference on Information Assurance and Security*. doi:10.1109/IAS.2009.252

[2] Fernandez, E., Ajaj, O., Buckley, I. y Delessy, N. (2012). A Survey of Patterns for Web Services Security and Reliability Standards. *Future Internet 2012*. doi:10.3390/fi4020430

[3] ISO/IEC-25040:2011. (2011). *Systems and Software Engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation Process*.

[4] Luna, L. F., Garcia, J. R., y Romero, G. (2009). *Modelo Integral de Evaluación del Gobierno Electrónico: Una Propuesta Preliminar*.

[5] Mokbel, M., y Jiajin, L. (2008). Integrated security architecture for web services and this challenging. *Journal of Theoretical and Applied Information Technology*, p. 518-525.

[6] Mougouei, D., Wan, N. W., y Moein, M. (2012). Measuring Security of Web Services in Requirement Engineering Phase. *International Journal of Ciber-Security and Digital Forensis (IJCSDF)*, p. 89-98.

[7] NTP-ISO/IEC-14598-2:2005. (2005). INGENIERIA DE SOFTWARE. Tecnología de la Información - Evaluación del Producto Software. Parte 2: Planificación y Gestión. *Comisión de reglamentos técnicos y comerciales - INDECOPI*.

[8] NTP-ISO/IEC-27001:2014. (2014). TECNOLOGÍA DE LA INFORMACIÓN: Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. *Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI*.

[9] NTP-ISO/IEC-9126-3:2004. (2004). INGENIERÍA DE SOFTWARE. Calidad del Producto. Parte 3: Métricas Internas. *Comisión de reglamentos técnicos y comerciales - INDECOPI*.

[10] Ordiales, J. L., Crasso, M., y Mateos, C. (2013). Estimating Web Service interface quality through conventional object oriented metrics. *CLEI Electronic Journal, 16*.

[11] Saravanaguru, K., y Krishnakumar, V. (2013). Securing Web Services Using XML Signature and XML Encryption. *School of Computer Science and Engineering*.

[12] Singaravelu, L., Wei, J., y Pu, C. (2008). A Secure Information Flow Architecture for Web Services. *SCC '08 Proceedings of the 2008 IEEE International Conference on Services*, p. 182-189.

[13] Singhal, A., Winograd, T., y Scarfone, K. (2007). *NIST 800-95. Guide to Segure Web Services.* EE. UU.: Instituto Nacional de Estándares y Tecnología.

[14] Soupionis, Y., y Kandias, M. (2012). *Web Services Security Assessment, An Authentication focused Approach*.

[15] Vieira, M., Antunes, N., y Madeira, H. (2009). Using Web Security Scanners to Detect Vulnerabilities in Web Services. *IEEE/IFIP Intl Conf. on Dependable Systems and Networks*.