Modelo de evaluación de seguridad para transmitir datos usando Web Services

Ing. Edgar Gómez Enciso

gomez.enciso@gmail.com

UPG Ingeniería de Sistemas e Informática
Escuela de Posgrado "Pedro Alejandro Fernández"
Universidad Nacional Mayor de San Marcos
Lima, Perú, Lima 32

Resumen. *Las plataformas de Web Services actuales ofrecen diversas soluciones de software basadas en estándares para integrar aplicaciones, automatizar los procesos y transferir información confidencial, motivo por el cual, la seguridad del Web Service es considerado una característica muy importante para una entidad que busca brindar un mejor servicio al usuario, además, obtener una infraestructura integral y disponible, permitiendo compartir información de manera confiable. Una forma de responder a esta necesidad es estimando el nivel de seguridad que se otorga en la transferencia de datos, siendo necesario el desarrollo de un modelo para evaluar la seguridad, usando estándares de evaluación. El modelo de evaluación propuesto responde a la necesidad de disponer de una herramienta que permita estimar la seguridad en la transmisión de datos mediante el Web Service. El modelo permite mostrar los procedimientos para realizar una evaluación a través del análisis de los requerimientos y las métricas de seguridad, en dos casos de estudio, arrojando que el mismo es adecuado, completo y conciso. En este paper, se presentan los conceptos y procesos fundamentales para realizar una evaluación de la seguridad en la transmisión de datos usando el Web Service con el fin de que las entidades puedan contar con un mecanismo confiable y permita determinar los aspectos más relevantes de la seguridad.*

Palabras clave: Evaluación de Seguridad, Métricas de Seguridad, 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. Furthermore, the service provides a comprehensive infrastructure that permits the sharing of information in a reliable manner. One way to fulfill such need is estimating the security level that is offered in transferring data. To this end, it is necessary to develop a model to evaluate security, using standards for evaluation. The proposed model will satisfy the need of having a tool that allows for estimating the security in the transmission of data through the Web Service. The model shows the procedures to perform an evaluation by means of the analysis of the requirements and the security measures. In two case studies, the model proved to be adequate, precise and complete. This paper presents the fundamental concepts to perform an evaluation of the security in the transmission of data using the Web Service, so that the entities can have a reliable mechanism that permits to determine the most relevant security aspects.*

Keywords: Safety Assessment, Security Metrics, Web Services

1. Introducción

La falta de implementación de las medidas de seguridad en los Web Services y el incremento del número de ataques cada vez más especializados y organizados hace importante y fundamental un método para evaluar la seguridad de la transmisión de datos por medio del Web Services que actualmente existen en las empresas e instituciones del sector gobierno.

Los riesgos y las vulnerabilidades de seguridad más comunes que existen en la actualidad, hacen necesaria la tarea de protección y vigilancia de los datos de una entidad. Por medio de esta investigación, se propone un método para evaluar la seguridad en la transmisión de datos, basado en la medición de las métricas y las características de seguridad, detallándose de manera específica los procedimientos necesarios para realizar la evaluación.

Este modelo evalúa las cinco categorías de la seguridad de información: Autenticación, Autorización, Confidencialidad, Integridad y No repudio, las cuales son consideradas importantes, al tener en cuenta los aspectos mínimos de Seguridad que se requieren. El estudio del modelo de evaluación se ha realizado en dos Web Services del sector gobierno. Los resultados muestran que al estimar la evaluación, la seguridad del Web Service se debe enfocar en obtener los riesgos mínimos de las vulnerabilidades.

El principal aporte de este modelo de evaluación es que se ha comprobado con dos casos de estudio, donde se han utilizado estándares de seguridad en su implementación y propone métricas para realizar la evaluación, a partir de los entregables.

2. 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 [Fomin+00]. Los protocolos más estudiados son el XML Encryption, el XML Digital Signature y el WS-Security [Singaravelu +07]. En los últimos años, se ha dado mayor impulso al estudio de las distintas especificaciones de la familia de WS-Security, que se muestra en la figura 2, para tratar el tema de la interoperabilidad y la seguridad de servicios[Miyauchi04] La figura 1 muestra la familia de protocolos del Web

Services.

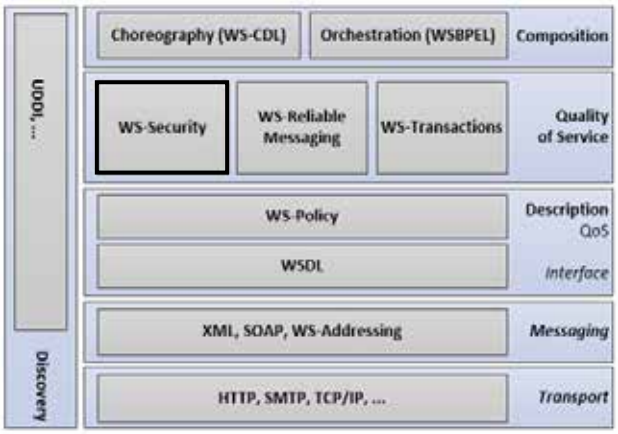

Figura 1. Familia de Protocolos del Web Service [Singaravelu+07].

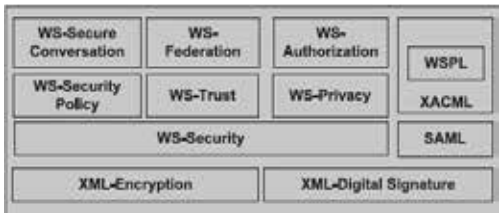

Figura 2. Especificaciones del WS-Security [Singaravelu+07].

2.1 Arquitectura de la seguridad

El objetivo de la Arquitectura del Web Service es precisar los detalles de la seguridad a nivel del mensaje de la lógica de negocios [Uma+11]. En el diseño de la seguridad de aplicaciones del Web Services, la autenticación y autorización son temas importantes de investigación [Singaravelu+07]. La figura 3 muestra el modelo de la arquitectura de ISO-WSP.

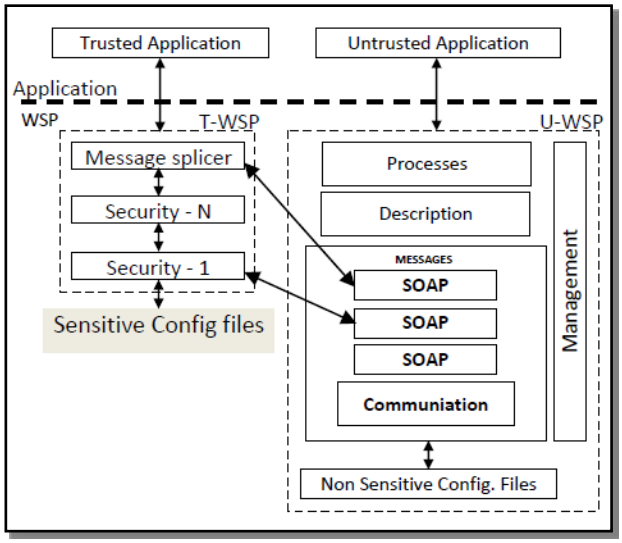

Figura 3. Arquitectura de ISO-WSP [Uma11]

2.2 Seguridad del sistema de información

El objetivo de la seguridad de los sistemas, es mantener la integridad, disponibilidad, privacidad y la autenticidad de la información que es operado por el ordenador [Simens00]. Existe información que debe ser pública, otros pueden ser visualizados por un grupo de usuarios restringidos, y los demás pueden ser accedidos solo por usuarios privados. Para realizar un análisis de la seguridad de la información, se deberá conocer las características de lo que se pretende proteger [Bermeo12].

2.3 Calidad de seguridad del Web Service

La calidad de la seguridad del Web Service es un campo que ha tenido una prolífica actividad investigadora en los últimos años, si bien ha estado centrada en la calidad de los procesos que se siguen en el desarrollo del software [Mougouei+12]. Prueba de ello es la gran cantidad de modelos y estándares de evaluación y mejora de procesos de software que han surgido durante las últimas décadas: ISO 90003, ISO 12207, ISO 15504, CMM, CMMI, etc. En definitiva, son pocas las aportaciones que se han hecho sobre la seguridad, como el reciente estudio de la familia ISO 27000 y anteriormente con ISO 15408 o el NIST SP 800-55 [Piattini+09].

a. NIST SP 800-55

Comprende un conjunto de directrices sobre las medidas de seguridad de la información a nivel de programas. Se emplean controles para ayudar a una organización a evaluar los procedimientos y las políticas de seguridad [Chew08]. Uno de los aspectos más destacados de la norma es la inclusión del modelo de madurez de la organización y los objetivos del modelo de madurez de la seguridad de información [Ross07].

b. ISO/IEC 27001

Basados en el concepto de mejora continua y la seguridad de la información, la norma especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el Ciclo de Deming. La norma es consistente con las mejores prácticas descritas en ISO/IEC 17799 [Brewer+10].

c. ISO/IEC 27004

El estándar fue diseñado para ser usado en conjunción con la norma ISO/IEC 27001, la norma sirve como un documento que orienta el uso de las métricas durante el desarrollo y facilite la evaluación de la conformidad de los controles y los procesos del software [Fomin+00].

3. Modelo Propuesto para la Evaluación de la Seguridad del Web Service

La evaluación del Web Service es un proceso complejo, por ello es muy conveniente que el profesional cuente con un plan de evaluación y con procedimientos específicos bien definidos que le permitan saber en cada caso qué debe hacer y, en definitiva, que le facilite el trabajo. La figura 4 muestra el modelo propuesto para realizar la evaluación de la seguridad del Web Service.

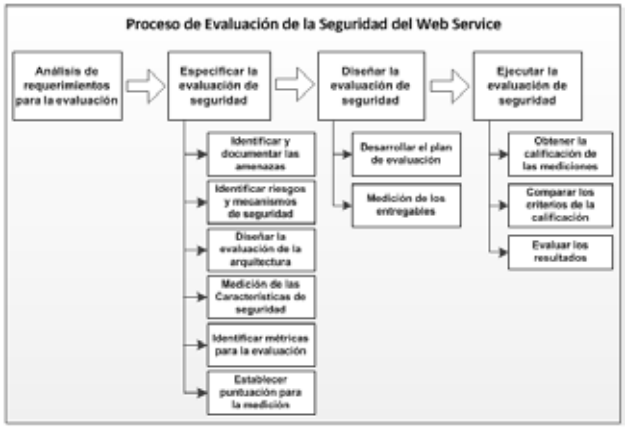

Figura 4. Proceso de evaluación de la seguridad del WS (elaboración propia).

3.1 Análisis de requerimientos para la evaluación

Para realizar el análisis de requerimientos, se establecen controles en cada característica de seguridad a partir de un diagnóstico descriptivo de las necesidades del usuario, los documentos de casos de prueba, las restricciones y los estándares, para llegar a una definición clara de lo que se quiere realizar en la evaluación.

3.2 Especificar la evaluación de seguridad

Realizar un análisis de las especificaciones de seguridad, los artefactos que se poseen y las métricas que se van a emplear para realizar la medición de la evaluación. El proceso de identificar los controles y diseñar el modelo de evaluación, implica tener seleccionados de manera ordenada todos los artefactos para realizar la medición y obtener conclusiones que nos muestre el resultado óptimo.

a. Identificar y documentar las amenazas

Durante el diseño del Web Service, es importante utilizar controles para identificar y evaluar los riesgos de las amenazas más conocidas, luego documentarlos y realizar el seguimiento respectivo mediante pruebas. Para entender mejor, se muestra a continuación una lista de las amenazas más comunes.

- Descubrimiento accidental (usuarios autorizados que pueden toparse con un error en la lógica del WS).
- Atacante curioso (usuarios no autorizados que notaron algo mal en el Web Service).
- Atacante motivado (como personal disgustado o un atacante pagado).
- Malware automatizado (busca las vulnerabilidades conocidas con poco de malicia e inteligencia).
- Crimen organizado (generalmente desfiguran el WS).

b. Identificar riesgos y mecanismos de seguridad

Una forma de identificar los riesgos es aplicando los procedimientos para capturar las evidencias, neutralizando los posibles riesgos y ataques a la seguridad que se presenten, con esto se busca que el impacto sea el menor posible cuando ocurra un incidente, ver la Tabla 1.

Tabla 1: Riesgos y mecanismos de seguridad identificado

Característica	Riesgo de Seguridad	Mecanismo de seguridad
Autenticación	Acceso no autorizado al Web Service	Proporcionar autenticación 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 los datos
Confidencia_ lidad	Acceso a información confidencial	Garantizar el cifrado de los datos confidenciales
No repudio	Negación de una acción realizada	Garantizar el no repudio de la firma digital

c. Diseñar la evaluación de la arquitectura

El arquitecto es el responsable de regular el diseño y la construcción del Web Service. Debe cubrir los riesgos típicos para superar los posibles eventos externos. Si el diseño de la arquitectura determina los atributos de calidad del sistema, entonces es posible evaluar las decisiones arquitectónicas y su impacto sobre dichos atributos.

d. Medición de las características de seguridad

El proceso de medición que se realiza es a partir de los artefactos obtenidos en el análisis de requerimientos, las entrevistas y cuestionarios realizados a los usuarios involucrados con la seguridad del Web Service. Una técnica de evaluación es asignando valores porcentuales a cada característica de seguridad, a continuación se detalla.

Autenticación: Esta métrica mide el número de veces que un atacante debe autenticarse antes de tener el acceso y poder vulnerar la seguridad del Web Service. Cuanto mayor son las condiciones de autenticación, menor es el alcance de la vulnerabilidad, ver la calificación en Tabla 2.

Nivel	Criterio
Múltiple	La protección de autenticidad del usuario es completa (76% a 100%)
Admisible	La protección de autenticidad del usuario no está completa (51% a 75%)
Regular	Tiene poca protección de autenticidad del usuario (26% a 50%)
Simple	Tiene mínima protección de autenticidad del usuario (1% a 25%)

Tabla 2: Calificación de la autenticación

Autorización: Mediante esta métrica se mide cuán complejo resulta aprovechar la vulnerabilidad de acceso. Algunas de las vulnerabilidades, requieren interacción del usuario para obtener un resultado por parte del atacante o requieren condiciones de acceso de Administrador. La tabla 3 muestra la calificación.

Nivel	Criterio
Alto	Existen condiciones de acceso bien específicas para cada usuario (81% a 100%)
Medio-Alto	Las condiciones de acceso no están bien determinados (61% a 80%)
Moderado	Las condiciones de acceso están medianamente definidos (41% a 60%)
Medio-Moderado	Las condiciones de acceso son poco específicas y seguras (21% a 40%)

Bajo	No solicita mínimas condiciones específicas de acceso (1% a 20%)

Tabla 3: Calificación de la autorización

Integridad: La métrica viene a medir el impacto sobre la integridad de la información de un ataque satisfactorio. El efecto del ataque es que el mensaje puede ser modificado sin que el destinatario pueda comprobarlo, para comprobar la integridad del mensaje se adjunta al mismo otro conjunto de datos cifrados. Ver la calificación de la integridad de datos en la tabla 4.

Nivel	Criterio
Integral	Los mensajes mantienen la integridad de la información explícita (81% a 100%)
Medio-Integral	El mensaje es interceptado y bloqueado al ser modificado por un tercero (41% a 60%)
Parcial	La información del mensaje solo es leída por otros usuario (61% a 80%)
Medio-Parcial	Algunos mensajes son interceptados y modificados por terceros (21% a 40%)
Mínimo	Los mensajes sufren modificaciones durante el trayecto al destino (1% a 20%)

Tabla 4: Calificación de la integridad

Confidencialidad: Mediante este valor se mide el impacto sobre la confidencialidad de un ataque satisfactorio. Es la propiedad de prevenir la divulgación de información a personas que no cuenten con la debida autorización. Un incremento de impacto en la confidencialidad, incrementa también el valor de la vulnerabilidad. En la tabla 5, se muestra la calificación.

Nivel	Criterio
Absoluto	La confidencialidad de información es fehaciente para el usuario (76% a 100%)
Regular	La implementación de la confidencialidad de información es incompleta (51% a 75%)
Parcial	La confidencialidad de información está parcialmente implementada (26% a 50%)
Mínimo	Existe mínima confidencialidad de información de mensajes (1% a 25%)

Tabla 5: Calificación de la confidencialidad

No Repudio: Es el valor de la medida del impacto en caso se produzca un ataque exitoso. Es un servicio de seguridad que permite probar la participación de las partes en una comunicación. El no repudio en origen, es porque el destinatario recibe un acuse de recibo del origen de envío, creado por el emisor. El no repudio en destino, es porque el emisor tiene un acuse de recibo que crea el receptor. En la Tabla 6, se observa la calificación.

Nivel	Criterio
Completo	El no repudio de recepción o envío de mensajes es correcto (81% a 100%)
Medio-Completo	El no repudio de recepción o envío de mensajes es casi conforme (61% a 80%)
Parcial	El no repudio de recepción o envío de mensajes está implementado parcialmente (41% a 60%)
Medio-Parcial	El no repudio de recepción o envío de mensajes es deficiente (21% a 40%)
Mínimo	El no repudio de recepción o envío de mensajes es mínima (1% a 20%)

Tabla 6: Calificación del no repudio

e. Identificar métricas para la evaluación

En esta sección se identifican y se elaboran las métricas que serán empleados para realizar las mediciones sobre la seguridad del Web Service. Las métricas nos muestran el resultado de la medición realizada a los entregables del producto, expresado en valores numéricos. Los resultados nos revelan si es necesario implementar mayor seguridad durante la transmisión de datos, o si hay algún mecanismo de seguridad en particular que no es comprendido con claridad durante el desarrollo. La tabla 7 muestra el método de aplicación para evaluar los entregables.

	Métricas	Método de aplicación	Entregables a evaluarse
Autenticación	**AC1.** Autentica_ ción de credenciales del usuario de punto a punto	Contar número de pruebas realizadas a la validación de credenci ales en comparación con la cantidad de validación satisfactoria de las credenciales de los usuarios	- Reporte de pruebas de validación de las credenciales de los usuarios - Reporte de especifi_ caciones de accesos al WS y autorizaciones a los usuarios
	AC2. Verificación de autenticidad del usuario en la capa de transporte	Contar el número de validaciones detectada de autenticación del usuario, en compara_ ción con el número total de validaciones de autenticación de usuario implementadas utilizando el SSL/TSL	- Verificar que los controles de autentica_ ción del usuario se haya realizado con WS-Security o con SSL - Especificaciones de las pruebas de autenti ca ción de usuarios de punto a punto
	AC3. Verificación de autenticidad del origen de datos del usuario	Contar el número de pruebas que verifica la autenticidad del envío de información del usuario, comparado con la cantidad de los mensajes de detección de autenticidad de origen de datos del usuario	- Casos de prueba de implementación para la autenticación de datos del usuario - Reporte de pruebas de autenticación de usuarios en la capa de transporte (SSL/TLS)
	AC4. Utilización de Tokens para la autenticación del usuario	Cantidad de pruebas realizadas a los tokens de seguridad de autenticación de usuarios, en comparación con la cantidad de operaciones ilegales detectadas por el token	- Casos de prueba de los tokens realizados de autenticación de usuarios - Reporte de operaciones ilegales no permitidas por los tokens del WS
	AC5. Capacidad de detectar operaciones ilegales de acceso	Número de controles implementadas para detectar operaciones ilegales de acceso, en comparación con el número controles que detecta las operaciones ilegales realizadas en el acceso de cada usuario	- Casos de prueba de la validación de controles de acceso con pool de datos. - Especificaciones de los controles de acceso del Web Service - Reporte de pruebas con operaciones ilegales detectadas por los controles

Autorización	**AZ1.** Responsabi_ lidad de acceso al Web Service	Número de documentos asignados formalmente por los responsables del WS, en comparación con el total de WS documentados que existen en la institución	- Especificaciones de los accesos autorizados - Reporte de documentos de autorización de accesos - Documento de responsabilidad de los acceso al WS
	AZ2. Capacidad de administrar el control de acceso	Cantidad de WS que son administrados por los usuarios responsables de control de acceso, en comparación con el total de WS que existen en la institución	- Especificaciones de los accesos autorizados por el usuario responsable - Reporte de documentos que autorizan de accesos al WS por el usuario responsable
	AZ3. Conformidad de registro de revisiones de control de acceso	Contar el número de revisiones satisfactorias de pruebas de riesgo de acceso al WS, comparado con el número total de pruebas de riesgo realizadas por roles de usuarios	- Documento de especificaciones de los accesos autorizados por el usuario responsable - Reporte de pruebas a las validaciones de acceso al web Service por roles de usuarios
	AZ4. Capacidad de detectar autorizacio_ nes ilegales de control de acceso	Contar el número de operaciones ilegales de autorización de acceso detectadas, en comparación con el número de pruebas de autorización de acceso con múltiples operaciones realizadas	- 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	**IN1.** Verificación de cobertura de envío de datos	Contar el número de envíos satisfactorios realizados desde el servidor al cliente, comparado con el número total de envío de datos realizados	- Casos de prueba de envío de mensajes realizados - Reporte de pruebas de envío de mensajes realizados a los usuarios
	IN2. Conformidad de integridad del cifrado de mensajes	Cantidad de archivos cifrados digitalmente con WS-SSL/TLS de todo el mensaje, comparado con la cantidad de pruebas de cifrado de mensajes digitalmente	- Reporte de pruebas de autenticación de mensajes implementados con WS-SSL - Reporte de pruebas del correcto cifrado de mensajes punto a punto
	IN3. Integridad de mensajes con firmas digitales	Contar el número de mensajes firmados digitalmente para la autenticación con WS-Security comparado con el número total de pruebas realizadas de firmas digitales	- Reporte de pruebas de autenticación de men_ sajes implementados con WS-Security - Reporte de pruebas de verificación de integridad del mensaje punto-punto
Confidencialidad	**CO1.** Confidencia_ lidad del mensaje en la capa de transporte	Contar el número de pruebas realizadas a las sesiones de envío de mensajes SSL/TLS, en comparación con el número de mensajes enviados con sesiones establecidas	- Casos de prueba del establecimiento de sesiones SSL/TLS - Reporte de pruebas del establecimiento de sesiones SSL/TLS - Reporte de pruebas implementados con WS-Security
	CO2. Utilización de Tokens para confidencia_ lidad de mensajes	Contar el número de mensajes modificados por los tokens incorrectos, en comparación con el total de pruebas realizadas a los tokens de mensajes enviados,	- 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
	CO3. Utilización de certificado X.509 para encriptar y desencriptar mensajes	Contar el número de mensajes encriptados y desencriptados correctamente, en comparación con el número total de pruebas de certificación de mensajes realizados	- 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
	CO4. Validación de envío de mensajes en la estructura y contenido del XML	Contar el número de pruebas de los mensajes validado correctamente, en comparación con el número total de validaciones realizadas en los mensajes.	- Casos de pruebas de validación de datos implementados para los mensajes - Reporte de pruebas de validación de mensajes definidos e implementados
No Repudio	**NR1.** Verificación del no repudio del emisor	Contar el número de archivo implementados con XML-Signature, comparado con número total de pruebas realizado al archivo implementado con XML-Signature	- Reporte de pruebas de conformidad de acuse de recibo de archivos recibidos - Reporte de pruebas al historial de archivos enviados
	NR2. Verificación del no repudio del receptor	Contar número de archivos con acuse de recibo, comparado con el número de pruebas de archivos enviados al destinatario	- Reporte de pruebas al acuse de recibo de archivos enviados - Reporte de pruebas al historial de archivos recibidos

Tabla 7: Identificación de métricas y su método de aplicación para evaluar los entregables

f. Establecer puntuación para la medición

Luego, que se ha identificado las métricas de seguridad de cada característica, se realiza la puntuación porcentual de la seguridad obtenida para cada métrica. Esto sirve para medir el alcance del nivel de seguridad mínimo obtenido para transmitir datos mediante Web Services.

3.3 Diseñar la evaluación de seguridad

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

a. Desarrollar el plan de evaluación

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:

- Especificar los objetivos de la evaluación
- Identificar los indicadores principales

- Trazar las tareas para la recolección y análisis de datos
- Establecer un plan cronológico para el monitoreo

b. Medición de los entregables

Esta evaluación se concluye con un valor que debe ser asignado en función al cumplimiento de las necesidades de seguridad de cada característica. Esta medición se realiza con una valorización a cada entregable con la métrica correspondiente. Para que una evaluación sea satisfactoria, el resultado de cada característica debe ser superior al valor del nivel requerido por el equipo.

3.4 Ejecutar la evaluación de seguridad

Ejecutar la evaluación de la seguridad de un Web Service es una etapa muy importante que se desarrolla en todo el proceso de desarrollo del software. El procedimiento para evaluar durante el análisis de requerimientos y la implementación nos indica la calidad del producto obtenido. El proceso consta de 3 etapas:

a. Obtener la calificación de las mediciones

Para obtener los artefactos de la medición de la seguridad, se utiliza las métricas identificadas en la tabla 7. Luego utilizar un método de evaluación de los entregables, en función al cumplimiento de los requerimientos de seguridad, el resultado nos da el valor del peso obtenido, como se muestra en la tabla 8.

Característica	Métrica	Peso estimado	Peso obtenido	Diferencia	Calificación
Autenti_cación	AC1.	0.940	0.942	0.022	Aceptable
	AC2.	0.960	0.976	0.016	Aceptable
	AC3.	0.972	0.984	0.012	Aceptable
	AC4.	0.935	0.953	0.018	Aceptable
	AC5.	0.976	0.987	0.011	Aceptable
Autorización	AZ1.	0.987	0.977	-0.010	No Aceptable
	AZ2.	0.970	0.975	0.005	Aceptable
	AZ3.	0.980	0.989	0.009	Aceptable
	AZ4.	0.972	0.975	0.003	Aceptable
Integri_dad	IN1.	0.990	0.993	0.003	Aceptable
	IN2.	0.970	0.956	-0.014	No Aceptable
	IN3.	0.980	0.994	0.014	Aceptable
Confidencialidad	CO1.	0.970	0.996	0.026	Aceptable
	CO2.	0.980	0.957	-0.023	No Aceptable
	CO3.	0.982	0.989	0.007	Aceptable
	CO4.	0.980	0.984	0.004	Aceptable
No repudio	NR1.	0.975	0.988	0.013	Aceptable
	NR2.	0.970	0.983	0.013	Aceptable

Tabla 8: Calificación de las medidas de una evaluación

Según la figura 1, se puede manifestar que algunos entregables obtenidos no cumplen con la calificación esperada, 3 de las 18 métricas evaluadas dan un resultado negativo, mostrando que existen vulnerabilidades de seguridad que faltan implementarse en el Web Service. El resultado de la medición de los artefactos, nos sirven para analizar las conclusiones y los resultados obtenidos.

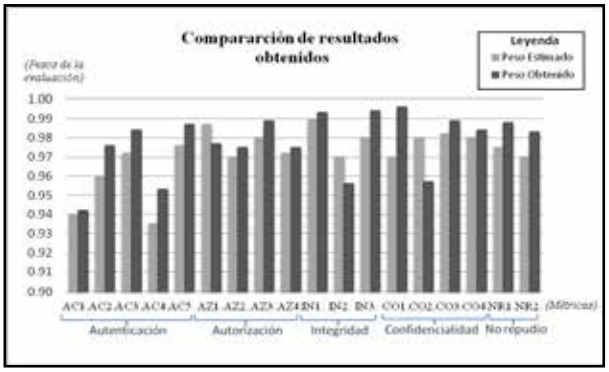

Figura 5. Comparación de resultados obtenidos

b. Comparar los criterios de la calificación

Los criterios que se toman en cuenta para comparar la calificación de los resultados, provienen a partir de una valorización de los entregables con cada métrica. Para que una calificación sea satisfactoria, el peso obtenido debe ser superior al peso estimado de seguridad requerido, ver la tabla 8. El promedio de los pesos estimados y obtenidos hace posible la calificación del nivel obtenido de cada característica de seguridad, como se observa en la tabla 9.

Característica	Peso estimado	Peso obtenido	Nivel obtenido	Resultado
Autenticación	0.953	0.968	Múltiple	Cumple
Autorización	0.977	0.979	Alto	Cumple
Confidencialidad	0.980	0.981	Integral	Cumple
Integridad	0.978	0.982	Absoluto	Cumple
No repudio	0.973	0.986	Completo	Cumple

Tabla 9: Comparación de las características de seguridad

c. Evaluar los resultados

La calificación de las métricas para cada entregable (tabla 8) y el análisis estadístico que se muestra en la figura 1, nos ayudan a describir con claridad la evaluación de la seguridad del Web Service. El resultado de la medición de los entregables, demuestra que en general todas las características de seguridad estimadas (tabla 9), cumplen satisfactoriamente con el requerimiento mínimos exigidos para la evaluación. Para que el modelo de evaluación propuesto tenga veracidad, se ha consultado a expertos dando su respectiva decisión a la conclusión satisfactoria para que el Web Service cumpla con los estándares de seguridad requeridos. Considerando esta técnica de evaluación de la seguridad del Web Service, creemos que se puede predecir las vulnerabilidades que existe en el Web Service durante su implementación o la adquisición.

4. Conclusiones y trabajos futuros

Con la presentación de este trabajo se concluye que, el modelo de evaluación de la seguridad propuesto es completo en cuanto a su especificación de la medición, adecuado en el contexto de evaluación y preciso en el resultado alcanzado. Cabe mencionar, que el modelo de evaluación propuesto es una herramienta metódica que a base de criterios y el uso de alguna técnica, mide, analiza y valora los artefactos con el fin de generar conocimiento útil para la toma de decisiones, la mejora de la gestión y el cumplimiento de los objetivos, obteniéndose un grado de aceptabilidad en la calidad de la transmisión de datos.

En un trabajo futuro, se prevé evaluar el grado de confianza del uso de los servicios en las aplicaciones desarrolladas en plataformas móviles basadas en una interfaz de funcionamiento seguro y confiable.

Referencias bibliográficas

[Brewer+10] D. Brewer, M. Nash: Insights into the ISO/IEC 27001 Annex A, 2010.

[Demchenko+05] Y. Demchenko, L. Gommans: Web Services and Grid Security Vulnerabilities and Threats Analysis and Model, 2005.

[Fernandez12] E. Fernandez: Introduction to the Special Issue on Recent Advances in Web Services, 2012.

[Fomin+00] V. Fomin, H. de Vries: ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for low adoption, 2008.

[Gulati+12] A. Gulati, S. Sharma y P. Mehmi: Proposing Security Requirement Prioritization Framework, 2012.

[Heyman+11] T. Heyman, R. Scandariato: Using Security Patterns to Combine Security Metrics, 2011.

[Islam+11] S. Islam, P. Falcarin: Measuring Security Requirements for Software Security, 2011.

ISO/IEC 17799:2000. Information Technology-Code of Practice for Information Security Management, 2000.

ISO/IEC TR 15504-2. Information Technology-Software Process Assessment, Part 2: A Reference Model Processes and Process Capability, 1998.

[Mougouei+12] D. Mougouei, W. Nurhayati, M. Moein: Measuring Security of Web Services in Requirement Engineering Phase, 2012.

[Miyauchi04] K. Miyauchi: XML Signature/Encryption-the Basis of Web Services Security, 2004.

[Piattini+09] D. Mellado, M. Piattini: Evaluación de la Calidad y Seguridad en Productos Software, 2009.

[Singaravelu+07] L Singaravelu, J Wei, C Pu: A Secure Middleware Architecture for Web Services, 2007.

[Stranacher09] K. Stranacher: Web-Service based transformation of digital signature formats, 2009.

[Uma+11] E. Uma, A. Kannan: Design of New Architecture for Providing Secure Web Services, 2011

[Venezia+06] C. Venezia. P. Falcarin: Communication Web Services Composition and Integration, 2006.

[W3C14] W3C-World Wide Web Consortium, 2014 http://w3c.es/