TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones

Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

Arquitectura para la detección violaciones a políticas de seguridad utilizando el método ABD

Yohandra Echeverria Castillo[1*], Mónica peña Casanova [2] ,Bárbara Laborí de la Nuez [3]

[1,2,3] Facultad 2, Universidad de las Ciencias Informáticas. Carretera a San Antonio Km 2 ½ Torrens. Boyeros. La Habana. Cuba.
[1] yoha@uci.cu, [2] monica@uci.cu, [3] barbaral@uci.cu

RESUMEN

Las trazas poseen una gran relevancia en la gestión de la seguridad informática, debido a que la información que en ellas se registran contribuye en las actividades de auditoría y análisis forense. Entre las trazas asociadas a la seguridad se encuentran las trazas generadas por el acceso a los servicios de red, específicamente a Internet a través de un proxy que permiten la identificación de violaciones de seguridad. A consecuencia de la transformación constante de los sistemas informáticos y al surgimiento de herramientas automáticas para gestionar las trazas, se hace necesario integrar las funcionalidades propias de las arquitecturas de software con los requisitos de seguridad informática definidos en la organización. En el presente artículo se expone mecanismos que determinarán la calidad de la arquitectura propuesta. Se propone una arquitectura para la detección de violaciones de seguridad a partir del análisis de trazas de navegación de Internet de los usuarios, basándose el método ABD (Método de Diseño Basado en la Arquitectura por sus siglas en inglés) y la arquitectura de seguridad de sistemas de información propuesta por el Instituto SANS para el diseño y descripción de los componentes de la arquitectura.

Palabras clave: trazas, usuarios, violaciones, seguridad, ABD

Architecture for detecting violations of security policies using the ABD method

ABSTRACT

Traces are highly relevant in computer security management, because the information recorded in them contributes to auditing and forensic analysis activities. Among the traces associated with security are the traces generated by access to network services, specifically the Internet through a proxy that allow the identification of security violations. As a result of the constant transformation of computer systems and the emergence of automatic tools to manage traces, it is necessary to integrate the functionalities of software architectures with the computer security requirements defined in the organization. This article exposes mechanisms that will determine the quality of the proposed architecture. Architecture is proponed for the detection of security violations from the analysis of Internet browsing traces of users, based on the ABD method (Architecture-Based Design Method) and the system security architecture of information proponed by the SANS Institute for the design and description of the components of the architecture.

INDEX TERMS: traces, users, violations, security, ABD

1. INTRODUCCIÓN

Las trazas poseen una gran relevancia en la gestión de la seguridad informática, debido a que la información que en ellas se registran contribuye en las actividades de auditoría y análisis forense, en el apoyo a investigaciones internas, establecimiento de líneas base y en la identificación de tendencias operacionales y problemas de comportamiento de los sistemas de información. Según el tipo de aplicaciones, se tienen trazas de software asociadas directamente a la seguridad y trazas relativas a los sistemas operativos, las aplicaciones y servicios que se encuentran en ejecución [1].

Según una encuesta realizada por el Instituto SANS (por sus siglas en inglés SysAdmin, Audit, Network, Security) la mayoría de las organizaciones, independientemente de su dimensión y las soluciones que tengan implantadas, no hacen uso en su totalidad de la información contenida en las traza [2]. Muchas de las herramientas que utilizan los especialistas de seguridad informática para obtener información a partir de las trazas obtenidas, no generan alarmas relacionada a las violaciones que cometen los usuarios cuando acceden a Internet a través de la red de las organizaciones, específicamente, las violaciones relacionadas a robo de credenciales y accesos a sitios comprometidos. Generalmente la revisión de las trazas, especialmente las de la navegación en Internet de los usuarios, ocurre ante la notificación de un evento, lo que hace que se proceda a buscar evidencia digital. Debido a que el cúmulo

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

de datos que se almacena en las trazas es tan grande, en reiteradas ocasiones el especialista no encuentra la información necesaria en tiempo.

El proceso de detección de violaciones de seguridad a partir del análisis de trazas de la navegación de Internet de los usuarios, requiere de variantes que normalicen los formatos existentes. Se deben definir estrategias de análisis y búsquedas que permitan la generación de alarmas y reportes ante la detección de alguna violación de seguridad a las políticas establecidas en la organización. En el presente artículo se expone un análisis de los diferentes formatos para definir la estructura de las trazas. Se propone una arquitectura para la detección de violaciones de seguridad a partir del análisis de trazas de navegación de Internet de los usuarios, siguiendo el método de diseño ABD complementado con la arquitectura de seguridad de sistemas de información propuesta por el Instituto SANS para el diseño y descripción de los componentes de la arquitectura. Se determina un formato común para la estandarización de la estructura de las trazas, permitiendo una mayor capacidad de análisis. Se evalúan las herramientas necesarias para la implantación de la arquitectura propuesta.

2. ENTRADAS DEL MÉTODO ABD

Partiendo por lo planteado por los analistas y especialistas de SourceForge [3], las funciones críticas que se deben tener en cuenta en la gestión de las trazas son las siguientes:

- ✓ Gestionar el almacenamiento de trazas.
- ✓ Gestionar el inventario de elementos gestionables.
- ✓ Proteger de los datos frente a modificaciones no autorizadas.
- ✓ Monitorear y generar alertas.
- ✓ Gestionar la configuración.
- ✓ Gestionar la búsqueda avanzada.
- ✓ Generar reportes e informes.
- ✓ Gestionar usuarios.
- ✓ Visualizar datos.

Requisitos funcionales abstractos

Los requisitos funcionales son las manifestaciones de cómo deben comportarse los sistemas. Definen la manera en que el sistema debe reaccionar a entradas particulares satisfaciendo las necesidades o expectativas del usuario. No obstante, como los requisitos funcionales suelen ser muy numerosos, pueden ser establecidos en diferentes niveles de abstracción, siendo concretados en las funcionalidades de un sistema [4]. En la Tabla 1 se presentan un conjunto de requisitos funcionales abstractos que pueden ofrecer la mayoría de las arquitecturas para la gestión de traza, procedentes de las funciones críticas analizadas con anterioridad.

Tabla 1: Requisitos funcionales abstractos.

Funciones	Requisitos funcionales abstractos
Gestionar el almacenamiento de trazas	Definir el tiempo de almacenamiento
	Gestionar la forma de almacenamiento
	Guardar las trazas que se generan
	Gestionar elementos automatizados

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

Gestionar el inventario de elementos gestionables.	Gestionar elementos no automatizados
	Registrar impacto de elementos gestionables
Proteger los datos a modificaciones no autorizadas	Realizar salvas de las trazas almacenadas
Monitorear y generar alarmas	Gestionar el monitoreo de las trazas
	Gestionar la generación de alarmas
Gestionar la configuración	Registrar configuraciones de computadoras
	Registrar configuraciones de sistemas operativos
	Registrar configuraciones de los servicios
Gestionar la búsqueda avanzada	Gestionar búsquedas avanzadas, a través de filtros
Generar reportes e informes	Obtener reporte sobre el análisis de los datos de las trazas
	Generar informes
Gestionar usuarios	Gestionar roles para el acceso a las trazas
Visualizar datos	Gestionar la visualización de los datos de las trazas

Requisitos de calidad

En las arquitecturas de gestión de trazas, la seguridad es un aspecto de criticidad alta, ya que puede verse comprometida información sensible, obtener acceso total a las trazas, y se puede interceptar, bloquear, o modificar cualquier dato almacenado en las trazas. La seguridad es la medida de la habilidad del sistema para resistir a usos no autorizados, mientras sigue proveyendo sus servicios. Además de asegurar la seguridad en cada una de las capas con el establecimiento de mecanismos [5]. De forma genérica se puede caracterizar sobre la base de los siguientes aspectos:

- ✓ Seguridad.
- ✓ Rendimiento.

En la Tabla 2, se muestran los requisitos asociados a la calidad de los atributos definidos anteriormente.

Tabla 2: Requisitos asociados a la calidad y sus atributos.

Ejemplos de requisitos asociados a la calidad y sus atributos	
Requisitos de rendimiento (RR)	
RR1	Establecer límites de tamaño y cantidad de trazas recolectadas y enviadas
RR2	Proporcionar mecanismos para enviar las trazas recolectadas
RR3	Optimizar los procesos realizados para ser ejecutados en el menor tiempo posible.

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

Requisitos de seguridad (RS)	
Requisitos de Integridad (RI)	
RI1	Comprobación de la autoría de la información enviada.
RI2	Almacenar y realizar copias de seguridad de las trazas almacenadas.
RI3	Poseer mecanismos para la transmisión segura de las trazas
Requisitos de confidencialidad (RC)	
RC1	Poseer un registro de los informes y reportes generados.
RC2	Poseer un mecanismo de control de acceso por roles.
Requisitos de disponibilidad (RD)	
RD1	Proveer mecanismos de almacenamiento y respaldo de los datos.
RD2	Proporcionar mecanismos de recuperación ante fallos
RD3	Proporcionar mecanismos para soportar múltiples tecnologías
Requisitos de aspectos del negocio y objetivos de la organización (RN)	
RN1	Proveer mecanismos que garanticen el desarrollo basado en componentes a partir de un conjunto común de activos fundamentales
RN2	Proveer mecanismos que garanticen la reutilización de componentes.
RN3	Proveer mecanismos que garanticen la reutilización de componentes de terceros.

Restricciones

Para garantizar el funcionamiento correcto de la arquitectura para la gestión de trazas, se tienen en cuenta ciertas restricciones, para el despliegue de la mismas [6]. El listado de restricciones, asociadas a los atributos antes descritos, se muestra en la Tabla 3.

Tabla 3: Listado de restricciones de entrada al método ABD.

Restricción	Atributo	Descripción
R1	Disponibilidad	El sistema debe funcionar las 24 horas de los 7 días de la semana durante todo el año.
R2	Disponibilidad	Se debe garantizar que la información que proveen las diferentes herramientas se encuentre disponible en un repositorio centralizado.
R4	Rendimiento	Se debe ajustar el período de monitoreo y las acciones de control.

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

R5	Seguridad	El acceso está controlado a través de un mecanismo de autenticación, el transporte y almacenamiento de trazas a través de mecanismos de cifrado.

Estrategias arquitectónicas

Teniendo en cuenta los requerimientos, atributos de calidad y restricciones se han seleccionado un conjunto de decisiones arquitectónicas las cuales, garantizan el éxito de la arquitectura:

- ✓ Adoptar arquitectura por capas.
- ✓ Utilizar mecanismos de sincronización entre tareas.
- ✓ Reutilizar componentes antes que construir.
- ✓ Emplear opciones arquitectónicas de encapsular y separación de conceptos.
- ✓ Monitorizar y controlar la recolección, almacenamiento y análisis de las trazas.
- ✓ Autenticación de usuarios.
- ✓ Identificación y detección de violaciones y ataques.
- ✓ Empleo de estándares para normalización de las trazas.

3. ADVPS: ARQUITECTURA PARA LA DETECCIÓN DE VIOLACIONES A POLÍTICAS DE SEGURIDAD, A PARTIR DEL ANÁLISIS DE LAS TRAZAS DE ACCESOS A INTERNET DE LOS USUARIOS.

Una vez seleccionados los requerimientos funcionales los atributos de calidad y las estrategias arquitectónicas a emplear, se procede en este apartado a describir la arquitectura ADVPS, diseñada con el objetivo de detectar violaciones a políticas de seguridad, a partir del análisis de las trazas de acceso a Internet de los usuarios

Principios de la ADVPS

Los principios de esta arquitectura se pueden resumir en los siguientes puntos:

- ✓ Escalable: posibilita que se puedan incorporar nuevos elementos de seguridad u otros equipos a la arquitectura.
- ✓ Tolerante a fallos: después de un fallo el tiempo estimado de recuperación debe ser mínimo y se debe recuperar la mayor cantidad de información.
- ✓ Eficiente: todos los sistemas de la arquitectura funcionan a su nivel óptimo, sin sobrecargarse.
- ✓ Segura: la arquitectura debe garantizar la seguridad en cada una de sus capas.
- ✓ Generalizable: podrá ser desplegada en cualquier organización que requiera la realización del análisis de trazas.
- ✓ Tecnológicamente independiente: la arquitectura es independiente de la tecnología que se emplee en cada organización.
- ✓ Bajo Acoplamiento: la arquitectura posibilita la modificación de una capa sin afectar a otras.

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

Premisas para la aplicación de la ADVPS

Adicionalmente se tienen en cuenta un conjunto de premisas consideradas necesarias para el despliegue exitoso de la ADVPS, obtenidas del análisis de las arquitecturas de seguridad. Estas son:

- El personal que opera las herramientas de despliegue de la arquitectura debe estar familiarizado con los objetivos de la organización y estar calificado tanto para operar la tecnología instalada como para apoyar los procesos que se desarrollan en la organización.
- La organización debe incentivar la adopción y el cumplimiento de políticas de seguridad informática para establecer el acceso a Internet por parte de los usuarios. Además de debe existir un marco jurídico asociado al uso de las infraestructuras de las Tecnología de la Información (TI).
- La organización debe contar con una infraestructura de hardware, que pueda ser utilizada para la gestión de las trazas sin que se comprometa el funcionamiento de la red y los servicios.

Estructura organizativa de la arquitectura

La arquitectura para la detección automática de violaciones a políticas de seguridad se ha dividido en cinco capas (generación, recolección y envío, normalización, almacenamiento, análisis, visualización de información y monitoreo) tal como se muestra en la. Fig.1. Una vez generadas las trazas, una herramienta se encarga de recolectar y enviar las trazas para su posterior almacenamiento e indexación, permitiendo las funciones de visualización y análisis de las trazas. Cada uno de las capas de la arquitectura están formado por herramientas que trabajan de forma integrada. La utilización de varias herramientas y su instalación requiere del manejo de múltiples ficheros de configuración.

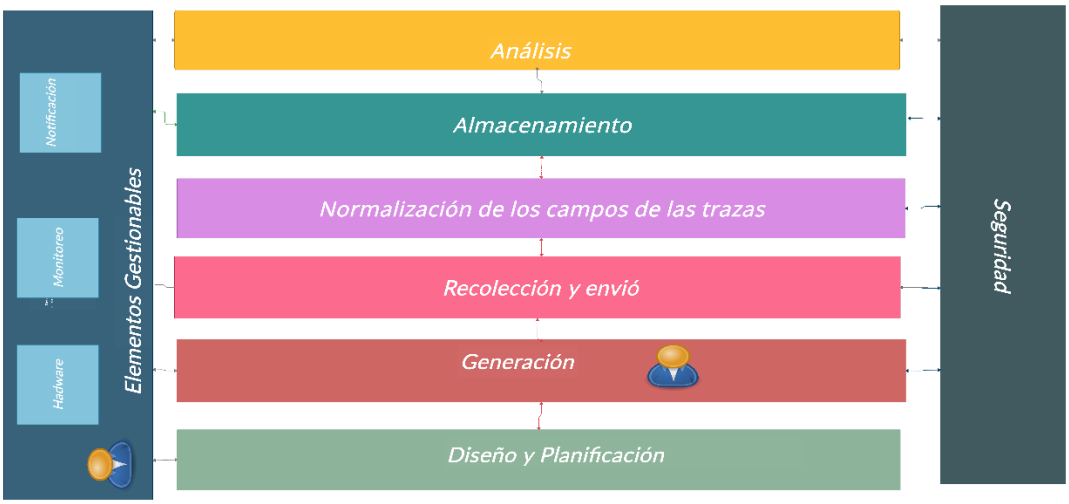

Figura 1: Componentes generales de la arquitectura para la detección de violaciones a políticas de seguridad.

4. RESPONSABILIDADES, ATRIBUTOS DE CALIDAD Y CAPAS DE ADVPS

En aras de profundizar en los detalles de ADVPS a continuación se presenta la relación entre los atributos de calidad y las capas que forman la arquitectura en la Tabla 4. De esta forma se evidencia como cada componente de la solución satisface uno o varios atributos de calidad que garantizan el éxito de la arquitectura [7].

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

Tabla 4: Relación componentes, responsabilidad y atributos de calidad de ADVPS.

Capas	Responsabilidad	Atributo
Recolección y envió		
	Establecer el límite de la cantidad de traza recolectadas	Rendimiento
	Utilizar el protocolo TCP para la transmisión de las trazas	Seguridad Rendimiento
	Utilizar mecanismos de cifrado de extremo a extremo para él envió de las trazas	Seguridad Rendimiento
Normalización de las trazas		
	Normalizar los campos de las trazas, permitiendo la optimización de los tiempos de búsquedas	Rendimiento
Almacenamiento		
	Realizar copias de seguridad de las trazas almacenadas.	Seguridad
	Proveer mecanismos de almacenamiento y respaldo de los datos.	Seguridad
	Proporcionar mecanismos de recuperación ante fallos	Seguridad
	Poseer un mecanismo de control de acceso por roles.	Seguridad
Análisis		
	Generar reportes	Seguridad
	Generar informes de los eventos detectados	Seguridad
Seguridad		
	Establecer mecanismos de seguridad sobre los medios de transporte	Seguridad

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

	Establecer procedimientos sobre los activos que generan las trazas, mediante el control de acceso, roles y responsabilidades	Seguridad
	Establecer la capacidad de recursos para el almacenamiento	Seguridad

Relación de los requisitos de calidad abstractos y las estrategias arquitectónicas

Mediante los requisitos de calidad abstracto la arquitectura puede alcanzar sus atributos y definir la forma en que la arquitectura puede modificarse e integrarse con otros sistemas [8]. En la Tabla 5 se describen la relación de los requisitos de calidad abstractos y las estrategias arquitectónicas.

Tabla 5: Relación de los requisitos de calidad abstracto y las estrategias arquitectónicas.

Atributo	Requisitos abstractos de calidad	Estrategias arquitectónicas	ADVPS
Aspectos del negocio y Objetivos de la Organización	Proveer mecanismos que garanticen la reutilización de componentes. Proveer mecanismos que garanticen el desarrollo basado en componentes a partir de un conjunto común de activos fundamentales	Emplear opciones arquitectónicas de encapsular y separación de conceptos. Adoptar arquitectura por capas	Organización de la arquitectura por capas. Reutilización de componentes. Puede ser desplegada en cualquier organización que requiera la realización del análisis de trazas.
Seguridad	Poseer un mecanismo de control de acceso por roles. Poseer un registro de los informes y reportes generados	Autenticación de usuarios Monitorizar y controlar la recolección, almacenamiento y análisis de las trazas	Garantizar la seguridad en cada una de sus capas. Las trazas se almacenan en una infraestructura de almacenamiento segura y bien administrada
Seguridad	Proveer mecanismos de almacenamiento y respaldo de los datos Proporcionar mecanismos de recuperación ante fallos Proporcionar mecanismos para soportar múltiples tecnologías	Arquitectura por capa. Tolerancia a fallos Mecanismos de sincronización entre tareas	Es independiente de la tecnología que se emplee en cada organización para puesta en funcionamiento de los sistemas y servicios Las herramientas de despliegue permiten la tolerancia a fallos
Rendimiento	Establecer límites de tamaño y cantidad de trazas recolectadas y enviadas	Emplear opciones arquitectónicas de encapsular y separación de conceptos.	Organización de la arquitectura por capas. Establecimiento de rangos de tiempo para el

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

	Proporcionar mecanismos para enviar las trazas recolectadas Optimizar los procesos realizados para ser ejecutados en el menor tiempo posible	Utilizar mecanismos de sincronización entre tareas	monitoreo y análisis de las trazas.

5. VALIDACIÓN DE LA ARQUITECTURA

Se realizó la aplicación de Focus Group para evaluar el proceso de gestión de trazas de navegación de Internet de los usuarios. Se seleccionaron 7 especialistas de seguridad para realizar la evaluación del comportamiento que presenta las soluciones sobre la base de los atributos de calidad propuestos, los cuales a partir de sus propias experiencias evaluaron el comportamiento. Los resultados de la técnica se muestran en la Tabla 6.

Tabla 6: Resultado de la aplicación de la técnica Focus Group.

Atributo	Estado
Rendimiento	65%
Seguridad	80%

Árbol de Utilidad

A partir de los requisitos del negocio abstractos se genera el árbol de utilidad (Ver la Tabla 9) en base a los requerimientos de los atributos de calidad y las directrices que presenta la arquitectura ADVPS. El árbol de utilidad contiene los escenarios que ponen a prueba a la arquitectura ADVPS. Se construyó con el objetivo de verificar el cumplimiento de los requerimientos de los atributos de calidad observados como escenarios. Teniendo en cuenta la priorización de cada escenario en base a dos dimensiones (D1, D2) [9]:

D1: Importancia del escenario en relación al éxito del sistema, el cual emplea para su valoración los criterios que se muestran en la Tabla 7.

Tabla 7: Criterios de valoración de la dimensión D1.

Importancia	Descripción	Valor
Bajo (B)	Importancia casi nula para el éxito del sistema.	1
Medio (M)	Importancia media para el éxito del sistema.	2
Alto (A)	Importancia alta para el éxito del sistema.	3

- D2: Grado de dificultad que posee el escenario para ser realizado por la arquitectura, según la estimación que se muestra en la Tabla 8.

Tabla 8: Criterios de valoración de la dimensión D2.

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

Dificultad	Descripción	Valor
Bajo (B)	Esfuerzo bajo para cumplir el escenario.	1
Medio (M)	Esfuerzo medio para cumplir el escenario.	2
Alto (A)	Esfuerzo alto para cumplir el escenario.	3

En la Tabla 9, se muestra el listado de escenarios, propuestos por los especialistas consultados en para los atributos, disponibilidad, seguridad y rendimiento. Además, inspirados en el Método de Análisis de Acuerdos de Arquitectura (en lo adelante ATAM) [8-10], para cada escenario se evaluaron su importancia y su valor en los que, el aseguramiento de un atributo de calidad, puede afectar el cumplimiento de otro.

Tabla 9: Árbol de utilidad.

Requisito	Escenarios	Evaluación	Puntaje
Seguridad			
	Las herramientas que despliegan la arquitectura sufren una falla y deja de funcionar, el sistema debería estar en funcionamiento en un servidor de contingencia en al menos 3 minutos.	(A,B)	(3,1)
	Si el sistema reporta un mensaje de error de cualquier índole al usuario, el sistema seguirá su funcionamiento normalmente.	(A,M)	(3,2)
	El sistema está disponible las 24 horas durante los 7 días de la semana.	(A,B)	(3,1)
	Si existe un fallo eléctrico, el sistema puede iniciar nuevamente sin problemas.	(A,B)	(3,1)
	Un usuario está habilitado para visualizar cierta información de la base de datos, pero no información restringida.	(A,B)	(3,1)
	Solo el administrador de la red y otros usuarios con permisos de súper usuario poseen las autorizaciones para	(A,M)	(3,2)

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

	trabajar y modificar utilizando el sistema.		
Rendimiento			
	Se pueden hacer solicitudes simultáneas	(A,M)	(3,2)
	Extraer las salvas de información cuando el sistema se encuentre en su menor carga de procesamiento.	(A,B)	(3,2)

Los resultados son la consecuencia de calcular el promedio entre los pesos de los escenarios para cada atributo. Los pesos de los escenarios se obtienen a partir de la relación entre importancia y esfuerzo [10]. En la Tabla 10 se muestra un listado de los escenarios priorizados con su puntuación correspondiente.

Tabla 10: Listado de escenarios priorizados.

Requisito	Escenarios	Evaluación	Puntaje	Impacto
Seguridad				
	Las herramientas que despliegan la arquitectura sufren una falla y deja de funcionar, el sistema debería estar en funcionamiento en un servidor de contingencia en al menos 3 minutos.	(A,B)	(3,1)	90%
	Si el sistema reporta un mensaje de error de cualquier índole al usuario, el sistema seguirá su funcionamiento normalmente.	(A,M)	(3,2)	60%
	Si existe un fallo eléctrico, el sistema puede iniciar nuevamente sin problemas.	(A,B)	(3,1)	80%
	Un usuario está habilitado para visualizar cierta información de la base de datos, pero no información restringida.	(A,B)	(3,1)	100%
Rendimiento				
	Se pueden hacer solicitudes simultáneas	(A,M)	(3,2)	90%
	Extraer las salvas de información cuando el sistema se encuentre en su menor carga de procesamiento.	(A,B)	(3,2)	90%

Resultados de la evaluación de la arquitectura ADVPS mediante el método ATAM

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 3, Julio-Septiembre, 2023, p. 43-55 ISSN 1729-3804

La evaluación de la propuesta arquitectónica frente a los escenarios priorizados fue de gran utilidad para analizar las debilidades y fortalezas de la arquitectura ADVPS. Teniendo en cuenta los riesgos, puntos de concesión y de sensibilidad encontrados a partir de la evaluación realizada, facilita que se adhieran a la arquitectura de software nuevos componentes. En la Fig. 2 se establece una comparación entre el estado de los atributos antes y después de aplicar la arquitectura. Los resultados son obtenidos a partir de la aplicación de técnica de Focus Group, notando un aumento en los requisitos de calidad de la investigación.

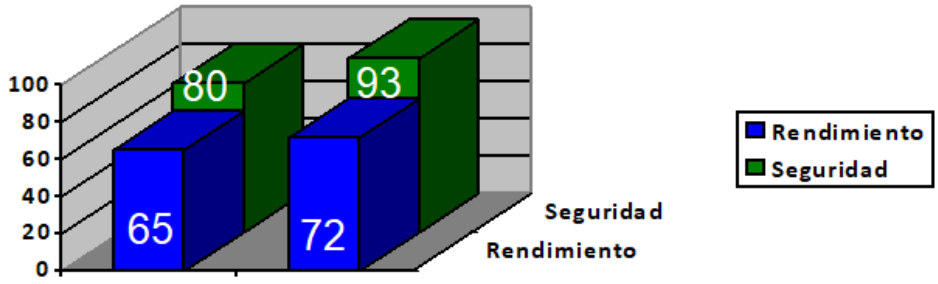

Figura 2: Comparación de los estados anteriores de los requisitos de calidad.

6. CONCLUSIONES

El empleo del método ABD facilita el diseño de la arquitectura de ADVPS a partir de los requisitos procedentes de las funciones críticas establecidas. Estas funciones pueden ser ofrecidas por la mayoría de las arquitecturas para la gestión de trazas. El método de evaluación de arquitectura ATAM y grupo focal demuestran el impacto positivo de la arquitectura en los atributos de calidad. Lo cual demuestra como el diseño de la arquitectura contribuye a elevar los atributos de calidad seguridad de la información contenida en las trazas y el rendimiento de las herramientas que intervienen en el despliegue de la arquitectura.

REFERENCIAS

[1] D. Schipper, M. Aniche, y A. van Deursen, Tracing Back Log Data to its Log Statement: From Research to Practice, 2019 IEEE/ACM 16th International Conference on Mining Software Repositories (MSR), may 2019, pp. 545-549. doi: 10.1109/MSR.2019.00081.

[2] Dale, Chris, «2020 SANS Enterprise Cloud Incident Response Survey | SANS Institute». https://www.sans.org/white-papers/39805/ (accedido sep. 05, 2021).

[3] J. Rushby, Bus Architectures for Safety-Critical Embedded Systems, en Embedded Software, Berlin, Heidelberg, 2001, pp. 306-323. doi: 10.1007/3-540-45449-7_22.

[4] K. Siu, H. Herencia-Zapana, D. Prince, y A. Moitra, A Model-Based Framework for Analyzing the Security of System Architectures, en 2020 Annual Reliability and Maintainability Symposium (RAMS), ene. 2020, pp. 1-6. doi: 10.1109/RAMS48030.2020.9153607.

[5] G. Mazlami, J. Cito, y P. Leitner, Extraction of Microservices from Monolithic Software Architectures, en 2017 IEEE International Conference on Web Services (ICWS), jun. 2017, pp. 524-531. doi: 10.1109/ICWS.2017.61.

[6] C. Castellanos, B. Pérez, D. Correal, y C. A. Varela, A Model-Driven Architectural Design Method for Big Data Analytics Applications, en 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), mar. 2020, pp. 89-94. doi: 10.1109/ICSA-C50368.2020.00026.

[7] F. Bachmann, L. Bass, G. Chastek, P. Donohoe, y F. Peruzzi, The Architecture Based Design Method, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, ene. 2000. Accedido: sep. 06, 2021. [En línea]. Disponible en: https://apps.dtic.mil/sti/citations/ADA375851

[8] M. U. Ashraf y W. Aljedaibi, ATAM-based Architecture Evaluation Using LOTOS Formal Method, Int. J. Inf. Technol. Comput. Sci., vol. 9, pp. 10-18, mar. 2017, doi: 10.5815/ijitcs.2017.03.02.

[9] Rick Kazman, Mark Klein, y Paul Clements, ATAM:SM Method for Architecture Evaluation. TECHNICAL REPOR, ago. 2000. Disponible en: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2000_005_001_13706.pdf

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

[10] M. U. Ashraf y W. Aljedaibi, «ATAM-based Architecture Evaluation Using LOTOS Formal Method», Int. J. Inf. Technol. Comput. Sci., vol. 9, pp. 10-18, mar. 2017, doi: 10.5815/ijitcs.2017.03.02.

[11] Rick Kazman, Mark Klein, y Paul Clements, «ATAM:SM Method for Architecture Evaluation». TECHNICAL REPOR, ago. 2000. Disponible en: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2000_005_001_13706.pdf

[12] M. Zaharaddeen, «Software architecture evaluation using Architecture Tradeoff Analysis Method (ATAM): A case study UUM learning zone system», Accedido: sep. 07, 2021. [En línea]. Disponible en: https://www.academia.edu/33276426/Software_architecture_evaluation_using_Architecture_Tradeoff_Analysis_Method_ATAM_A_case_study_UUM_learning_zone_system

[13] M. Zaharaddeen, Software architecture evaluation using Architecture Tradeoff Analysis Method (ATAM): A case study UUM learning zone system», Accedido: sep. 07, 2021. [En línea]. Disponible en: https://www.academia.edu/33276426/Software_architecture_evaluation_using_Architecture_Tradeoff_Analysis_Method_ATAM_A_case_study_UUM_learning_zone_system

SOBRE LOS AUTORES

- **Yohandra Echeverria Castillo**: Ingeniera en Ciencias Informática. Especialista de Seguridad Informática, Profesor Asistente.No.ORCID: 0000-0001-6163-2819
- **Mónica peña Casanova**: Ingeniera en Telecomunicaciones, Máster en Telemática y Doctora en Ciencias Técnicas. Profesora Titular. No.ORCID: 000-0003-2500-4510
- Bárbara Laborí de la Nuez: Ingeniera en Electrónica.Máster en Sistemas Digitales. Profesora Asistente. Jefa del Programa De Educación Superior de Ciclo Corte de Administración de Redes y Seguridad Informática. No.ORCID: 0000-0001-8114-0969

CONFLICTO DE INTERESES

No existen conflictos de intereses ni de los autores ni de las instituciones a las cuales pertenece en relación al contenido del artículo aquí reflejado.

CONTRIBUCIONES DE LOS AUTORES

Debe especificar la contribución de cada autor al presente artículo atendiendo a su porciento de contribución y los aspectos atendidos (Ej: conceptualización, preparación, creación y desarrollo del artículo, revisión crítica de cada una de las versiones del borrador del artículo y aprobación de la versión final a publicar, contribución a la idea y organización del artículo, sugerencias acertadas para la conformación de la versión final)

- **Yohandra Echeverria Castillo**: conceptualización: 100%, preparación:100%, creación:100%y desarrollo del artículo :100%, revisión crítica de cada una de las versiones del borrador del artículo:80%y aprobación de la versión final a publicar:100%, contribución a la idea: 100%y organización del artículo: 100%, sugerencias acertadas para la conformación de la versión final:100%.
- **Mónica Peña Casanova**: conceptualización: 100%, preparación:100%, creación:90%y desarrollo del artículo 90%, revisión crítica de cada una de las versiones del borrador del artículo:100%y aprobación de la versión final a publicar:100%, contribución a la idea: 100%y organización del artículo: 100%, sugerencias acertadas para la conformación de la versión final:100%.
- **Bárbara Laborí de la Nuez**: conceptualización: 100%, preparación:100%, creación:90%y desarrollo del artículo 90%, revisión crítica de cada una de las versiones del borrador del artículo:100%y aprobación de la versión final a publicar:100%, contribución a la idea: 100%y organización del artículo: 100%, sugerencias acertadas para la conformación de la versión final:100%.

Manuscrito recibido: 06-01-2022, aceptado: 04-05-2023
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele