ISSN 0798 1015

REVISTA ESPACIOS

4 décadas difundiendo conocimiento

Vol. 41 (Nº 17) Año 2020. Pág. 20

Modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube con base en las normas ISO 27017 y 27018

Safety model for mitigation of vulnerabilities in cloud storage environments based on ISO 27017 and 27018

TENELEMA, Esthela N. 1; MÉNDEZ, Pablo M. 2; VILLA, Henry M. 3; CAIZA, Diego G. 4

Recibido: 30/01/2020 • Aprobado: 28/04/2020 • Publicado 14/05/2020

Contenido

RESUMEN:
Se elaboró un modelo de seguridad basado en las normas ISO 27017 y 27018; se evaluó en dos escenarios: el primero con el modelo de seguridad y el segundo que no lo considera; se establecieron y ponderaron los posibles riesgos, estableciéndose los más críticos. El modelo contempla directrices de seguridad para aliviar problemas comunes de almacenamiento en la nube. La probabilidad de que los riesgos ocurran se redujo un 75 % en comparación con el prototipo que no las considera.
Palabras clave: Almacenamiento de la nube, modelo de seguridad, norma ISO 27017, norma ISO 27018.

ABSTRACT:
A security model based on ISO 27017 and 27018 standards was developed; it was evaluated in two scenarios; the first with the security model and the second that does not consider it; Possible risks were established and weighted, establishing the most critical ones. The model includes security guidelines to alleviate common cloud storage problems; the probability of risks occurring was reduced by 75% compared to the prototype that does not consider them.
Keywords: Cloud storage, security model, ISO 27017, ISO 27018.

1. Introducción

Hoy en día tener la información digitalizada ya no es suficiente. Se requiere copia de seguridad en la nube para las cantidades ingentes de información que acumulan empresas y particulares. Correos electrónicos, vídeos, fotos, música y otros tantos contenidos y servicios se gestionan a través de la nube (Gastón, 2017). Dicho de manera sencilla, la informática en la nube es el suministro de servicios informáticos (incluidos servidores, almacenamiento, bases de datos, redes, *software*, análisis e inteligencia) a través de internet ("la nube"), cuyo objetivo es ofrecer una innovación más rápida, recursos flexibles y economías de escala. Lo habitual es pagar solo por los servicios utilizados en la nube, de tal forma que lo ayude a reducir los costos operativos, a ejecutar la infraestructura con más eficacia y a escalar a medida que cambian las necesidades de su negocio (Microsoft Azure, 2020). En la arquitectura que se utiliza en la nube para almacenar información, los datos residen sobre todo en servidores localizados en algún sitio de internet y la aplicación se ejecuta tanto en los servidores de la nube como en el navegador del usuario; por ejemplo, cuando se utiliza *Gmail*, *Google Maps*, servicios de *Yahoo* o muchos de los servicios de *eBay*5, se utiliza dicha arquitectura (Cabral, 2016). En comparación con los métodos de almacenamiento tradicionales, el almacenamiento en la nube plantea nuevos desafíos en seguridad de datos, confiabilidad y administración. Por lo tanto, los datos, al dejar de guardarse en un ordenador, pueden estar sujetos a riesgos ya que se deja de tener control sobre ellos. Los ciberdelincuentes no se centran ya en redes personales, sino atacan una nube y consiguen acceder a lo que guarda, obteniendo mucha más información de un solo golpe. Por eso, a pesar de las innumerables ventajas, una de las principales barreras en la adopción de este tipo de solución es la preocupación de sus usuarios con la privacidad de los datos almacenados de ellos, y

esta preocupación se vuelve aún más compleja cuando se externaliza el servicio, creando incertidumbre para los usuarios del contratista acerca de la privacidad de los datos sensibles de sus usuarios finales.

Actualmente se han realizado varias investigaciones previas acerca del tema en cuestión, entre ellas.

- Sun *et. al*. (2018) evaluaron un sistema de seguridad cuantificable para diferentes nubes a las que se puede acceder mediante una API6 consistente (Red Hat, 2020). Dicho sistema incluye un módulo de visualización, módulo de evaluación de seguridad, módulo de recuperación de la seguridad, modelo de escaneo de seguridad, modelo de administración de seguridad, motor de dase de datos de vulnerabilidades de seguridad y APIs consistentes para la seguridad en la nube. El modelo de evaluación de seguridad se compone de un conjunto de elementos que corresponden a diferentes campos, como informática, almacenamiento, red, mantenimiento, seguridad de aplicaciones.

  El proceso desarrollado se resume en tres partes:

- Colecciones de seguridad y artículos.
- Proceso de evaluación de seguridad cuantificable.
- Reparación de la vulnerabilidad de seguridad.

Lee *et. al*. (2017) parten de la visualización de la seguridad en la nube como servicio (SECaaS) 7. Proponen una mejora en las tecnologías de computación en la nube al igual que el paradigma SIEM8 tradicional, con la finalidad de cambiar a servicios de seguridad basados en la nube. La propuesta es una arquitectura SIEM que se pueda implementar en la plataforma SECaaS, la cual han estado desarrollando para analizar y reconocer la amenaza cibernética inteligente basada en tecnologías de virtualización (Viewnext, 2020). La arquitectura propuesta se resume en lo siguiente:

Un motor SIEM para procesar los datos recopilados, el almacenamiento SIEM para guardar los datos recopilados y los resultados del análisis, y la capa de usuario SIEM para garantizar el servicio de seguridad al usuario.

Jeyaraj (2018) se enfoca y explora los desafíos de seguridad que enfrentan las entidades en la nube; abarca entidades como el proveedor de servicios, propietario de los datos y usuario. Se enmarca en la cripto-nube, que constituye un acuerdo diferente de comunicación, computación y nivel de servicio, estudiando las causas y los efectos de varios ataques cibernéticos.

El objetivo de la presente investigación fue implementar un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube, con base en las normas ISO 27017 Y 27018. La hipótesis planteada en la investigación es: "El modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube mejorará el nivel de seguridad de la misma".

2. Metodología

La presente investigación puede clasificarse como cuasi-experimental debido a que se escoge la metodología que será utilizada para el diseño de nuevos controles de seguridad para almacenamiento en la nube. El diseño será transversal puesto que los resultados obtenidos en las pruebas realizadas con base en la muestra determinada serán comparados. Para realizar la comparación de los resultados obtenidos se utilizará la escala de Likert para cada uno de los indicadores.

Indicadores de variable independiente (Modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube)

Para la variable independiente, se consideraron los siguientes indicadores y escala de Likert que se muestra en el Cuadro 1:

Complejidad: elementos que dentro del diseño e implementación se relacionan entre sí, y cuyo comportamiento, propiedades no son evidentes a simple vista.

Facilidad de diseño e implementación: cualidad, condición característica que en el diseño e implementación no causa demasiada dificultad u obstáculo.

Tiempo de diseño e implementación: duración del diseño e implementación que determina épocas, períodos, horas, días, para esta investigación se lo medirá en días.

Recursos necesarios: medios o ayuda que se utiliza en la fase de diseño e implementación.

Cuadro 1
Escala de Likert para calificación
variable independiente

Complejidad	Facilidad de diseño e implementación	Tiempo de diseño e implementación (días)	Recursos necesarios	Código
Muy baja	Muy baja	1 a 5	3 a 5	5
Baja	Baja	6 a 10	6 a 8	4
Media	Media	11 a 15	9 a 11	3
Alta	Alta	16 a 20	12 a 14	2
Muy Alta	Muy Alta	>= 20	>=15	1

Fuente: elaboración propia [Autores]

Indicadores de variable dependiente (Seguridad de la información)

Para la variable dependiente, se consideraron los siguientes indicadores, los cuales serán analizados con Kali Linux y su aplicación Greenbone (analizador de vulnerabilidades) con base en la escala de Likert del Cuadro 2:

Número de vulnerabilidades: cantidad de debilidades encontradas en la plataforma de almacenamiento en la nube.

Número de riesgos mitigados: cantidad de eventos mitigados en la plataforma de almacenamiento en la nube.

Número de Logs: eventos o acciones que afectan a un proceso particular (evidencia del comportamiento del sistema). Posibles vulnerabilidades.

Cuadro 2
Escala de Likert para calificación
variable dependiente

Número de vulnerabilidades	Número de riesgos mitigados	Número de Logs	Código
<=10	<=2	<=9	5
11 a 20	3 a 4	10 a 19	4
21 a 30	5 a 6	20 a 29	3
31 a 40	7 a 8	30 a 39	2
> 40	> 8	>= 40	1

Fuente: elaboración propia [Autores]

Con el análisis previo realizado, para la comprobación de la hipótesis de investigación se dio los siguientes valores a la variable independiente X:

X = Modelo de seguridad
X1 = Mejora la seguridad
X2 = No mejora la seguridad

En los cuales se comprobó el impacto en relación a la variable dependiente que son el número de vulnerabilidades, riesgos mitigados y logs encontrados en el Prototipo I y Prototipo II.

Para la prueba de hipótesis planteada se utilizó la prueba de chi cuadrado o X2, que es una prueba no paramétrica a través de la cual se mide la relación entre la variable dependiente e independiente.

Además, se considera la hipótesis nula Ho y la hipótesis de investigación Hi.

Hi: *El modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube,* ***mejorará el nivel de seguridad*** *de la misma.*

Ho: *El modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube,* ***no mejorará el nivel de seguridad*** *de la misma.*

Para el cálculo de chi cuadrado, se muestra en el Cuadro 3, en la que se ubican las frecuencias observadas de cada Indicador.

Cuadro 3
Contingencia de frecuencias
observadas para X2

	Indicadores	Prototipo I	Prototipo II	TOTAL
MEJORA LA SEGURIDAD	Número de vulnerabilidades	5	0	5
	Número de riesgos mitigados	5	0	5
	Número de logs	5	0	5
NO MEJORA LA SEGURIDAD	Número de vulnerabilidades	0	1	1
	Número de riesgos mitigados	0	2	2
	Número de logs	0	2	2
	TOTAL	**15**	**5**	**20**

Fuente: elaboración propia [Autores]

Para las frecuencias esperadas se estableció los valores que se esperaría encontrar si las variables no estuvieran relacionadas. Chi cuadrado parte del supuesto de "no relación entre las ellas" y se evaluará si es cierto o no, analizando si sus frecuencias observadas son diferentes de lo que pudiera esperarse en caso de ausencia de correlación.

La frecuencia esperada de cada celda, se calcula mediante la siguiente fórmula aplicada a la tabla de frecuencias observadas.

$$fe = \frac{(total\_filas) * (total\_columnas)}{N}$$

Donde:

N: Número total de frecuencias observadas.

Aplicando la fórmula a los valores del Cuadro 3 se obtiene la tabla de contingencia de valores esperados, como se muestra en el Cuadro 4.

Cuadro 4
Contingencia de frecuencias esperadas para X2

	Indicadores	**Prototipo I**	**Prototipo II**	**TOTAL**
MEJORA LA SEGURIDAD	Número de vulnerabilidades	3,75	1,25	5
	Número de riesgos mitigados	3,75	1,25	5
	Número de logs	3,75	1,25	5
NO MEJORA LA SEGURIDAD	Número de vulnerabilidades	0,75	0,25	1
	Número de riesgos mitigados	1,50	0,50	2
	Número de logs	1,50	0,50	2
	TOTAL	**15**	**5**	**20**

Fuente: elaboración propia [Autores]

Una vez obtenida la tabla de frecuencias esperadas, se aplica la siguiente fórmula de chi cuadrado.

$$x^2 = \sum \frac{(o - E)^2}{E}$$

Donde:
O: Frecuencia observada en cada celda
E: Frecuencia esperada en cada celda

En el Cuadro 5 se muestra el cálculo del valor de X2, obteniendo un valor de 20.

Cuadro 5
Cálculo de X2

	Prototipos	**Indicadores**	**Obs**	**Esp**	**Obs-Esp**	**(Obs-Esp)2**	**(Obs-Esp)2/ Esperadas**
MEJORA LA SEGURIDAD	PI	Mejora/Número de vulnerabilidades Prototipo I	5	3,75	1,25	1,56	0,42
		Mejora/Número de riesgos mitigados Prototipo I	5	3,75	1,25	1,56	0,42
		Mejora/Número de logs Prototipo I	5	3,75	1,25	1,56	0,42
	PII	Mejora/Número de vulnerabilidades Prototipo II	0	1,25	-1,25	1,56	1,25
		Mejora/Número de riesgos mitigados Prototipo II	0	1,25	-1,25	1,56	1,25
		Mejora/Número de logs Prototipo II	0	1,25	-1,25	1,56	1,25
NO MEJORA LA	PI	No mejoras/Número de vulnerabilidades Prototipo I	0	0,75	-0,75	0,56	0,75

SEGURIDAD		No mejoras/Número de riesgos mitigados Prototipo I	0	1,50	-1,50	2,25	1,50
		No mejoras/Número de logs Prototipo I	0	1,50	-1,50	2,25	1,50
	PII	No mejoras/Número de vulnerabilidades Prototipo II	1	0,25	0,75	0,56	2,25
		No mejoras/Número de riesgos mitigados Prototipo II	2	0,50	1,50	2,25	4,50
		No mejoras/Número de logs Prototipo II	2	0,50	1,50	2,25	4,50
						TOTAL	**20,00**

Fuente: elaboración propia [Autores]

Alcance

El alcance de la investigación es correlacional, debido a que determina controles de seguridad para almacenamiento en la nube y podrá ser aplicado en cualquier institución que lo requiera para proteger la información almacenada en ella.

Población

Debido a la naturaleza de la investigación, se considera que la población es infinita, porque las pruebas realizadas con los prototipos se pueden ir generando indefinidamente en el tiempo. Las pruebas se realizarán a los servidores implementados; el primero, que incluye los controles de seguridad; el segundo, que no los considera, aplicado en los diferentes criterios establecidos, lo que permitirá determinar la validación del instrumento propuesto.

Unidad de análisis

La unidad de análisis fue las pruebas realizadas a los servidores implementados de almacenamiento en la nube.

Muestra

Para validar la implementación de los controles de seguridad establecidos se realizó pruebas en base a los criterios considerados para almacenamiento en la nube, los cuales determinarán si existe mejora o no.

Procedimientos

Se procede a realizar una búsqueda de información de estudios primarios acerca de la plataforma para almacenamiento en la nube más utilizados, como se muestra en el Cuadro 6.

Cuadro 6

Comparación de las herramientas para almacenamiento en la nube

	Nextcloud	Google Drive	Office 365	ownCloud	box	CITRIX	Dropbox
Licencia	Fuente abierta	Propietario	Propietario	Propietario	Propietario	Propietario	Propietario
Almacenamiento Ilimitado	✓	✓	✓	✓	Varía según el plan	✗	Varía según el plan
Soporte de archivos grandes	✓	✓	10GB	✓	5GB	10GB	20GB
Autohospedado / Local	✓	✗	✗	✓	✗	✓	✗
Clientes móviles							
Carga automática de imágenes / Video	✓	✓	✓	✓			
Clientes de escritorio							

Sincronización LAN	✗	✗	✗	✗	✗	✗	✓
Extensible con aplicaciones	✓	✗	✓	✓	✓	✗	✓
Integración de Outlook	✓	✓	✓	💵	💵	✓	✓
Búsqueda de texto completo	✓	💵	✓	✓	💵	✓	💵
Versionado de archivos	✓	Limitado	Limitado	✓	Limitado	✓	Limitado
Metadatos de archivo	✓	✓	✓	✓	💵	✓	💵
Ver PDF, imágenes, videos	✓	✓	✓	✓	✓	✓	✓
Chat integrado de audio / video / texto	✓	✓	✓	✗	✗	✓	✓
Calendario móvil / integración de contactos	✓	✓	✓	✓	✗	✗	✗
Oficina en línea en *web* / móvil	✓	✓	✓	✓ / ✗	✓	✓	✓
File drop (Carga de archivos del cliente)	✓	✓	✗	✓	✗	✓	✓
Bloquear descargas	✓	✓	✓	✗	✓	✓	✓
Verificación de videos	✓	✗	✗	✗	✗	✗	✗
Intercambio entre servidores	✓	✗	✗	✓	✗	✗	✗
Cifrado del lado del servidor	✓	✓	✓	✓	✗	✓	✗
Cifrado del lado del cliente	✓	✗	✗	✗	✗	✗	✗
Verificación de video	✓	✗	✗	✗	✗	✗	✗
Protección de pirateo de fuerza bruta	✓	✓	✓	✓	✗	✓	✓
Política de contraseña compatible con NIST	✓	✗	✓	✗	✓	✗	✗
Interfaz de usuario web asegurada con CSP 3.0	✓	✓	✗	✗	✗	✗	✗
Atributo de *cookie* del mismo sitio	✓	✓	✓	✓	✗	✓	✓
Control de acceso a archivos	✓	✗	✗	✓	✗	✗	✗
Derechos de acceso a la aplicación	✓	✓	✓	✗	✗	✗	✓

*Significado de Simbología:

Aplica

No Aplica

Pagado

Linux

Windows

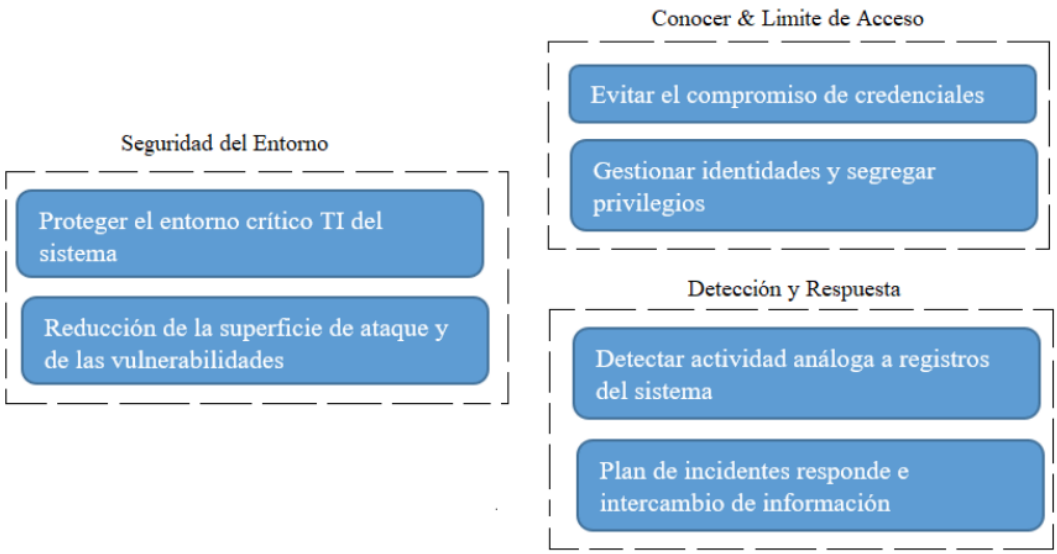
Apple

Android

Elaboración del Modelo de Seguridad

Se diseñó un modelo de seguridad que describe una serie de controles obligatorios o recomendados para la mitigación de vulnerabilidades en ambientes de almacenamiento en la nube, con base en las normas ISO 27017 y 27018. El modelo de seguridad se basó en los siguientes objetivos como se muestran en la Figura 1.

Figura 1
Objetivos generales del modelo de seguridad



Fuente: elaboración propia [Autores]

Estructura del modelo de seguridad

El modelo se basó en los siguientes controles de seguridad de la información:

Protección de la plataforma de virtualización. - Proteger la plataforma de virtualización y las máquinas virtuales (VMs) que hospedan los componentes relacionados con el almacenamiento en la nube al mismo nivel que los sistemas físicos.

Protección del entorno de almacenamiento en la nube. - Asegurar la protección de la infraestructura de almacenamiento en la nube de elementos del entorno de TI general y del entorno externo que se encuentren potencialmente comprometidos.

Protección contra *malware*. - Asegurar que la infraestructura de almacenamiento de la nube esté protegida en contra de *malware*.

Integridad de la base de datos. - Asegurar la integridad de los registros de la base de datos para el almacenamiento en la nube.

Monitor de integridad de archivos. - Detectar y prevenir actividad irregular en el sistema para contrarrestar una manipulación de los archivos o directorios monitorizados.

Planeación de respuesta a incidentes cibernéticos. - Asegurar un enfoque congruente y efectivo para la gestión de incidentes cibernéticos.

Pruebas de penetración. - Validar la configuración de seguridad operativa e identificar brechas de seguridad al realizar pruebas de penetración.

Política de contraseñas. - Asegurar que las contraseñas sean lo suficientemente resistentes contra ataques comunes a las mismas, al implementar y hacer valer una política de contraseñas efectiva.

Fortalecimiento del sistema. - Reducir la superficie de ciberataque de los componentes relacionados con el almacenamiento en la nube al realizar el fortalecimiento del sistema.

Autenticación de múltiples factores. - Prevenir que la amenaza que pudiera poner en compromiso un simple factor de autenticación permita el acceso a la plataforma de almacenamiento en la nube mediante la implementación de autenticación de múltiples factores.

Compromiso de las partes. - Protección de las partes a través de un contrato de servicio (cliente y proveedor del servicio) de acuerdo a la base legal de cada país y/o SLA del proveedor

Escenarios de prueba

Se establecieron los siguientes escenarios de prueba para el análisis de vulnerabilidades de almacenamiento en la nube con base en las normas ISO 27017 y 27018:

Escenario 1

Se utiliza el Prototipo I, que contempla las directrices propuestas para el modelo de seguridad en la nube.

Escenario 2

Se utiliza el Prototipo II, que no tiene o contempla las directrices propuestas de implementación del modelo de seguridad en la nube.

3. Resultados

De acuerdo al análisis de las diferentes plataformas de almacenamiento en la nube, se selecciona a NextCloud con base en las siguientes características frente a las demás.

Almacenamiento ilimitado	Oficina en línea en web / móvil
Soporte de archivos grandes	File drop (carga de archivos del cliente)
Autohospedado / local	Bloquear descargas
Clientes móviles	Verificación de video
Carga automática de imágenes / video	Intercambio entre servidores
Clientes de escritorio	Cifrado del lado del servidor
Sincronización LAN	Cifrado del lado del cliente
Extensible con aplicaciones	Verificación de video
Integración de Outlook	Protección de pirateo de fuerza bruta
Búsqueda de texto completo	Política de contraseña compatible con NIST
Versionado de archivos	Interfaz de usuario web asegurada con CSP 3.0
Metadatos de archivo	Con el atributo de cookie del mismo sitio
Ver Pdf, imágenes, video	Control de acceso a archivos
Chat integrado de audio / video / texto	Derechos de acceso a la aplicación
Calendario móvil / integración de contactos	

Con la plataforma de almacenamiento de la nube selecciona, los resultados que se obtuvieron en el Prototipo I, con el modelo de seguridad, y el Prototipo II, que no la considera son:

Indicadores de variable independiente

Los resultados de la variable independiente considerando la escala de Likert para los indicadores: complejidad, factibilidad de diseño e implementación, tiempo de diseño e implementación, recursos necesarios, se muestra en el Cuadro 7.

Cuadro 7
Evaluación Prototipo I y II respecto a la variable independiente

Nº	Modelo de Seguridad en ambientes de almacenamiento en la nube	Prototipo I				Prototipo II			
		Complejidad	Facilidad de diseño e implementación	Tiempo de diseño e implementación	Recursos necesarios	Complejidad	Facilidad de diseño e implementación	Tiempo de diseño e implementación	Recursos necesarios

1	Protección de la plataforma de virtualización	5	5	5	5	3	3	3	3
2	Protección del entorno de almacenamiento en la nube	4	4	4	4	1	1	2	3
3	Protección contra *malware*	5	5	5	5	3	3	4	3
3	Integridad de la base de datos	3	3	4	4	1	1	1	3
5	Monitor de integridad de archivos	4	4	5	5	3	3	3	4
6	Planeación de respuesta a incidentes cibernéticos	4	4	4	5	3	3	3	4
7	Pruebas de penetración	3	3	5	5	3	3	2	3
8	Política de contraseñas	5	5	5	5	3	3	4	3
9	Fortalecimiento del sistema	3	3	3	3	1	1	1	4
10	Autenticación de múltiples factores	5	5	5	5	3	3	4	3
11	Compromisos de las partes	4	4	3	4	2	2	3	4
TOTAL		**45**	**45**	**48**	**50**	**26**	**26**	**30**	**37**

Fuente: elaboración propia [Autores]

Interpretación de los indicadores (variable independiente)

Complejidad

El nivel de complejidad con relación a la variable del Prototipo I a la II es bajo. Puesto con un marco claro de controles de seguridad es más simplificado el diseño e implementación de la solución de almacenamiento en la nube.

Facilidad de diseño e implementación

La facilidad en el diseño e implementación con relación a la variable del Prototipo I a la II es poco, puesto el Prototipo I tiene pautas, directrices para el diseño e implementación mientras que en el Prototipo II tiene que analizar una estrategia para empezar el diseño e implementación.

Tiempo de diseño e implementación

El tiempo de diseño e implementación con relación a la variable del Prototipo I es poco a la del Prototipo II, puesto como se mencionó en el ítem anterior, el Prototipo II tiene que considerar una estrategia para empezar en el diseño e implementación requerido, lo que con lleva más esfuerzo y tiempo.

Recursos necesarios

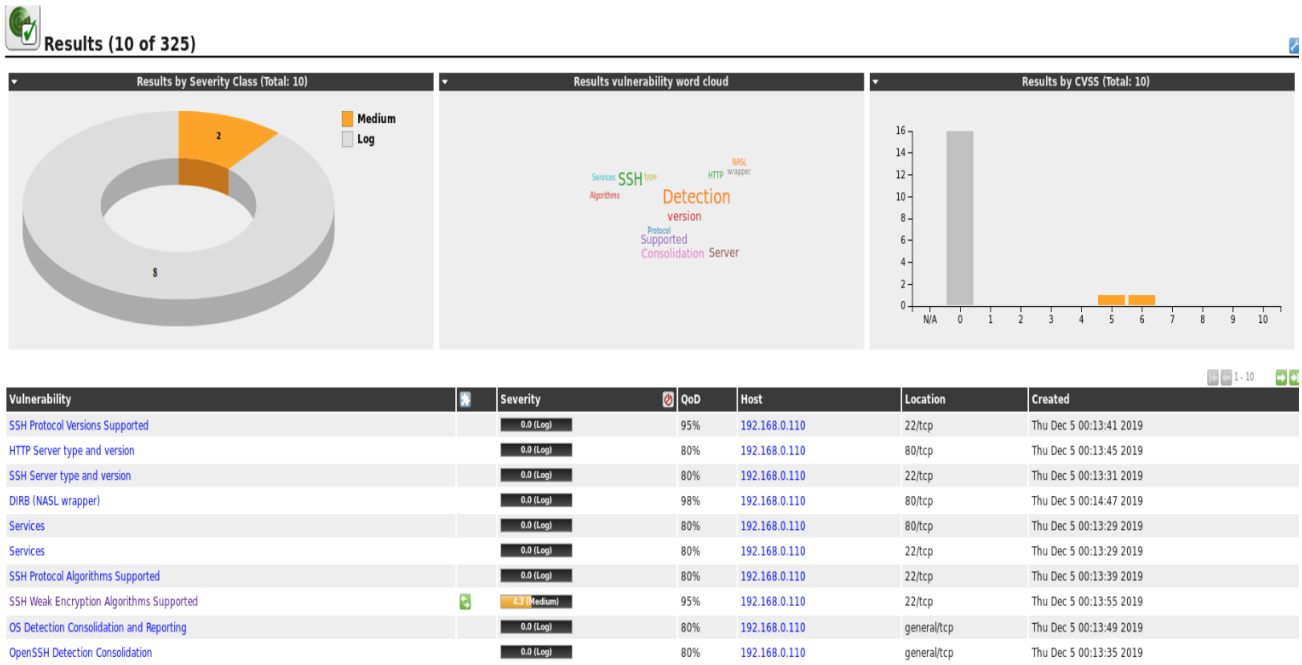
Los recursos necesarios con relación a la variable del Prototipo I son muy poco a la del Prototipo II, puesto al no estar claro las pautas y directrices a seguir en el Prototipo II se puede optar por escoger recursos que son inadecuados o en demasía.

Indicadores de variable dependiente

De acuerdo al análisis de Kali Linux y su aplicación Greenbone se obtuvieron las vulnerabilidades de red, conformadas por rutinas que comprueban la presencia de un problema de seguridad específico conocido o

potencial en el almacenamiento en la nube, como se muestran en la Figura 2 para el Prototipo I y la Figura 3 para el Prototipo II.

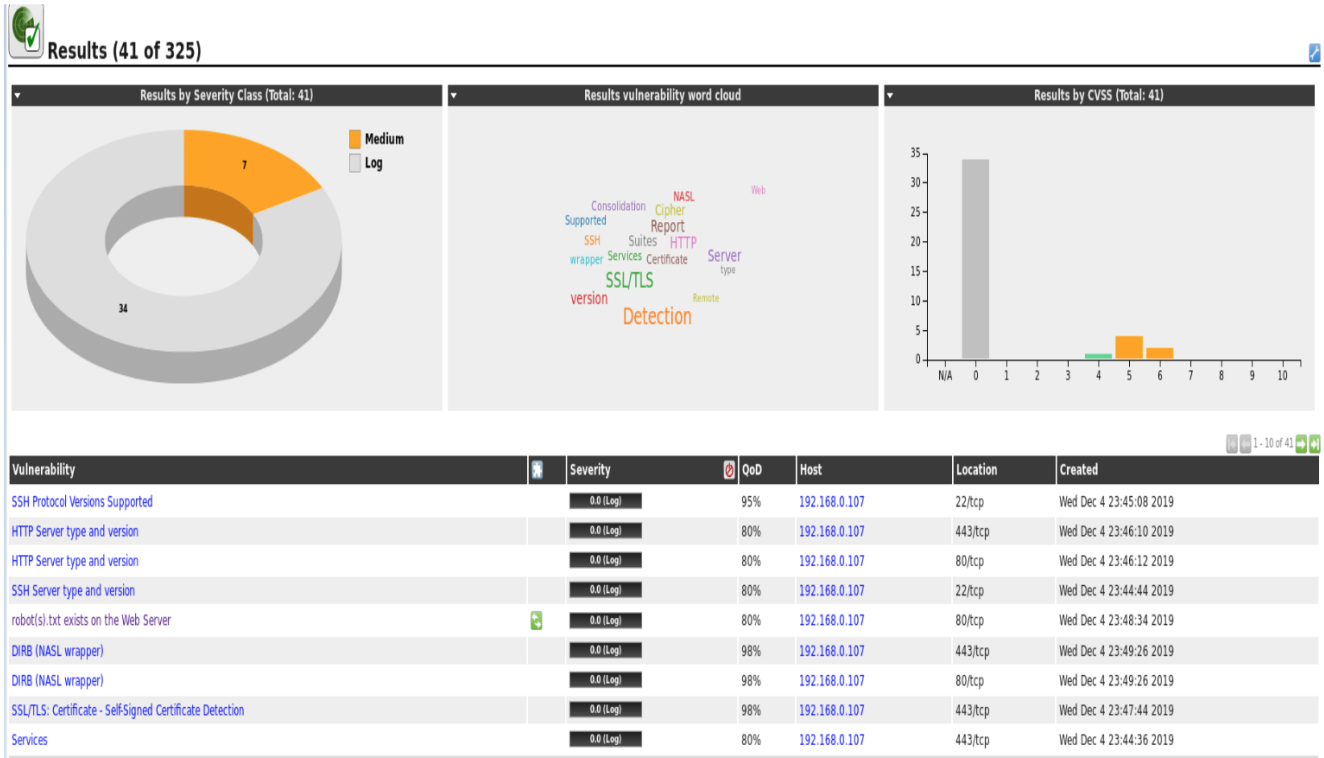
Figura 2
Análisis de vulnerabilidades por la herramienta Greenbone en el Prototipo I que considera el modelo de seguridad



Vulnerability	Severity	QoD	Host	Location	Created
SSH Protocol Versions Supported	0.0 (Log)	95%	192.168.0.110	22/tcp	Thu Dec 5 00:13:41 2019
HTTP Server type and version	0.0 (Log)	80%	192.168.0.110	80/tcp	Thu Dec 5 00:13:45 2019
SSH Server type and version	0.0 (Log)	80%	192.168.0.110	22/tcp	Thu Dec 5 00:13:31 2019
DIRB (NASL wrapper)	0.0 (Log)	98%	192.168.0.110	80/tcp	Thu Dec 5 00:14:47 2019
Services	0.0 (Log)	80%	192.168.0.110	80/tcp	Thu Dec 5 00:13:29 2019
Services	0.0 (Log)	80%	192.168.0.110	22/tcp	Thu Dec 5 00:13:29 2019
SSH Protocol Algorithms Supported	0.0 (Log)	80%	192.168.0.110	22/tcp	Thu Dec 5 00:13:39 2019
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.0.110	22/tcp	Thu Dec 5 00:13:55 2019
OS Detection Consolidation and Reporting	0.0 (Log)	80%	192.168.0.110	general/tcp	Thu Dec 5 00:13:49 2019
OpenSSH Detection Consolidation	0.0 (Log)	80%	192.168.0.110	general/tcp	Thu Dec 5 00:13:35 2019

Fuente: elaboración propia [Autores]

Figura 3
Análisis de vulnerabilidades por la herramienta Greenbone en el Prototipo II que no considera el modelo de seguridad



Vulnerability	Severity	QoD	Host	Location	Created
SSH Protocol Versions Supported	0.0 (Log)	95%	192.168.0.107	22/tcp	Wed Dec 4 23:45:08 2019
HTTP Server type and version	0.0 (Log)	80%	192.168.0.107	443/tcp	Wed Dec 4 23:46:10 2019
HTTP Server type and version	0.0 (Log)	80%	192.168.0.107	80/tcp	Wed Dec 4 23:46:12 2019
SSH Server type and version	0.0 (Log)	80%	192.168.0.107	22/tcp	Wed Dec 4 23:44:44 2019
robot(s).txt exists on the Web Server	0.0 (Log)	80%	192.168.0.107	80/tcp	Wed Dec 4 23:48:34 2019
DIRB (NASL wrapper)	0.0 (Log)	98%	192.168.0.107	443/tcp	Wed Dec 4 23:49:26 2019
DIRB (NASL wrapper)	0.0 (Log)	98%	192.168.0.107	80/tcp	Wed Dec 4 23:49:26 2019
SSL/TLS: Certificate - Self-Signed Certificate Detection	0.0 (Log)	98%	192.168.0.107	443/tcp	Wed Dec 4 23:47:44 2019
Services	0.0 (Log)	80%	192.168.0.107	443/tcp	Wed Dec 4 23:44:36 2019

Fuente: elaboración propia [Autores]

Los resultados de la variable dependiente se muestran el Cuadro 8:

Cuadro 8
Resultados después del análisis de vulnerabilidades

Indicadores	Prototipo I	Prototipo II

Número de vulnerabilidades	5	1
Número de riesgos mitigados	5	2
Número de logs	5	2
TOTAL	**15**	**5**

Fuente: elaboración propia [Autores]

Además, una vez definidos los valores esperados y obtenidos, se ha determinado que Chi cuadrado con 11 grados de libertad tiene un valor crítico de y con los resultados de la investigación se ha calculado un valor de 20, siendo significativo.

Los resultados obtenidos en la presente investigación, se compararon otros trabajos con el mismo enfoque, resaltando los siguientes aspectos:

Sun *et. al*. (2018) realiza una evaluación de un sistema de seguridad en la nube, mientras que en esta investigación se plantea un marco o estándar de controles de seguridad preventivos como correctivos para el almacenamiento en la nube.

Lee et. al. (2017) propone una arquitectura SIEM en la plataforma SECaaS, pero no contempla directrices para un diseño e implementación de seguridad en la nube, que esta investigación si lo considera.

Jeyaraj (2018), se enmarca en la cripto-nube observando causas y efectos de los ataques cibernéticos, en cambio esta investigación aparte de hacer este análisis dentro de sus controles le muestra la manera de como implementar una solución para protegerse.

4. Conclusiones

Considerando las normas ISO 27017 y 27018, se definieron once controles de seguridad para el almacenamiento en la nube: protección de la plataforma de virtualización, protección del entorno de almacenamiento en la nube, protección contra malware, integridad de la base de datos, monitor de integridad de archivos, planeación de respuesta a incidentes cibernéticos, pruebas de penetración, política de contraseñas, fortalecimiento del sistema, autenticación de múltiple factores, compromiso de las partes, que son parte íntegra del modelo de seguridad planteado y que ayudan en la mitigación de vulnerabilidades a las que se enfrenta la seguridad en la nube hoy en día.

El modelo de seguridad para almacenamiento en la nube implantado en el Prototipo I considerando los resultados de los indicadores de la variable dependiente se obtuvo un valor total de 15, que representa un 75% más seguro en comparación al Prototipo II que obtuvo un valor total de 5.

En la elaboración e implementación del modelo de seguridad para ambientes de almacenamiento en la nube, la principal tarea fue encaminada a los proveedores de servicios en la nube, puesto que son los responsables de garantizar que la organización esté protegida contra el acceso no autorizado, las violaciones de datos y otras amenazas.

Con las pruebas y análisis comparativo realizados a los prototipos planteados, se logra evidenciar que el modelo de seguridad elaborado e implantado ayuda a mejorar los niveles de seguridad de la nube y la mitigación de vulnerabilidades que, *a posteriori*, podrían convertirse en amenazas o riesgos para la organización o cliente que la utilice.

Se observa que una administración de seguridad de la información centralizada mejora el análisis y el filtrado del tráfico, agilizando el monitoreo de eventos de red y del sistema, importante para reducir las actualizaciones de *software* y políticas.

Con el apalancamiento, implantación y gestión de un modelo de seguridad para la nube, los usuarios podrán acceder de forma segura a sus datos y a las aplicaciones dentro de ella, sin importar dónde se encuentren o qué dispositivo utilicen, dándole así una ventaja competitiva para que las organizaciones operen a escala, reduzcan costos de tecnología y utilicen sistemas ágiles.

Las amenazas de seguridad evolucionan constantemente y se vuelven cada vez más sofisticadas; por esta razón, es fundamental que el departamento de tecnologías de la información sea cauteloso al momento de trasladar los sistemas de misión crítica a la nube. Con el proveedor que se contrate el servicio deberá estar en la capacidad de ofrecer la mejor seguridad de su clase y que se adapte a las necesidades o requerimientos de su organización.

Se recomienda que este modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube con base en las normas ISO 27017 y 27018, se tome como punto de partida para mejorar los niveles de seguridad y que se vaya actualizando y complementando, debido al constante crecimiento de amenazas.

Referencias bibliográficas

Aceves, M. (2016). *Security-as-a-Service La Destrucción de la Tiranía de los Appliances.* Recuperado de https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/CISO/Security-As-A-Service_CISO-Mty-Abr16.pdf

Cabral, B. (2016). *Consideraciones para el almacenamiento de archivos digitales en la nube informática en bibliotecas universitarias.* Recuperado de http://rev-ib.unam.mx/ib/index.php/ib/article/view/57909/51874

Gastón, L. (2017). *Qué es el almacenamiento en la nube.* Recuperado de https://www.bbva.com/es/que-es-el-almacenamiento-en-la-nube/

Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering (vol. 71, pp. 465-476). Alemania: Elsevier.

Cita en el texto (Jeyaraj, 2018, p 28-42)

Lee, J., Kim, Y., Kim, J., & Kim, I. (2017). Toward the SIEM architecture for cloud-based security services. Trabajo presentado en la Conferencia sobre Comunicaciones y Seguridad de Red. Las Vegas, NV, USA. Recuperado de https://ieeexplore.ieee.org/document/8228696

Microsoft Azure. (2020). *Qué es la informàtica en la nube.* Recuperado de https://azure.microsoft.com/es-es/overview/what-is-cloud-computing/

Red Hat. (2020). *Qué son las API y para qué sirven.* Obtenido de https://www.redhat.com/es/topics/api/what-are-application-programming-interfaces

Sun, A., Gao, G., Ji, T., & Tu, X. (2018). One Quantifiable Security Evaluation Model for Cloud Computing Platform. Trabajo presentado en la Sexta Coferencia Internacional sobre Nube Avanzada y Big Data . Lanzhou, China. Recuperado de https://ieeexplore.ieee.org/document/8530839

Viewnext (2020). *¿Qué es un SIEM?.* Recuperado de https://www.viewnext.com/que-es-un-siem/

---

1. Profesional orientado a la Seguridad Informática. Ecuador. Escuela Superior Politécnica de Chimborazo. Ingeniera en Sistemas Informáticos. bbesmeralda_89@hotmail.com

2. Profesor y profesional orientado a la Seguridad Informática. Ecuador. Universidad Nacional de Chimborazo. Ingeniero en Sistemas Informáticos. Magíster en Seguridad Telemática. pmendez@unach.edu.ec

3. Profesor y profesional orientado a la Seguridad Informática. Ecuador. Universidad Nacional de Chimborazo. Ingeniero en Sistemas Informáticos. Magíster en Seguridad Telemática. hvilla@unach.edu.ec

4. Profesional orientado a la Seguridad Informática. Ecuador. Universidad Nacional de Chimborazo. Ingeniero en Electrónica Telecomunicaciones y Redes. Magíster en Seguridad Telemática. diegomix07@hotmail.com

5. Es un sitio destinado a la subasta de productos a través de internet. Fundado en 1995, es uno de los pioneros en este tipo de transacciones. Desde 2002 *eBay* es propietario de *PayPal*. Desde 2015 su director ejecutivo (CEO) es Devin Wenig.

6. Una API es un conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar el *software* de las aplicaciones (Hace falta una referencia si no son conceptos muy conocidos).

7. Es un modelo de cómputo en la nube que entrega servicios administrados de seguridad a través de la internet. SECaaS está basado en el modelo SaaS, pero se limita a servicios especializados de seguridad de información (Hace falta una referencia si no son conceptos muy conocidos).

8. SIEM es un acrónimo que significa *Security Information and Event Mangement* y que se traduce como gestión de información y eventos de seguridad (Hace falta una referencia si no son conceptos muy conocidos).

Revista ESPACIOS. ISSN 0798 1015
Vol. 41 (Nº 17) Año 2020

[Índice]