ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD PARA MITIGACIÓN DE VULNERABILIDADES EN AMBIENTES DE ALMACENAMIENTO EN LA NUBE CON BASE EN LAS NORMAS ISO 27017 Y 27018

ESTHELA NATALY TENELEMA ARIAS

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA – ECUADOR

Septiembre – 2020

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

El Tribunal del PROYECTO DE INVESTIGACIÓN CERTIFICA QUE:

El trabajo de titulación titulado "IMPLEMENTACIÓN DE UN MODELO DE SEGURIDAD PARA MITIGACIÓN DE VULNERABILIDADES EN AMBIENTES DE ALMACENAMIENTO EN LA NUBE CON BASE EN LAS NORMAS ISO 27017 Y 27018", de responsabilidad de la Ing. Esthela Nataly Tenelema Arias, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Dr. Rodney Eduardo Mejía Garces; Mag. **PRESIDENTE DEL TRIBUNAL**	Rodney Eduardo Mejía Garces Firmado digitalmente por Rodney Eduardo Mejía Garces Fecha: 2020.09.30 16:59:48 -05'00'
Ing. Pablo Martí Méndez Naranjo Msc. **DIRECTOR**	
Ing. Henry Mauricio Villa Yánez Msc. **MIEMBRO**	
Ing. Diego Gustavo Caiza Méndez Msc. **MIEMBRO**	

Riobamba, septiembre 2020

DERECHOS INTELECTUALES

Yo, Esthela Nataly Tenelema Arias, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en **Trabajo de Titulación modalidad Proyectos de Investigación**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

ESTHELA NATALY TENELEMA ARIAS
No. Cédula: 020202187-9

DECLARACION DE AUTENTICIDAD

Yo, Esthela Nataly Tenelema Arias, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Proyecto de Investigación de Maestría.

Riobamba, julio 2020

ESTHELA NATALY TENELEMA ARIAS
No. Cédula: 020202187-9

DEDICATORIA

Dedico este trabajo principalmente a Dios, por ser mi sustento, refugio, y guía en momentos que estuve a punto de caer.

A mi hijo y esposo, que, con palabras, como “vamos mami”, “mi amor le apoyamos”, supieron enseñarme fortaleza, esmero, y lucha para cumplir los sueños y metas propuestas.

A mis padres que con sus consejos, valores y principios impartidos crearon en mí, una persona llena de fuerza y coraje para luchar por lo que queremos y no desmayar en el camino.

Esthela Tenelema

AGRADECIMIENTO

Agradezco a cada una de las personas que de una u otra manera supieron ser mi sustento, apoyo, y empuje. Agradezco a los docentes por los conocimientos impartidos y experiencia en las aulas de clases, y de manera muy especial al Director y los Miembros del Tribunal de tesis que han aportado significativamente en la elaboración de este trabajo.

Esthela Tenelema

TABLA DE CONTENIDO

RESUMEN **9**
ABSTRACT **10**

CAPÍTULO I
1. INTRODUCCIÓN **11**
1.1. Problema de investigación 11
1.1.1. Planteamiento del problema *11*
1.1.2. Formulación del problema *13*
1.1.3. Sistematización del problema *14*
1.2. Justificación de la investigación 14
1.2.1. Justificación teórica *14*
1.2.2. Justificación metodológica *15*
1.2.3. Justificación práctica *15*
1.3. Objetivos 16
1.3.1. Objetivo general *16*
1.3.2. Objetivos específicos *16*
1.4. Hipótesis 16
1.5. Estructura del proyecto de investigación 16

CAPÍTULO II
2. MARCO TEÓRICO **18**
2.1. Estado del arte 18
2.2. Almacenamiento en la nube 24
2.2.1. Antecedentes *24*
2.2.2. Tipos de almacenamiento en la nube *25*
2.2.3. Características de almacenamiento en la nube *26*
2.2.4. Ventajas y Desventajas *27*
2.2.5. Ciclo de vida de la seguridad de los datos *28*
2.3. Computación en la Nube 29
2.3.1. Antecedentes *29*
2.3.2. Características de la Computación en la Nube. *31*
2.3.3. Clasificación de la seguridad en la computación en la nube *32*
2.3.4. Riesgos a tomar en cuenta en la computación en la nube *37*
2.4. ISO 27017: Controles de Seguridad para Servicios Cloud 38

2.4.1. Antecedentes ... *38*
2.4.2. Importancia ... *40*
2.4.3. Nuevos Controles de seguridad en la ISO 27017 ... *41*
2.4.4. Beneficios ... *41*
2.5. ISO 27018: Requisitos para la protección de la información de identificación personal (PII) en sistemas Cloud ... 42
2.5.1. Antecedentes ... *42*
2.5.2. Importancia ... *43*
2.5.3. Controles de seguridad en la ISO 27018 ... *44*
2.5.4. Beneficios ... *45*
2.6. Modelo de Seguridad ... 46
2.6.1. Antecedentes ... *46*
2.6.2. Características ... *47*
2.7. Análisis de las principales vulnerabilidades ... 48
2.8. Determinación de la plataforma para almacenamiento en la nube ... 54

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN ... 59
3.1. Tipo de investigación ... 59
3.2. Diseño de la investigación ... 59
3.3. Métodos y técnicas ... 59
3.3.1. Métodos ... *60*
3.3.2. Técnicas ... *60*
3.4. Instrumentos ... 60
3.5. Validación de instrumentos ... 61
3.6. Elaboración del modelo de seguridad ... 62
3.6.1. Estructura del modelo de seguridad ... *62*
3.7. Implementación del modelo de seguridad ... 78
3.8. Definición de los escenarios de prueba ... 93
3.9. Hipótesis ... 93
3.9.1. Determinación de variables ... *93*
3.9.2. Operacionalización conceptual ... *94*
3.9.3. Operacionalización metodológica ... *94*

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN 96

4.1. Desarrollo de las pruebas 96

4.1.1. Indicadores de la variable independiente 96

4.1.2. Indicadores de la variable dependiente 101

4.1.3. Ponderación de indicadores 105

4.2. Comprobación de hipótesis 107

4.2.1. Estadística descriptiva 107

4.2.2. Estadística inferencial 109

CONCLUSIONES 114

RECOMENDACIONES 115

BIBLIOGRAFÍA

ANEXOS

LISTA DE TABLAS

Tabla 1-2 Colecciones de seguridad e ítems para la evaluación del modelo de seguridad (cuantificación) 20
Tabla 2-2 Comparación de la encuesta desde la perspectiva de tres niveles básicos con encuestas existentes. 23
Tabla 3-2 Ventajas y Desventajas de la Nube Pública 25
Tabla 4-2 Ventajas y Desventajas de la Nube Privada 26
Tabla 5-2 Ventajas y Desventajas de la Nube Hibrida 26
Tabla 6-2 Comparación de trabajos existentes basados en seguridad de datos y almacenamiento en la nube 34
Tabla 7-2 Vulnerabilidades de la Infraestructura Cloud 48
Tabla 8-2 Tabla comparativa entre plataformas para almacenamiento en la nube……...56
Tabla 1-3 Requerimientos del sistema - Nextcloud……..……...……..78
Tabla 2-3 Operacionalización conceptual……...…..94
Tabla 3-3 Operacionalización metodológica……..…..95
Tabla 1-4 Escala de calificación de la complejidad…….……..96
Tabla 2-4 Escala de calificación de facilidad de diseño e implementación…….….96
Tabla 3-4 Escala de calificación de tiempo de diseño e implementación (días)…….....97
Tabla 5-4 Escala de calificación recursos necesarios…….....97
Tabla 6-4 Evaluación Prototipo I y II respecto a la variable independiente…….98
Tabla 7-4 Resultados de los indicadores de la variable dependiente…….....104
Tabla 8-4 Tabla de escalas para el Indicador 1: Número de vulnerabilidades…….104
Tabla 9-4 Tabla de escalas para el Indicador 2: Número de riesgos mitigados…….104
Tabla 10-4 Tabla de escalas para el Indicador 3: Número de logs……104
Tabla 11-4 Códigos del Indicador 1: Número de vulnerabilidades……...105
Tabla 12-4 Códigos del Indicador 2: Número de riesgos mitigados…….106
Tabla 13-4 Códigos del Indicador 3: Número de logs…….....107
Tabla 14-4. Resultados de indicadores……108
Tabla 15-4 Tabla de contingencia de frecuencias observadas……110
Tabla 16-4 Tabla de contingencia de frecuencias esperadas…….111
Tabla 17-4 Cálculo de X2……....112
Tabla 18-4 Tabla de distribución de X2……113

LISTA DE FIGURAS

Figura 1-2 Sistema de evaluación de seguridad para la plataforma de computación en la nube 19
Figura 2-2 Arquitectura SIEM para el servicio basado en la nube 21
Figura 3-2 Flujo para el análisis de correlación utilizando minería de datos 22
Figura 4-2 Arquitectura de cripto-nube
……...223
Figura 1- 3 Objetivos generales del Modelo de Seguridad 62
Figura 2 -3 Diagrama base de la plataforma de almacenamiento en la nube 79
Figura 3 -3 Diagrama con el modelo de seguridad en la plataforma de almacenamiento en la nube 79
Figura 4 -3 Habilitación cifrado de disco VM 80
Figura 5-3 Solicitud de clave de cifrado de disco de la VM 80
Figura 6-3 Activación zona dmz a nivel del firewall 81
Figura 7-3 Mecanismo SELinux a nivel de la plataforma de almacenamiento en la nube 81
Figura 8-3 Configuración de snort para el análisis de vulnerabilidades 81
Figura 9 -3 Actualización de base de datos clamav 82
Figura 10-3 Ejecución en segundo plano del análisis de posibles virus 82
Figura 11-3 Script para respaldo de la base de datos 83
Figura 12-3 Ejecución en segundo plano de respaldo de la base de datos 83
Figura 13-3 Instalación de aide 83
Figura 14-3 Chequeo mediante aide a nivel del sistema operativo 84
Figura 15-3 Dos archivos añadidos y modificados que lo detecto aide 84
Figura 16-3 Inicio de sesión de Mantis Bug Tracker 85
Figura 17-3 Creación de un incidente en Mantis Bug Tracker 85
Figura 18-3 Seguimiento al incidente reportado en Mantis Bug Tracker 86
Figura 19-3 Identificación de IP (almacenamiento en la nube) 86
Figura 20-3 Análisis de vulnerabilidades con Metasploit 87
Figura 21-3 Directorios visibles y fáciles de vulnerar 87
Figura 22-3 Corrección del archivo de configuración 88
Figura 23-3 Nuevo análisis de vulnerabilidades 88
Figura 24-3 Habilitación de políticas de contraseñas en nextcloud 89
Figura 25-3 Instalación de Google Authenticator 89
Figura 26-3 Lectura de QR para los clientes OTP 90
Figura 27-3 Autenticación ssh mediante dos factores 90
Figura 28-3 Comando para convertir archivos en inmutables 90

Figura 29-3 Error al tratar de modificar un archivo inmutable 91
Figura 30-3 Inicio de sesión con el primer factor de autenticación 91
Figura 31-3 Inicio de sesión con el segundo factor de autenticación..... 92
Figura 32-3 Aplicación Terns of service..... 92
Figura 1-4 Reporte de análisis de vulnerabilidades Prototipo I 102
Figura 2-4 Reporte de análisis de vulnerabilidades Prototipo II 103
Figura 3-4 Curva de X2 113

LISTA DE GRÁFICOS

Gráfico 1-2 Prueba de vulnerabilidades en la nube.....49
Gráfico 2-2 Manejo de incidentes de seguridad en la nube 50
Gráfico 3-2 Encriptación de Datos y redes en la nube 50
Gráfico 4-2 Auditorias en la nube.....51
Gráfico 5-2 Administración de accesos de los usuarios en la nube 51
Gráfico 6-2 Lock-In / Dependencia de los productos de un Proveedor específico en la nube.....52
Gráfico 7-2 Aplicación de parches en la nube 52
Gráfico 8-2 Desarrollo de Aplicaciones en la nube 53
Gráfico 9-2 Almacenamiento de datos en la nube 53
Gráfico 1-4 Variable independiente en relación al Prototipo I 99
Gráfico 2-4 Variable independiente en relación al Prototipo II 99
Gráfico 3-4 Variable independiente en relación a los Prototipos I y II.....100
Gráfico 4-4 Análisis de vulnerabilidades por la herramienta Greenbone en el Prototipo I que considera el modelo de seguridad 101
Gráfico 5-4 Análisis de vulnerabilidades por la herramienta Greenbone en el Prototipo II que no considera el modelo de seguridad 102
Gráfico 6-4 Resultados obtenidos (de acuerdo a la escala) del Indicador 1: Número de vulnerabilidades 105
Gráfico 7-4 Resultados obtenidos (de acuerdo a la escala) del Indicador 2: Número de riesgos mitigados.....106
Gráfico 8-4 Resultados obtenidos (de acuerdo a la escala) del Indicador 3: Número de logs .107
Gráfico 9-4 Resultados totales de la comparación.....108

LISTA DE ANEXOS

ANEXO A: MATRIZ DE RIESGO PARA AMBIENTES DE ALMACENAMIENTO EN LA NUBE CON BASE EN LA ISO 27017 Y 27018.

ANEXO B: MODELO DE CONTRATO DE SERVICIO PARA EL ALMACENAMIENTO EN LA NUBE.

ANEXO C: HERRAMIENTA OPENVAS O GREENBONE PARA ANÁLISIS DE VULNERABILIDADES

ANEXO D: ESTRUCTURA O ESQUEMA DEL MODELO DE SEGURIDAD

RESUMEN

La presente investigación se plantea la implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube con base en las normas ISO 27017 y 27018, en el cual se analizó instituciones internacionales enmarcadas en la seguridad de la información que realizaron aportes importantes en exponer las vulnerabilidades más conocidas en la actualidad. Se analizó los controles expuestos en las normas ISO 27017 (Controles de Seguridad para Servicios Cloud) y 27018 (Requisitos para la protección de la información de identificación personal (PII) en sistemas Cloud). Con lo antes señalado se elaboró un modelo de seguridad basado en tres objetivos generales como: Seguridad del Entorno, Conocer & Limite de Acceso, Detección y Respuesta. El modelo de seguridad contempla una estructura como: información general del control, definición del control, guía de implementación; el mismo que se lo implementó en un prototipo de almacenamiento en la nube previamente seleccionado entre otros de su tipo. Se evaluó en dos escenarios, el primero con el prototipo que tiene implementado el modelo de seguridad y el segundo prototipo que no lo considera donde se estableció y ponderó los riesgos a presentarse enfocados a la confidencialidad, integridad, y disponibilidad de la información, estableciéndose los riesgos más críticos. Del estudio realizado se estableció un modelo con estrategias de seguridad desde la perspectiva de la construcción, operación y respuesta a incidentes de seguridad para aliviar los problemas comunes de almacenamiento en la nube; adicionalmente se redujo sustancialmente el promedio de ponderación de la probabilidad que los riesgos ocurran en un 75% frente a la situación que no la considere.

Palabras claves: <ALMACENAMIENTO EN LA NUBE>, < VULNERABILIDADES EN LA NUBE>, <MODELO DE SEGURIDAD>, < NORMA ISO 27017>, <NORMA ISO 27018>, <COMPUTACIÒN EN LA NUBE>.

ABSTRACT

This research proposes the implementation of a security model to mitigate vulnerabilities in the cloud storage environments, based on the ISO 27017 and 27018 standards. International institutions framed in information security that made essential contributions in exposing the most known vulnerabilities today were analyzed. The controls presented in the ISO 27017 (Security Controls for Cloud Services) and 27018 (Requirements for the protection of personally identifiable information (PII) in Cloud systems) were analyzed. With those as mentioned above, a security model was developed based on three general objectives, such as Environment Security, Know & Access Limit, Detection, and Response. The security model includes a structure being general control information, control definition, implementation guide, the same that was implemented in a prototype of cloud storage previously selected among others of its kind. It was evaluated in two scenarios, the first one with the prototype having the security model implemented, and the second one not considering it where the risks to be presented were established and weighed focused on the confidentiality, integrity, and availability of the information, determining the most critical threats. From the study carried out, a model was established with security strategies from the perspective of construction, operation, and response to security incidents to alleviate common cloud storage problems. Also, the average weighting of the probability that the risks occur was substantially reduced by 75% compared to the situation that does not consider it.

Keywords: <CLOUD STORAGE>, <VULNERABILITIES IN THE CLOUD>, <SECURITY MODEL>, <ISO 27017 STANDARD>, <ISO 27018 STANDARD>, <CLOUD COMPUTING>.

14-08-2020

0209-DBRAI-UPT-2020

CAPÍTULO I

1. INTRODUCCIÓN

En este Capítulo, se determina el enfoque u orientación general, identificación del problema, justificación, objetivos e hipótesis que se desea comprobar con el desarrollo de la investigación.

1.1. Problema de investigación

1.1.1. Planteamiento del problema

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)

El almacenamiento en la nube de la información ofrece reducciones de los consumidores en lo que respecta a los costes de inversión en la infraestructura de Tecnologías de la Información (TI) permitiendo entornos heterogéneos, que cooperan entre sí en tiempo real.

Con el fin de proporcionar servicios de almacenamiento de datos como el almacenamiento en la nube, se utiliza software para interconectar y facilitar la colaboración entre diferentes tipos de dispositivos de almacenamiento. En comparación con los métodos de almacenamiento tradicionales, 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; si no atacan una nube y consiguen acceder a lo que guarda, obteniendo mucha más información de un solo golpe. A pesar de 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.

Si bien la "nube pública" es el modelo de computación en nube con mayor presencia en América Latina, resulta fundamental contar con una red privada, pues minimiza la exposición ante amenazas externas. Las nubes públicas pueden ser gratuitas o basarse en el modelo de pago por consumo/uso, aunque conllevan varios riesgos, incluidos el entorno de múltiples arrendatarios donde el servidor host aloja máquinas virtuales de otras compañías, junto con costos ocultos y la incapacidad del usuario para controlar la redundancia y cuestiones con atacantes maliciosos, entre otras preocupaciones. (Aranda Software, 2018)

Para el 2020, se espera que la magnitud de almacenamiento en la nube por usuario ascienda a 1,7 gigabytes (GB) al mes, muy por encima de los 513 megabytes (MB) cada 30 días de 2015. Pues bien, en tres años, algo más de un tercio de la carga de este tráfico se deberá a los medios 2.0. En el presente, esta proporción es del 29%. Seis de cada diez internautas en el mundo, esto es, unos 2.300 millones de personas, recurrirán al cloud computing en los próximos cuatro ejercicios. La cifra ya era elevada en 2015 —1.300 millones—, pero no tanto. (MICÓ, 2017)

En el Ecuador no existen normativas específicas que rijan los servicios de Computing pero si existen lineamientos sustentados en la ley de Comercio Electrónico, firmas electrónicas y mensajes de texto, específicamente en el Título V "De las infracciones Informáticas", Capítulo I, en donde se estipulan artículos que aplican el uso de equipos informáticos y seguridades en los datos, los cuales son válidos y aplicables para el caso de los servicios de publicación , exposición y almacenamiento de información, brindadas por las tecnologías de Cloud Computing. (Ortíz et. al, 2016)

Es necesario establecer un modelo de seguridad para entender cuáles son las oportunidades y riesgos cuando se tiene la información en la nube.

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

- En la investigación realizada por Armstrong Nhlabatsi; Thein Thun; Niamul Khan; Yijun Yu; Arosha Bandara; Khaled Khan; Bashar Nuseibeh; Sebastian Hanigk (2014), denominada "Traceability for Adaptive Information Security in the Cloud", sostiene que uno de los requisitos previos para la seguridad de la información adaptativa es el uso de la trazabilidad como un medio para comprender la relación entre los requisitos de seguridad y las políticas de seguridad. Usando un ejemplo, motivamos la necesidad de mejorar la trazabilidad en el desarrollo de aplicaciones en la nube.
- En la investigación realizada por Amit Hendre; Karuna Pande Joshi (2015), denominada "A Semantic Approach to Cloud Security and Compliance", presenta un estudio para revisar las amenazas potenciales que enfrentan los consumidores de la nube y determinar los modelos

de cumplimiento y los controles de seguridad que deben implementarse para administrar el riesgo. Sobre la base de este estudio, se ha desarrollado una ontología que describe los controles de seguridad en la nube, las amenazas y los cumplimientos. También en el mismo estudio se desarrolla una aplicación que clasifica las amenazas de seguridad que enfrentan los usuarios de la nube y determina automáticamente controles de alto nivel de seguridad y cumplimiento de políticas que deben activarse para cada amenaza.

- La investigación realizada por Diao Zhe; Wang Qinghong; Su Naizheng; Zhang Yuhan (2017) denominada "Study on Data Security Policy Based on Cloud Storage", presenta una propuesta de seguridad de los datos del almacenamiento en la nube y formula la política de seguridad del almacenamiento en la nube correspondiente. Combina los resultados de la investigación académica existente mediante el análisis de los riesgos de seguridad de los datos del usuario en el almacenamiento en la nube y aborda un tema de la tecnología de seguridad relevante, que se basa en las características estructurales del sistema de almacenamiento en la nube.
- En la investigación realizada por Ling Li; Xiaoguang An (2018), denominada "Research on Storage Mechanism of Cloud Security Policy", se enfoca en la comparación y mejora del almacenamiento de políticas con el fin de cumplir los requisitos de almacenamiento de la política de seguridad en la nube. La tecnología de almacenamiento de políticas se refiere a una tecnología utilizada para realizar el almacenamiento de las políticas creadas por los usuarios y la información relevante de las políticas. El repositorio de políticas puede llevar a cabo la administración centralizada y el procesamiento de varias políticas y su información relevante. En la actualidad, los repositorios de políticas populares generalmente incluyen el almacenamiento de políticas para bases de datos relacionales o el almacenamiento de políticas para un servidor de directorios o un archivo en un formato fijo, como el formato de archivo XML (Extensible Markup Language).

Por lo mencionado anteriormente, se considera los servicios en la nube una parte esencial de muchas organizaciones; para lo cual se propone la implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube.

1.1.2. Formulación del problema

¿Cuál sería el nivel de mejora en la seguridad con la implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube con base en las normas ISO 27017 y 27018?

1.1.3. Sistematización del problema

- ¿Qué controles se deben analizar para la implementación de un modelo de seguridad de almacenamiento en la nube, considerando las normas ISO 27017 y 27018?
- ¿Cómo elaborar un modelo de seguridad para la mitigación de vulnerabilidades en ambientes de almacenamiento en la nube?
- ¿Cómo implementar el modelo de seguridad para la mitigación de vulnerabilidades en un ambiente de almacenamiento en la nube?
- ¿Qué resultados se obtendrán al implementar el modelo de seguridad en escenarios reales de almacenamiento de la nube?

1.2. Justificación de la investigación

1.2.1. Justificación teórica

En la presente investigación se plantea mejorar la seguridad de la información mediante la implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube.

El almacenamiento de la nube es un nuevo modelo de almacenamiento eficiente, esta característica permite que los datos y demás información estén siempre disponibles independientemente del equipo de trabajo, protegiendo de esta manera estos ante indisponibilidad de dichos equipos, así como proporcionando acceso a la información desde cualquier ubicación o dispositivo. (Diaz et. al, 2014)

La nube proporciona conveniente acceso a la red bajo demanda, es un centralizado conjunto de recursos informáticos configurables que se puede desplegar rápidamente con gran eficiencia y gastos de gestión mínimos. Su ventaja sin precedentes, permite un cambio de paradigma fundamental en cómo desplegar y entregar servicios informáticos, es decir posibilita la externalización informática, tal que tanto los individuos como las empresas puede evitar cometer grandes desembolsos de capital. Aunque los beneficios de la nube son grandes, la seguridad y la privacidad son las preocupaciones porque en la nube los proveedores de servicios (CSP) son administraciones separadas, entidades moviéndose en la nube pública comercial, priva a los usuarios del control directo sobre los sistemas que gestionan sus datos y aplicaciones. Todavía se enfrenta a la seguridad interna y externa, amenazas de privacidad, incluyendo fallas de medios, software, malware, errores de administrador, etc. (Evaluando Cloud, 2018)

Las normas que se utilizaran como base en el modelo de seguridad para almacenamiento en la nube son las Normas ISO/IEC 27017 y ISO/IEC 27018.

La Norma ISO/IEC 27017 trata de los Controles de Seguridad para Servicios Cloud, la misma que proporciona controles para proveedores y clientes de servicios en la nube. A diferencia de muchas otras normas relacionadas con la tecnología, la norma ISO 27017 aclara las funciones y las responsabilidades para ayudar a que los servicios en la nube sean tan seguros como el resto de los datos incluidos en un Sistema de Gestión de la Información certificado. (ISO Tools, 2017)

La Norma ISO/IEC 27018 trata de Tecnología de la Información - Código de Prácticas para la Protección de la Información de Identificación Personal (PII) en la nube en calidad de procesadores PII, el objetivo perseguido por la norma ISO 27018 es crear un conjunto de normas, procedimientos y controles mediante los que los proveedores de servicios en la nube que actúan como "procesadores de datos". Pueden garantizar el cumplimiento de las obligaciones legales en materia de tratamiento de los datos personales. Al mismo tiempo proporciona a los consumidores potenciales de servicios cloud una herramienta comparativa útil para ejercer su derecho de verificar y auditar los niveles de cumplimiento de las regulaciones establecidas por el proveedor. (ISO Tools, 2017)

ISO 27017 agrega un código de conducta de seguridad a la adquisición de servicios en la nube y la ISO 27018 es el primer estándar internacional que ofrece técnicas de seguridad en la privacidad y protección de la información personal identificable (PII).

1.2.2. Justificación metodológica

Mediante la implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube se pretende disminuir la probabilidad de sufrir incidentes de seguridad tales como la intromisión, robo de la información, y así incrementar los niveles de seguridad.

1.2.3. Justificación práctica

La demostración práctica de la investigación se efectuará en dos escenarios de prueba, en el primero con una solución de almacenamiento en la nube con la implementación de un modelo de seguridad para almacenamiento en la nube propuesta y el segundo con un escenario que no las considere.
Posteriormente se medirá entre los dos escenarios de prueba la efectividad de la implementación del modelo de seguridad de la información para almacenamiento en la nube.

1.3. Objetivos

1.3.1. Objetivo general

- 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.

1.3.2. Objetivos específicos

- Investigar los controles de seguridad para almacenamiento en la nube, considerando las normas ISO 27017 y 27018.
- Elaborar el modelo de seguridad para la mitigación de vulnerabilidades en ambientes de almacenamiento en la nube.
- Implementar el modelo de seguridad para la mitigación de vulnerabilidades en un ambiente de almacenamiento en la nube.
- Analizar los resultados que se obtendrán al implementar el modelo de seguridad en escenarios reales de almacenamiento de la nube.

1.4. Hipótesis

¿La implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube, mejorará el nivel de seguridad de la misma?

1.5. Estructura del proyecto de investigación

La estructura del proyecto de investigación se compone de lo siguiente:

- En el **CAPÍTULO I INTRODUCCIÓN.** Se determina el enfoque u orientación general, identificación del problema, justificación, objetivos e hipótesis que se desea comprobar con el desarrollo de la investigación.

- En el **CAPÍTULO II MARCO DE REFERENCIA.** Se recopilará definiciones de diferentes autores sobre conceptos referentes al almacenamiento en la nube, modelo de seguridad, norma ISO 27017 y 27018.

- En el **CAPÍTULO III DISEÑO DE INVESTIGACIÓN**. Se detalla el tipo de investigación, diseño, métodos, técnicas, instrumentos con su respectiva validación, adicionalmente se crea e implementa el modelo de seguridad con escenarios de pruebas en el cual que incluye el modelo de seguridad elaborado y el segundo el que no las considere.

- En el **CAPÍTULO IV RESULTADOS Y DISCUSIÓN**. Se desarrollan las pruebas en los escenarios establecidos, se analizan, comparan los resultados obtenidos y se comprueba la hipótesis planteada.

- En las **CONCLUSIONES** y **RECOMENDACIONES.** Se enuncian los resultados obtenidos y las sugerencias luego de realizar la investigación.

- En la **BIBLIOGRAFÍA.** Se enlistan las referencias utilizadas para el desarrollo de la investigación.

- En los **ANEXOS.** Se adjunta la información adicional utilizada.

CAPÍTULO II

2. MARCO TEÓRICO

En este Capítulo, se recopilará definiciones de diferentes autores sobre conceptos referentes al almacenamiento en la nube, norma ISO 27017 y 27018, modelo de seguridad,

2.1. Estado del arte

En la actualidad se está realizando investigaciones relacionadas con el tema en estudio, las cuales han aportado al presente trabajo de investigación para:

- Comprender de mejor manera la teoría relacionada con el almacenamiento en la nube y en si el concepto de "cloud computing".
- Identificar la descripción del problema y los objetivos planteados en las investigaciones realizadas.
- Conocer el proceso, metodología desarrollado o empeñado por los autores para realizar las investigaciones.
- Determinar las métricas, indicadores o parámetros que los autores utilizan para realizar las pruebas.
- Determinar el aporte que realizan los autores en las investigaciones realizadas.
- Observar los resultados y conclusiones obtenidas en base a las pruebas realizadas que hacen los autores.

Entre las principales investigaciones, se mencionan:

Investigación: "One Quantifiable Security Evaluation Model for Cloud Computing Platform" (Sun, Gao, Ji, & Tu, 2018)

La motivación de los autores del artículo científico nace de la evaluación de un sistema de seguridad cuantificable para diferentes nubes a las que se puede acceder mediante una API consistente. El sistema de evaluación incluye un motor de exploración de seguridad, un motor de recuperación de seguridad, un modelo de evaluación cuantificable de seguridad, un módulo de visualización, etc. El modelo de evaluación de seguridad se compone de un conjunto de elementos de evaluación que corresponden a diferentes campos, como informática, almacenamiento, red, mantenimiento, seguridad de aplicaciones. y etc.

El proceso desarrollado se resume en lo siguiente:

- Se crea una seguridad cuantificable en el sistema de evaluación para plataforma única o cruzada en la nube.
- Se realiza la evaluación cuantificable de seguridad que incluye seguridad en el módulo de visualización, base de datos de vulnerabilidades de seguridad, motor de escaneo de seguridad, motor de recuperación, evaluación de seguridad modelo, módulo de establecimiento de modelo y mantenimiento de modelo.

El sistema en mención se muestra en la Figura 1-2.

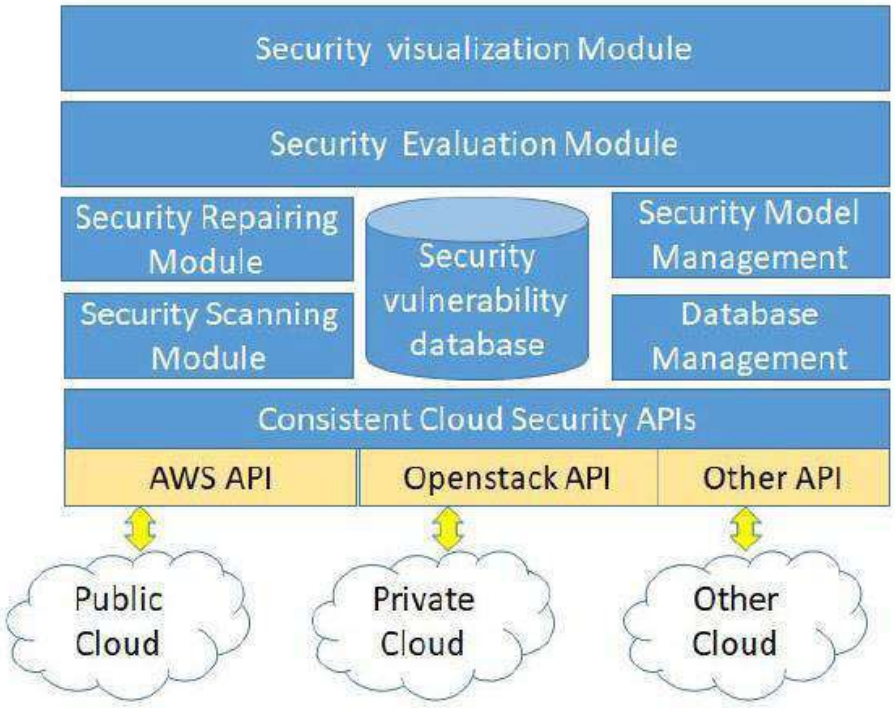


Figura 1-2 Sistema de evaluación de seguridad para la plataforma de computación en la nube

Fuente: Sun, Gao, Ji, & Tu, 2018

En la evaluación del modelo de seguridad se reúne una colección compuesta por campos de seguridad como P = $\{P_1, P_2, P_3, P_4, ..., P_N\}$. P_i es una de las colecciones de seguridad informática, colección de seguridad de almacenamiento, colección de seguridad de red, colección de mantenimiento de seguridad, colección de seguridad de aplicaciones y etc. Un P_i de P incluye diferentes elementos de control de seguridad de P_{ij}, como SO de servidor físico, sistema operativo VM, sistemas de contenedores y otros artículos de vulnerabilidad, y todos los elementos que componen P_i como se muestra en la Tabla 1-2.

$$P_i = \{P_{i1}, P_{i2}, P_{i3}, P_{i4}, ..., P_{iM}\}$$

Tabla 1-2 Colecciones de seguridad e ítems para la evaluación del modelo de seguridad (cuantificación)

INDEX	COLLECTION NAME	MAIN ITEMS	INDICADOR
P_1	Computing Security Collection	Physical (Host) Machine OS	P_{11}
		Virtual Machine OS	P_{12}
		Container System	P_{13}
		Other devices (GPU, FPGA, etc.)	P_{14}
P_2	Storage Security Collection	Storage Physical Machines	P_{21}
		Storage of Virtual Machines	P_{22}
		Object Storage	P_{23}
		Block Storage	P_{24}
		File Storage	P_{25}
P_3	Network Security Collection	Network Configure	P_{31}
		Network logs	P_{32}
		Network Device	P_{33}
P_4	Maintain Security Collection	Maintain Plan	P_{41}
		Management Architecture	P_{42}
		Running Safety Inspection	P_{43}
P_5	Application Security Collection	Application System Logs	P_{51}
		Behavior Audit	P_{52}
		Access Control Strategy	P_{53}

Fuente: Sun, Gao, Ji, & Tu, 2018

La vista de seguridad en la nube es el puntaje de seguridad real de todo tipo de verificar elementos para la vista de recursos en la nube del usuario. Los el administrador puede adquirir la vista de seguridad global correspondiente a la nube total.

Sin embargo, la investigación realizada no presenta una guía a seguir en la búsqueda de mejorar seguridad en cualquier nube; ya que su enfoque es en un sistema de evaluación de seguridad cuantificable para entorno de nube única o multi-nube con API consistente y privilegio de acceso del sistema operativo en la nube.

Investigación: "Toward the SIEM architecture for cloud-based security services" (Lee, Kim, Kim, & Kim, 2017)

La motivación de los autores del artículo científico parte de la visualización de la seguridad en la nube como servicio (SECaaS). Se propone una mejora en las tecnologías de computación en la nube, al igual que el paradigma SIEM (Security Information and Event Management) 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 misma que ha estado desarrollando para analizar y reconocer la amenaza cibernética inteligente basada en tecnologías de virtualización.

La arquitectura propuesta se resume en lo siguiente:

La arquitectura SIEM diseñada consiste principalmente en 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 como se muestra en la Figura 2-2.

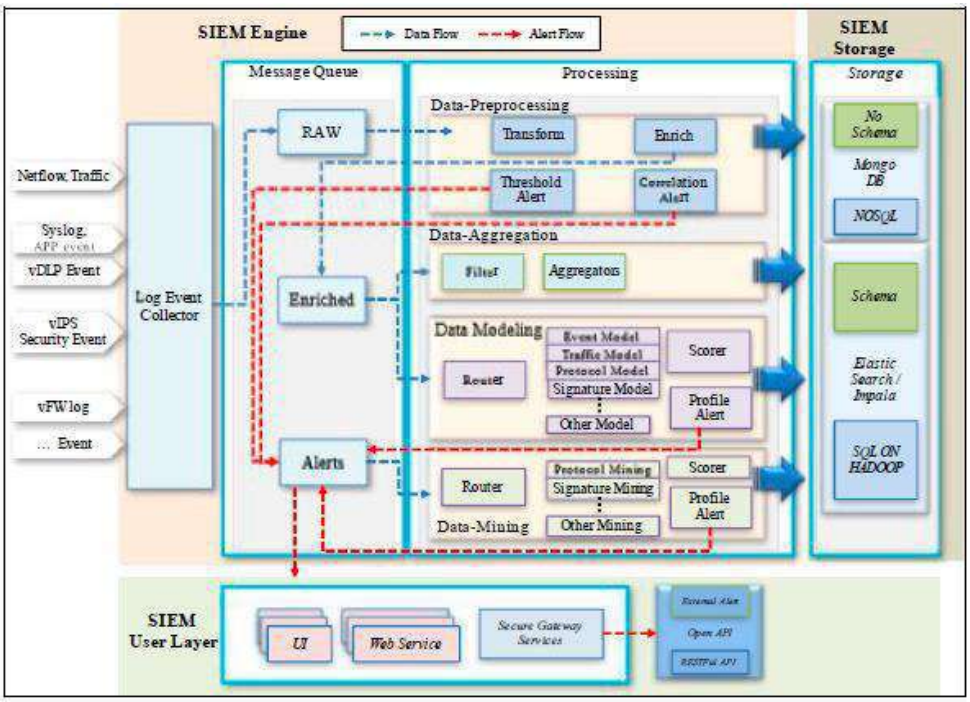


Figura 2-2 Arquitectura SIEM para el servicio basado en la nube

Fuente: Lee, Kim, Kim, & Kim, 2017

El motor SIEM tiene como objetivo apoyar en el análisis inteligente de amenazas y salida de datos relevantes basados en sus diversos procesamientos de datos, tales como modelado de datos y minería de datos. Para el Servicio SECaaS, la capa de usuario SIEM es la encargada en el soporte de respuesta a incidentes, actividades de una gran variedad de fuentes. Para ello, es necesario que el Administrador de identificadores de datos en SIEM puede identificar cada evento y registro de seguridad separado por cada inquilino basado en la nube de servicios de seguridad. El motor SIEM incluye principalmente el análisis de series de tiempo y el análisis de correlación para proporcionar un servicio SIEM basado en la nube, como se explica en la Figura 3-2.

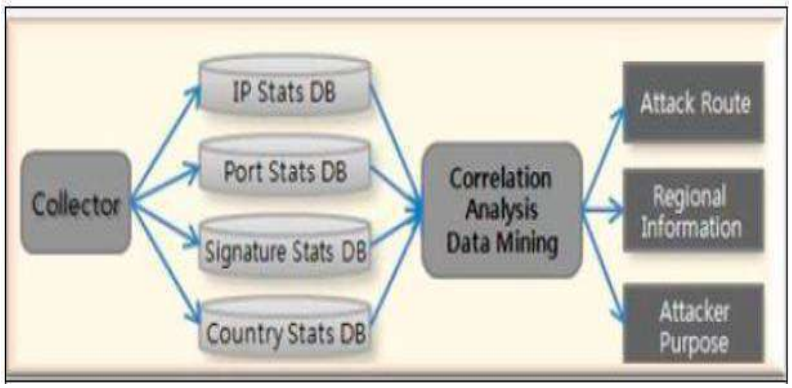


Figura 3-2 Flujo para el análisis de correlación utilizando minería de datos

Fuente: Lee, Kim, Kim, & Kim, 2017

Se concluye que la presente propuesta utiliza una analítica de correlación misma que es la más importante de los diversos métodos analíticos, por lo cual en el presente estudio se maneja Redes Neuronales para detectar la amenaza basada en el aprendizaje del modelo de seguridad de datos en la nube.

Sin embargo, la investigación planteada en este artículo científico tiene un alto nivel de utilización de redes neurológicas, modelos matemáticas, y técnicas algorítmicas, lo cual es complejo de entender sin una mayor preparación en el área.

Investigación: "Recent security challenges in cloud computing" (Andrews Jeyaraj, 2018)

La motivación de los autores del artículo científico se enfoca y explora los desafíos de seguridad que enfrentan las entidades en la nube. Abarca entidades como el proveedor de servicios en la nube, propietario de los datos y usuario de la nube. 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.

La arquitectura crypto-cloud se resume en lo siguiente:

La arquitectura de una cripto-nube propuesta consta de tres entidades básicas: la autoridad de datos (el propietario de los datos), el consumidor de los datos y el proveedor de servicios de almacenamiento en la nube (CSSP).

Su proceso inicia cuando la autoridad de datos carga los archivos cifrados y el consumidor o usuario de la nube ha autenticado el acceso a los archivos, después de estas condiciones se cumplan, el archivo solicitado se puede descargar y descifrar utilizando tokens y credenciales apropiadas. Estas entidades antes descritas enfrentan diferentes desafíos de seguridad en los niveles de comunicación, computación y acuerdos de nivel de servicio (SLA). A continuación, se presenta la arquitectura de una cripto-nube en la Figura 5-2.

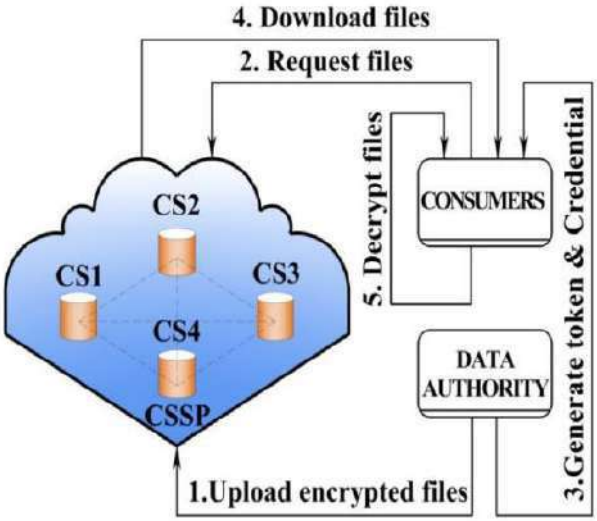


Figura 4-2 Arquitectura de cripto-nube

Fuente: Jeyaraj, 2018

En la Tabla 2-2 se muestra una comparación de la encuesta realizada por el autor de este artículo científico en tres niveles básicos de la seguridad en la nube con encuestas similares; en la que se muestra que solo unos pocos artículos han realizado una encuesta sobre la causa raíz y el efecto de los problemas a nivel computacional específicamente a nivel de máquina virtual, nivel de hipervisor y nivel de hardware. Hay una necesidad imperiosa de una exploración más grande e intensiva en el nivel SLA en este tema.

Tabla 2-2 Comparación de la encuesta desde la perspectiva de tres niveles básicos con encuestas existentes.

S. NO	AUTHOR	COMMUNICATION LEVEL		COMPUTATIONAL/FUNCTIONAL LEVEL				SLA LEVEL
		NETWORK LEVEL	APPLICATION LEVEL	VIRTUALIZATION			DATA SECURITY	
				V.M level	Hypervisor level	Hardware level		
1	Ali, 2015	X		X	X		X	X
2	Rong, 2013						X	X
3	Zissis, 2012		X	X		X	X	
4	Sun, 2011	X	X				X	
5	Sahzad, 2014	X					X	X
6	Ran, 2015	X					X	
7	Soofi, 2014	X	X				X	
8	Warhade, 2014	X	X				X	
9	Padhy, 2011	X	X	X			X	X

10	Denz, 2013			X	X	X		
11	Ouedraogo, 2015			X	X		X	X
12	Rawat, 2014					X	X	
13	Our survey	X	X	X	X	X	X	X

Fuente: Jeyaraj, 2018

Se concluye que existe una gran necesidad de abordar los problemas relacionados con la seguridad en la comunicación, la computación y el acuerdo de nivel de servicio de computación en la nube ya que los desafíos de seguridad son numerosos, lo que proporciona varias oportunidades para que los piratas informáticos rompan un cripto-sistema.

La investigación planteada como bien menciona anteriormente, solo da pautas y sugerencias de seguridad en la nube, y pone hincapié que se debe profundizar más a detalle en la seguridad de computación en la nube.

2.2. Almacenamiento en la nube

2.2.1. Antecedentes

Desde que se creó Internet, las personas han tenido más información a su alcance de la que nunca habían tenido antes en toda la historia. Al hacer cada día más cosas directamente en Internet, en lo que se conoce como la "nube", y guardar los datos en ella en vez de hacerlo en los dispositivos se está generando un gran contenido de datos útiles para los negocios. Y, por otro lado, se están requiriendo almacenamientos en la nube cada vez más potentes. (Marquina, 2017)

Del inglés cloud storage, el almacenamiento en la nube es un servicio que nos permite guardar, de forma segura, todo tipo de datos, documentos o archivos en servidores online que son administrados normalmente por un proveedor de servicio. Esto es lo mismo que decir que estamos "contratando" un espacio privado de la red donde almacenamos nuestra información. Y contratar no siempre es sinónimo de pagar por ello, ya que la mayoría de plataformas de almacenamiento disponen de versiones gratuitas, eso sí, con un límite de espacio.

El almacenamiento en la nube es un modelo de informática en la nube que almacena datos en Internet a través de un proveedor de informática en la nube que administra y opera el almacenamiento en la nube como un servicio. Se obtiene bajo demanda con capacidad y costo oportunos, y elimina la necesidad de tener que comprar y administrar su propia infraestructura de

almacenamiento de datos. Esto le otorga agilidad, escala global y durabilidad con acceso a los datos en cualquier momento y lugar. (AWS, 2020)

2.2.2. Tipos de almacenamiento en la nube

Existen varios tipos de almacenamiento en la nube siendo 3 de ellos los más comunes.

2.2.2.a Nube pública

La nube pública se trata de un servicio en la nube que requiere poco control administrativo y que se puede acceder en línea por cualquier persona que esté autorizada. El almacenamiento en la nube pública utiliza un mismo conjunto de hardware para hacer el almacenamiento de la información de varias personas, con medidas de seguridad y espacios virtuales para que cada usuario puede ver únicamente la información que le corresponde.

Tabla 3-2 Ventajas y Desventajas de la Nube Pública

VENTAJAS	INCONVENIENTES
• Escalabilidad • Ahorro de tiempo y costes • Mayor eficiencia de los recursos	• La infraestructura es compartida • Hay poca transparencia para el cliente de cloud ya que no se sabe el resto de recursos que se puede estar compartiendo

Fuente: Tenelema Esthela, 2019

Este servicio es alojado externamente, y se puede acceder mediante Internet, y es el que usualmente una persona individual puede acceder, por su bajo costo y el bajo requerimiento de mantenimiento. (Castro, 2019)

2.2.2.b Nube privada

La nube privada funciona exactamente como el nombre sugiere. Un sistema de este tipo está diseñado específicamente para cubrir las necesidades de una persona o empresa. Este tipo de almacenamiento en la nube puede ser presentado en dos formatos: on-premise (en la misma oficina o casa) y alojado externamente. Este modelo es más usado por empresas, no tanto así las personas individuales.

Tabla 4-2 Ventajas y Desventajas de la Nube Privada

VENTAJAS	INCONVENIENTES
• Cumple con las políticas internas, ofreciendo mayor seguridad que la pública • Control total de los recursos	• Elevado coste • Dependencia de la infraestructura contratada.

Fuente: Tenelema Esthela, 2019

En este modelo la empresa tiene el control administrativo, y por lo tanto le es posible diseñar y operar el sistema de acuerdo a sus necesidades específicas.

2.2.2.c Nube híbrida

La nube híbrida es el tercero de los principales tipos de almacenamiento en la nube. Ofrecen, como su nombre sugiere, una combinación de almacenamiento en nubes públicas y privadas, de tal forma que le es posible a los usuarios el personalizar las funciones y las aplicaciones que se adaptan mejor a sus necesidades, así como los recursos que se utilizan.

Tabla 5-2 Ventajas y Desventajas de la Nube Hibrida

VENTAJAS	INCONVENIENTES
• Maximiza el valor al utilizar recursos privados y compartidos • Reducción de costes	• Riesgo al combinar dos modelos de implementación diferente • Control de la seguridad entre ambas nubes.

Fuente: Tenelema Esthela, 2019

La nube híbrida es particularmente valiosa para cargas de trabajo dinámicas altamente cambiantes. Un ejemplo típico es que se configure de tal forma que los datos más importantes se almacenen en un sistema de almacenamiento en la nube privada, mientras que los datos menos importantes se pueden almacenar en una nube pública con acceso disponible por una gran cantidad de personas a distancia. (Castro, 2019)

2.2.3. Características de almacenamiento en la nube

- Mejora los recursos tecnológicos.
- Los costos se reducen.
- Acceso a los documentos casi a tiempo real, sin necesidad de cargas de alta duración.
- Permite compartir recursos con independencia del dispositivo y la ubicación.
- Se optimiza su uso de manera automática.
- La seguridad es igual o mejor que otros sistemas convencionales.

- No requiere instalación ni mantenimiento ya que cada usuario accede desde diferentes lugares.

2.2.4. Ventajas y Desventajas

Las ventajas del almacenamiento en la nube se describen a continuación:

- Se integra con facilidad y rapidez con el resto de las aplicaciones empresariales.
- Se prestan servicios a nivel mundial proporcionando mayor capacidad, copias de seguridad y la reducción al mínimo de los tiempos de inactividad.
- Requiere una mínima inversión e infraestructura ya que solo es necesario contar con una plataforma en la nube y no hay que instalar ningún software.
- Se actualiza automáticamente.
- La aplicación elegida suele estar disponible para trabajar en horas o días.
- Favorece el uso eficiente de energía.

Adicional existe mecanismos o técnicas como ventaja para el almacenamiento en la nube como:

- Cifrado de información: información que almacena en la nube se puede codificar previamente o después de enviarla. Existe un alcance de seguridad de almacenamiento distribuido como Single Sign-On (SSO), Multi-Factor Autenticación (MFA) y eso es solo el comienzo. Esto implica que su información debe ser obtenida por lo general de una población que necesita una independencia en caso que su dispositivo es robado y así su seguridad está totalmente garantizada y no tenga que enfatizar que su información sea robada o vendida.
- Vale la pena tener una copia de seguridad: guardar su información en un servidor es extremadamente inseguro.

  Independientemente de si se desea utilizar el almacenamiento distribuido como su almacenamiento esencial en un framework, esto puede funcionar como un lugar para almacenar segundos duplicados de documentos en caso de que alguna vez requiera un traslado de la información.
- Aseguramiento contra los hackers: guardando la información en un marco de la nube brinda seguridad incluida de hackers y desgracias informativas. En la posibilidad de que un servidor se bloquea, la información en este momento será puesta de forma segura lejos en diferentes áreas. Esto en conjunto disminuye el peligro de desgracia de información. El marco

proporciona garantías incluidas de los programadores y desgracia de información. (Dhamdhere, 2018)

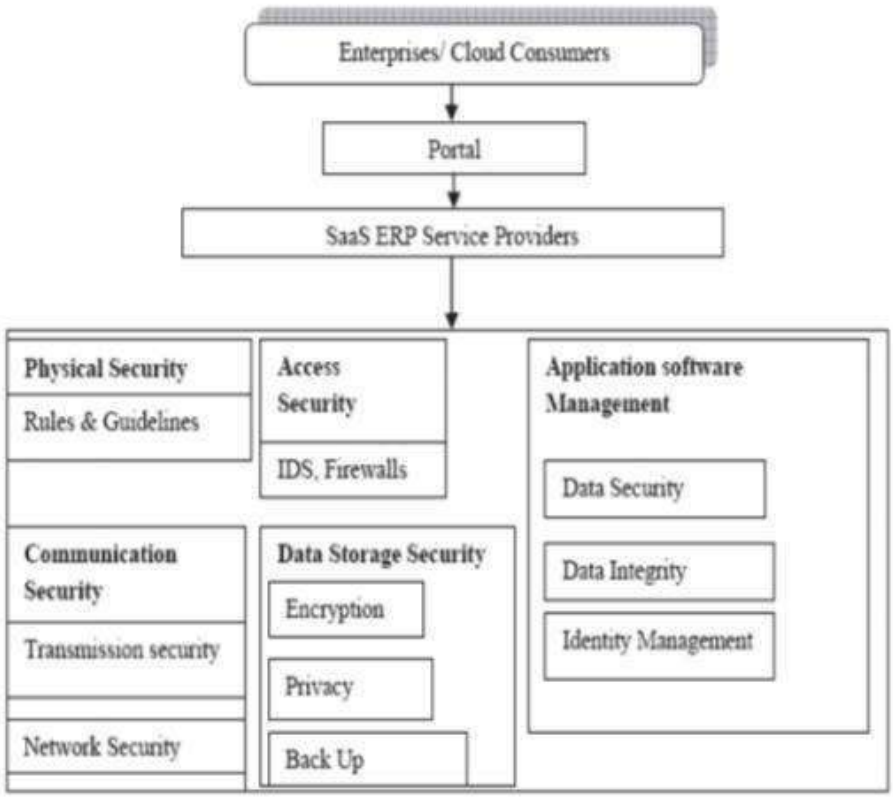


Figura 5-2 Marco de seguridad para el sistema empresarial basado en la nube

Fuente: Markandey, 2018

Las desventajas del almacenamiento en la nube se describen a continuación:

- Se necesita acceso a Internet.
- Existe cierta dependencia de los proveedores de este tipo de servicio confiando en su tecnología y funcionamiento.
- Se modifican continuamente las interfaces de las aplicaciones.
- Posible sobrecarga en los servidores si el número de usuarios es muy alto o no se sigue una política de uso adecuada.

2.2.5. Ciclo de vida de la seguridad de los datos

El ciclo de vida de los datos es necesario para comprender y gestionar la información en la entidad, dicha gestión incluye los procesos y políticas del cómo se usa la información y cómo se gobierna su uso. (MINTIC, 2016)

Figura 6-2 Ciclo de vida de seguridad de los datos

Fuente: MINTIC, 2016

El ciclo de vida tiene seis fases, desde la creación hasta la destrucción; su progreso se ve lineal pero no necesariamente pasan por todas las etapas después de su creación.

Creación: Creación es la reproducción de un nuevo contenido digital, o la alteración, actualización o modificación de contenido existente.

Almacenamiento: Proceso de ubicar los datos digitales en algún tipo de repositorio de almacenamiento y normalmente ocurre de forma prácticamente simultánea a su creación.

Uso: Los datos son visualizados, procesados, o utilizados de otro modo en algún tipo de actividad, no incluyendo su modificación.

Compartir: La información se hace accesible a otros, tales como otros usuarios, clientes, y colaboradores.

Archivado: Los datos dejan de ser usados activamente y entran en un almacenamiento de largo plazo. **Destrucción:** Los datos son destruidos de forma permanente usando medios físicos o digitales

2.3. Computación en la Nube

2.3.1. Antecedentes

La computación en la nube o informática en la nube, proviene del inglés “Cloud computing” es un arquetipo que permite el acceso a un grupo compartido de recursos informáticos para los usuarios de la nube bajo demanda a través de una red de ordenadores.

Cloud computing es un modelo tecnológico que busca desplazar a los servidores físicos y utilizar servidores virtuales mediante la nube y servicios dedicados al almacenamiento de información y aplicaciones que el usuario utiliza diariamente para el desarrollo de sus labores. Por lo que podemos decir que es el conjunto "infinito" de servidores de información desplegados a lo largo del todo mundo en centros de datos (Data Centers), donde se almacenan millones de aplicaciones Web (Web Apps) y enormes cantidades de datos (Big Data) a disposición de miles de organizaciones, empresas y cientos de miles de usuarios, los cuales se descargan y ejecutan directamente los programas y aplicaciones de software almacenados en dichos servidores tales como Google, Amazon, IBM o Microsoft. (Dhamdhere, 2018)

Como se ilustra en la Figura 6-2, la computación en la nube ha pasado de ser un elemento marginal a uno fundamental de las operaciones de TI. (Aisha Javed, 2017)

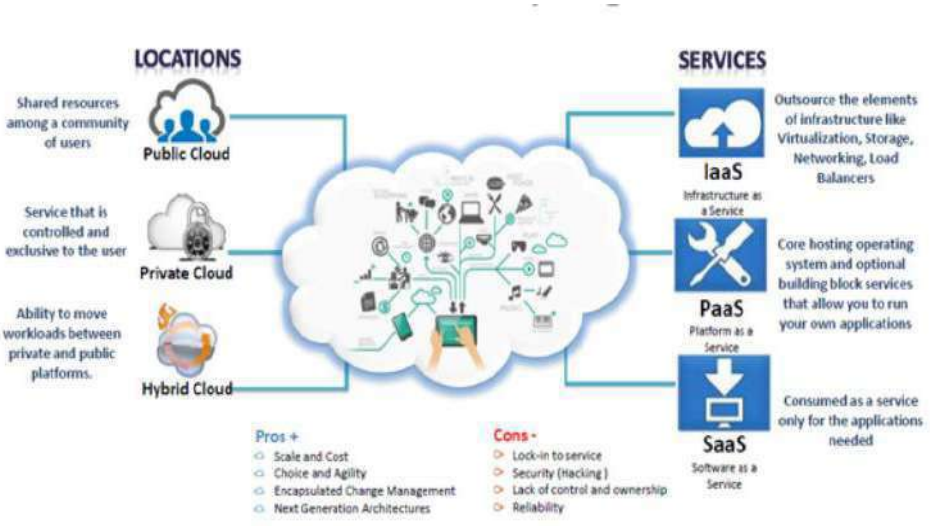


Figura 7-2 Cloud Computing

Fuente: Aisha Javed, 2017

Además, las soluciones de cloud computing disponibles en el mercado se dividen atendiendo a tres dimensiones o aristas:

- Familias (modelos de servicio): Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS) y Business Process as a Service (BPaaS).
- Formas de implementación (formas de integración y explotación): cloud público, cloud privado, cloud híbrido.
- Agentes intervinientes en el negocio: habilitador, proveedor, intermediario, suscriptor y auditor. (Aisha, 2017)

2.3.2. Características de la Computación en la Nube.

Las principales características de computación en la nube son:

1. Pago por uso: el cliente debe pagar en función del uso que realiza del servicio cloud contratado sabiendo que son unos costos bajos, en comparativa a los costos tradicionales por aplicación y dispositivos de almacenamiento. Además, nos permite utilizar un servicio de prueba antes de realizar la adquisición del servicio.
2. Abstracción: consiste en aislar los recursos informáticos contratados al proveedor de servicios cloud de los equipos informáticos del cliente, por lo que el mantenimiento de la infraestructura, actualización de sistemas, pruebas y demás tareas asociadas es trabajo del proveedor del servicio contratado.
3. Agilidad en la escalabilidad: consiste en aumentar o disminuir las funcionalidades ofrecidas al cliente y con ello el coste del servicio asociado, en función de las necesidades del negocio y de los usuarios, sin necesidad de nuevos contratos ni penalizaciones.
4. Multiusuario: permite a varios usuarios compartir los medios y recursos informáticos, permitiendo la optimización de su uso.
5. Autoservicio bajo demanda: permite al usuario acceder de manera flexible a las capacidades de computación, tales como el almacenamiento en servidores y redes, en la nube de forma automática y a medida que las vaya requiriendo, sin necesidad de una interacción humana.
6. Acceso sin restricciones: permite a los usuarios de acceder a los servicios contratados de cloud computing en cualquier lugar, en cualquier momento y con cualquier dispositivo que disponga de conexión a redes de servicio IP, tales como teléfonos móviles, dispositivos PDA u ordenadores portátiles.
7. Agrupación de recursos: los recursos informáticos del proveedor se agrupan para prestar servicios a diversos clientes utilizando un modelo de múltiples usuarios, con diferentes recursos físicos y virtuales asignados y reasignados de manera dinámica según la demanda. Generalmente, el cliente no tiene control o conocimiento de la ubicación exacta de los recursos proporcionados.
8. Elasticidad rápida: los recursos se asignan y liberan rápidamente, muchas veces de manera automática, lo que da al usuario la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.

Figura 8-2 Características de Computación en la Nube

Fuente: Valdez, 2015

2.3.3. Clasificación de la seguridad en la computación en la nube

Como se muestra en la Figura 9-2, el problema de seguridad de datos en Cloud Computing puede clasificarse.

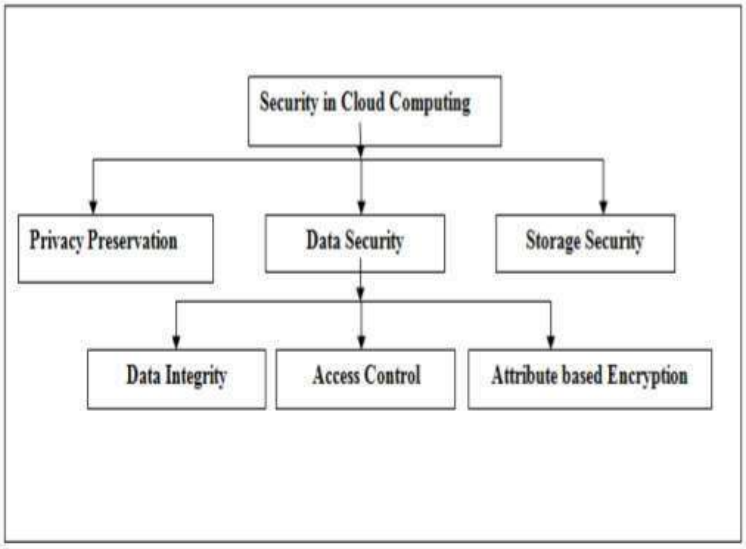


Figura 9-2 Clasificación de seguridad en la nube

Fuente: Rajeswari & R. Kalaiselvi, 2017

La seguridad de los datos se clasifica en tres diferentes categorías:

• La preservación de la privacidad define que la privacidad de la información personal e importante en la nube es crucial ya que los servidores en la nube no son confiables. La

confidencialidad y la autorización son principales requisitos de preservación de la privacidad en la nube.

• Seguridad en el almacenamiento define que el almacenamiento en la nube es la tarea de proporcionar integridad a los datos compartidos almacenados en servidores en la nube fiables.

• Seguridad de datos define que los datos o la seguridad de la información es el proceso de proteger los datos de usuarios no autorizados, reviniendo alteraciones y restringiendo el acceso de información sensible.

Sobre la seguridad de datos en la nube se tiene tres características importantes:

• Integridad de los datos: comúnmente está garantizada por validaciones utilizando herramientas criptográficas como resúmenes de mensajes, hash y digital firma etc.

• Control de acceso (AC): un control de acceso del sistema incluye componentes y métodos para especificar políticas de control de acceso para legítimas usuarios.

• Cifrado basado en atributos (ABE): el los datos cargados se cifran con ABE que define la política de acceso en los atributos relacionados con los datos. Por lo tanto, solo los usuarios autorizados con los atributos coincidentes pueden descifrar y acceder los datos. (Kalaiselvi, 2017)

Un estudio comparativo que se muestra a continuación en la Tabla 6-2, revela un esquema propuesto, de los servicios, la privacidad, confidencialidad, integridad, control de acceso y almacenamiento de 21 trabajos en papel de diferentes autores.

Tabla 6-2 Comparación de trabajos existentes basados en seguridad de datos y almacenamiento en la nube

AUTHOR	METHOD	SERVICE	PRIVACY	CONFIDENCIALITY	INTEGRITY	ACCESS CONTROL	STORAGE SECURITY
Younis A. Younis et al	Cloud computing using Access Control Architecture	Security access permission for multiple services	No	No	No	Yes	No
Varsha D Mali et al	User Authentication and Access Control Techniques in Cloud Computing	Cryptographic RBAC	Yes	Yes	No	Yes	No
Jun Li et al	Fine-grained Data Access Control Systems with User Accountability	ABE	No	No	No	Yes	No
Guoyuan Lin et al	Trust Based AC Policy	Trust Management, role-based access control	No	No	No	Yes	No

Yan Zhu et al	Temporal Acess Control	Temporal access control Encryption, proxy-based re-encryption	No	Yes	No	Yes	No
Saravana Kumar et al	Enhanced ABE	ABE using digitalasignature and asymmetric encryption	No	Yes	Yes	Yes	No
Shulan Wang et al	An Efficent File Hierarchy ABE Seheme	ABE using Integrated access structure	No	Yes	No	Yes	No
Shulan Wang et al	Attribute-Based Data Sharing Seheme	Two-party key issuing protocol, weighted	No	Yes	No	Yes	No
Tram Viet Xuan Phuong et al	Hidden Ciphertext Policy	ABE using hiddent access policy	No	Yes	No	Yes	No
Entao Luo et al	Hierarchical Multi-Authority and ABE Friend Discovery Scheme	ABE usuaing multi-authority friend discovery schemes	No	No	No	Yes	No

Nedhal A. et al	Data Integrity Verification Scheme	Mobile Multiple cloud Data integrity Verification	No	No	Yes	Yes	No
Alata Mohammed Hameed Al-Saffar et al	Identity Based technique	Data integrity and Confidentiality in the multiple cloud environment	No	Yes	Yes	No	No
Edoardo Gaetani et al	Block chain-based Database to Ensure Data Integrity	Integrity verification using Block chain database	No	No	Yes	No	No
L. Malina et al	Privacy preserving security solution	Non bilinear group signature scheme	Yes	Yes	Yes	Yes	No
Haralambos Mouratidisa et al	A framework to support selection of cloud providers	Modelling language and selection of CSP	Yes	No	No	Yes	No
Ulrich Greveler et al	Cloud Computing with a System that Preservers Privacy	Trust model prevents CSP from accessing outsourced data	Yes	No	Yes	Yes	No

Lifei Wei et al	Security and privacy for storage and computation	Discouragement of Privacy cheating and auditing oof secure computation	Yes	No	Yes	Yes	Yes
Yan Zhu et al	Cooperative Provable Data Possession for Integrity Verification	Hommomorphic verifiable response anda hash index hierarchy	No	No	Yes	Yes	Yes
Quian Wang et alAuditing anda Data Dynamics for Storage Security	Auditing anda Data Dynamics for Storage Security	verify the integrity of the dynamic in the cloud	No	No	Yes	Yes	Yes
Kan Yang et al	Secure Dynamic	privacy-preserving	Yes	No	Yes	Yes	Yes

Fuente: S. Rajeswari & R. Kalaiselvi, 2017

2.3.4. Riesgos a tomar en cuenta en la computación en la nube

Tanto si se contrata en la nube un servidor de correo, un servidor web, un CRM o un servicio de almacenamiento como si se decide contratar capacidad de proceso para instalar sus propias aplicaciones, se tiene que trasladar la seguridad que se exige a las instalaciones locales, a la nube.

La Figura 11-2. Muestra algunas estrategias para mitigar los riesgos que en mayoría van de estar regulados por el contrato y los acuerdos de servicio o ANS.

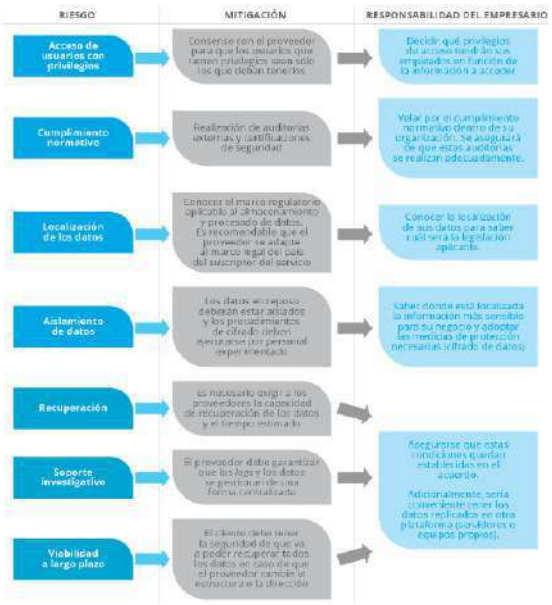


Figura 10-2 Riesgo-Mitigación Computación en la Nube

Fuente: Incibe,2018

2.4. ISO 27017: Controles de Seguridad para Servicios Cloud

2.4.1. Antecedentes

La norma ISO 27017: 2015 proporciona orientación tanto a los proveedores de servicios en la nube como a los consumidores de estos servicios en forma de objetivos, controles y pautas. Basado en la especificación de control de seguridad ISO 27002

- Se agrega información para los clientes y proveedores de servicios en la nube.
- Es un conjunto de control extendidos para computación en la nube:
  - Control y coordinación de gestión adicionales debido a la división de responsabilidad de seguridad
  - Control de riesgos debido a instalaciones compartidas cuando se usa la computación en la nube

- Impacto en los usuarios finales de la organización del cliente si utilizan servicios de computación en la nube
- Pruebas de aceptación para los servicios prestados y para actualizaciones / nuevas versiones
- Manejo de código móvil
- Métodos de autenticación para el uso del servicio en la nube
- Controles a nivel de aplicación que incluyen validación de datos de entrada / salida, integridad de mensajes
- Requisito de auditoría

El código de conducta de ISO/IEC 27017:2015 se diseñó para que las organizaciones lo usen como referencia para seleccionar controles de seguridad de la información de servicios en la nube cuando se implementa un sistema de administración de seguridad de la información en la nube basado en ISO/IEC 27002:2013. También lo pueden usar los proveedores de servicios en la nube como guía para implementar controles de protección comúnmente aceptados.

Esta norma internacional proporciona pautas adicionales de implementación específica de la nube basadas en ISO/IEC 27002, y ofrece controles adicionales para abordar las amenazas y los riesgos de seguridad de la información específicos de la nube relativos a las cláusulas 5 a 18 de ISO/IEC 27002: 2013 para los controles, instrucciones de implementación y otra información.

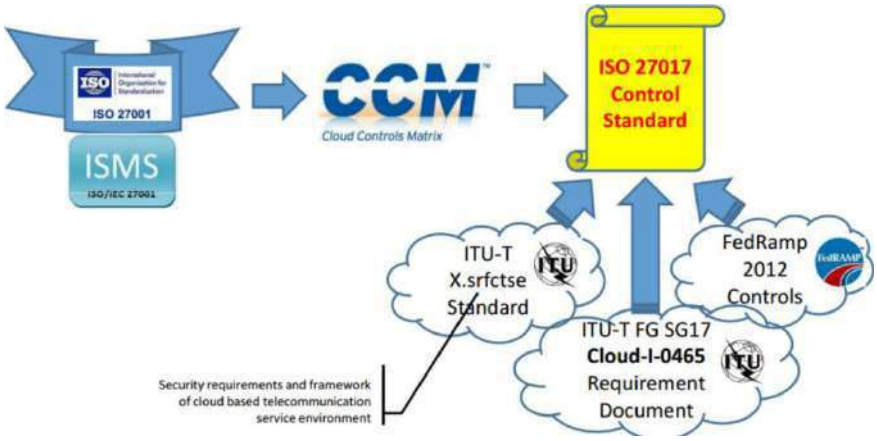


Figura 11-2 Controles de Métricas en la Nube

Fuente: **Sigea,2019**

2.4.2. Importancia

La norma internacional ISO/IEC 27017, relativa a la seguridad de los servicios cloud, es un código de conducta coherente con la norma ISO 27002. Es un complemento a esta última norma y establece buenas prácticas de seguridad en el marco de los servicios cloud.

La norma ISO 27017 no solo se enmarca en los proveedores de servicios cloud, sino también en la seguridad del conjunto de estos servicios; de hecho, también se tiene en cuenta el punto de vista del cliente. Estas exigencias adicionales permiten alinear las relaciones entre el cliente y el proveedor de servicios cloud.

Es un compendio de buenas prácticas en el que se incluyen recomendaciones para mejorar la seguridad del servicio, y no de un sistema de referencia de conformidad.

Estas recomendaciones se pueden integrar fácilmente en un sistema de gestión certificado ISO 27001. Los auditores de certificación si pueden incluir en las próximas auditorias de seguimiento una inspección del cumplimiento de estas buenas prácticas. De este modo, se cuenta con una evaluación independiente de la implementación de estos estándares de seguridad en los procedimientos.

Esta norma ayuda a que todos los datos que el cliente necesite para estar seguro de su protección frente a posibles riesgos. En el caso de proveedores de servicios cloud, estos deben proporcionar información a los clientes sobre la arquitectura, la tecnología utilizada, las medidas de seguridad adoptadas y las funcionalidades disponibles, así también sobre el contexto de uso (por ejemplo, la tecnología de cifrado utilizada o la localización geográfica de los centros de datos).

El proveedor también debe establecer el lugar que ocupa el cliente en estos procedimientos operativos y en la gestión de modificaciones, actualizaciones o incidentes. De manera general, la norma incide en la importancia de definir claramente el papel y las responsabilidades del cliente y del proveedor en materia de seguridad.

En el caso de los clientes de las empresas de cloud, la lectura de la norma les permite identificar los puntos más relevantes y le guía a la hora de elegir a sus partners. Los CIO (Chief Information Officer) quieren mayor flexibilidad y poder recurrir al proveedor más adecuado según el caso. Así pues, el suministro de los servicios informáticos evoluciona de forma natural desde un modelo en cadena hacia un modelo en red. La multiplicación de las relaciones comerciales y técnicas lleva aparejada una nueva complejidad que tenemos que aprender a gestionar.

La norma ISO 27017 permite estandarizar las relaciones entre los clientes y los proveedores de servicios cloud mediante un modelo de análisis e intercambio común, facilitando así la gestión. Las empresas que se ajustan a la norma ISO 27017, permiten que los usuarios de sus servicios disfruten de unas mejores garantías de seguridad. (OPENEXPO EUROPE, 2019)

2.4.3. Nuevos Controles de seguridad en la ISO 27017

Como se mencionó antes la ISO 27017 se basa sobre 37 de los controles de la ISO / IEC 27002, pero también presenta siete nuevos controles:

- Roles y responsabilidades compartidos en un entorno informático en la nube
- Eliminación y devolución de los activos del cliente del servicio en la nube tras la terminación del contrato
- Protección y separación del entorno virtual del cliente del de otros clientes
- Requisitos de fortalecimiento de las máquinas virtuales para satisfacer los requisitos del negocio
- Procedimientos para operaciones administrativas de un entorno informático en la nube
- Permitir a los clientes supervisar las actividades pertinentes en un entorno informático en la nube
- Alineación de la administración de seguridad para redes virtuales y físicas (MICROSOFT, Microsoft y la norma ISO/IEC 27017, 2020)

2.4.4. Beneficios

El camino hacia la nube puede estar pavimentado con malentendidos y aprensión. Cualquier organización que confía sensible los datos del cliente a un tercero han llegado a saber allí son áreas grises donde los derechos y responsabilidades no han sido claramente definido. Se han tomado muchas cosas en confianza y esa no es necesariamente la mejor receta para éxito.

La ISO / IEC 27017 puede demostrar ser muy útil a medida que una organización hace decisiones sobre la adopción de la nube y qué socios son adecuados a sus necesidades. Los CSP que elijan implementar ISO / IEC 27017 también pueden beneficiarse al saber que están ofreciendo una solución segura en que sus clientes pueden confiar, lo cual es muy útil en la construcción de una relación basada en la nube, y por supuesto, trabajando con sus clientes a través de su adopción el proceso ISO / IEC 27017 se protege de acusaciones perjudiciales o demandas judiciales que pueden interrumpir el negocio y dañar su marca. (Institution The British Standards, 2019)

2.5. ISO 27018: Requisitos para la protección de la información de identificación personal (PII) en sistemas Cloud

2.5.1. Antecedentes

La Norma ISO/IEC 27018 permite a los proveedores de nube pública evaluar riesgos e implementar controles para la protección de los datos personales almacenados. En él se incluye la privacidad en el modelo ISO para el gobierno de las TIC, que se suma a la calidad aportada por la Norma UNE-ISO/IEC 20000 y a la seguridad según las UNE-ISO/IEC 27001 e UNE-ISO/IEC 27002.

La ISO/IEC 27018 es el primer estándar internacional sobre privacidad en la nube. Esta norma se basa, fundamentalmente, en leyes y regulaciones emitidas en la Unión Europea. En este sentido, es importante tener en cuenta que la ISO/IEC 27018 puede ser tanto un estándar como un código de buenas prácticas para el proveedor de servicios de nube pública, según el caso, y que su publicación se ha adelantado a anuncios como el de la Comisión Europea de poner en marcha una iniciativa europea de computación en nube1 e incluso al todavía futuro Reglamento General de Protección de Datos2.

Desde el punto de vista de protección de datos, la ISO/IEC 27018 se basa en un esquema en el que el cliente del servicio es el responsable del tratamiento, es decir, quien decide sobre el tratamiento de los datos; y el proveedor es el encargado del tratamiento y debe tratar dichos datos siguiendo las instrucciones del cliente como se muestra en la Figura 12-2:

Figura 12-2 Proceso de tratamiento de Datos

Fuente: Fernàndez & Recio, 2015

La norma pretende ser "una referencia para la selección de los controles de protección información de carácter personal en el proceso de implementación de un sistema de gestión de seguridad de información basado en la norma ISO / IEC 27001 para un sistema cloud, o como un documento de orientación para las organizaciones para la implementación de los controles de protección de PII comúnmente aceptados"

2.5.2. *Importancia*

Un buen modelo de gobierno de TI no está completo sin una norma sobre protección de datos personales. En la actualidad, casi todas las organizaciones tratan datos personales y, con independencia de cuál sea la estadística que se considere, cada vez más lo hacen en la nube.

Ante esta realidad, la ISO/IEC 27018 constituye una herramienta clave. En el caso de proveedores de servicios de nube pública que estén certificados con la Norma ISO/IEC 27001, la ISO/IEC 27018 aporta un conjunto adicional de controles sobre privacidad. Es decir, ayuda también para identificar a proveedores de nube pública que tienen un buen gobierno de TI.

Así, el modelo ISO en Tecnologías de la Información y Comunicación (TIC) referido a la nube pública incorpora la calidad (Norma UNE-ISO/IEC 20000), seguridad (Normas UNE-ISO/IEC 27001 e ISO/IEC 27002) y privacidad (Norma ISO/IEC 27018). Y permite que cualquier organización se beneficie de los factores críticos de éxito a los que da lugar este modelo. Mismo que está orientado a los objetivos de negocio, ya sean nuevos proyectos o servicios; consta de dos parámetros primordiales que son el ciclo PDCA (motor orientado a la mejora continua) y el control interno de tecnologías de la información (conocimiento); la simplicidad del ciclo PDCA orientado a los objetivos de negocio facilita la labor de gestión y gobierno en las TIC; consiste en aplicar el control interno de tecnologías de la información (considerando los objetivos de negocio) a cualquier nueva tecnología, negocio o servicio; incorpora la calidad y la seguridad en los servicios y proyectos; contempla indicadores (objetivo de la métrica) y métricas orientadas al negocio en el mundo de las TIC; y cualquier proyecto de innovación se puede incorporar en este modelo.

Figura 13-2 Modelo ISO en TIC

Fuente: Fernàndez & Recio, 2015

2.5.3. Controles de seguridad en la ISO 27018

Entre las medidas o controles explicados por la norma ISO 27018 señalaría los siguientes:

- El proveedor, como responsable del tratamiento, tendrá que proporcionar las herramientas adecuadas para permitir y facilitar el ejercicio por el interesado, de los derechos de acceso, rectificación y cancelación en relación con el tratamiento de los datos.

- En relación con los fines del tratamiento, el proveedor debe velar por el cumplimiento del tratamiento a los únicos usos descritos al cliente en el momento de la contratación del servicio, en particular garantizando que los datos no serán utilizados para fines distintos de los especificados por el cliente, ni para el propósito de marketing directo o publicitario, a menos que haya consentimiento explícito, consenso de que, en cualquier caso, nunca será un requisito establecido por el proveedor para la función del servicio.

- Salvo que exista una prohibición establecida por la ley, la solicitud de divulgación de los datos personales por parte de las autoridades administrativas o judiciales será notificada sin demora al consumidor de servicios de nube.

- En cuanto al tema de la subcontratación, la norma establece, de forma particularmente incisiva, el derecho del cliente a conocer, incluso antes de empezar a utilizar el servicio, toda la cadena de los subcontratistas, los países en los que se establecen, la ubicación de los data centers utilizados por ellos y sus obligaciones en relación con el tratamiento de los

datos. También se reconoce el derecho del cliente a oponerse a eventuales cambios en la cadena de los subcontratistas, o de rescindir del contrato.

- El proveedor deberá notificar inmediatamente al cliente toda violación de los datos personales de los que derivan de una pérdida, destrucción, alteración, divulgación o acceso no autorizado, con el fin de permitir que el propietario y los interesados lo notifiquen a las autoridades de control en los plazos establecidos por la ley.

- El acuerdo de servicio debe establecer una política de traslado que detalla el método de restitución, transferencia y / o cancelación de sus datos en poder del proveedor en el cese de los efectos de dicho contrato.
- En relación con las medidas de seguridad de la información, sería conveniente que todo el personal del proveedor y de los subcontratistas estuviese vinculado a un acuerdo de confidencialidad, recibiese una formación adecuada, accediesen a los datos mediante operaciones de autentificación y login. (GP Liaison, 2019)

2.5.4. Beneficios

Esta norma advierte que el proveedor sea transparente en los términos y condiciones de sus servicios, y en las prácticas de negocio que lleva a cabo; y demuestre compromiso con el cliente para ayudarle a cumplir con las leyes y regulaciones sobre protección de datos personales o privacidad, y seguridad.

Además, le facilita la demostración de responsabilidad (accountability) en la adopción de medidas y en el desempeño de sus funciones como encargado del tratamiento, y facilita al cliente la prueba necesaria de que ha sido auditado de manera independiente y periódicamente.

En cuanto al cliente, hace posible que controle el tratamiento de los datos personales que ha encomendado al proveedor, pudiendo incorporar como parte del contrato o cláusulas contractuales los compromisos de dicho proveedor en virtud de la ISO/IEC 27018 y sabiendo qué información tiene que solicitarle. Además, tendrá garantías adicionales de limitación del uso de datos personales por parte del proveedor, que no podrá utilizarlos con fines de publicidad o marketing a menos que esté autorizado expresamente.

Por último, las autoridades de protección de datos y otras autoridades reguladoras podrán obtener fácilmente garantías de cumplimiento en caso de que sea necesario; podrán considerar la Norma ISO/IEC 27018 y otros estándares como una medida proactiva por quienes están sujetos al cumplimiento, ya sea el responsable o el encargado del tratamiento. Así mismo, les servirá de

marco de referencia para impulsar buenas prácticas y esquemas de autorregulación en materia de protección de datos personales.

2.6. Modelo de Seguridad

2.6.1. Antecedentes

El Modelo de Seguridad de la Información es el conjunto de procesos, procedimientos, metodologías, principios, políticas, estándares y controles, es adoptado para promover la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información, basado en mejores prácticas tendientes a preservar la confidencialidad, integridad y disponibilidad de la información, y que permite contar con lineamientos claros mantener un entorno razonablemente seguro, apoyado en los objetivos estratégicos del negocio.

Este modelo involucra todas las áreas de la organización, donde cada uno de los colaboradores, de acuerdo con sus funciones y rol en el negocio, será responsable en cierta medida por la protección de la información de la empresa y de sus clientes.

El modelo de seguridad de la información se utiliza para describir con precisión la estrategia de seguridad de un sistema de información por métodos formales o informales, que se basa en la estructura del sistema de seguridad de la información.

La Figura 12-2 muestra la arquitectura de los niveles de seguridad de la información multinivel. En la actualidad, se discuten tres famosos modelos de seguridad basados en políticas de seguridad multinivel: el modelo BellLaPadula, el modelo Biba y el modelo Clark-Wilson.

Figura 14-2 Arquitectura de seguridad de información multinivel

Fuente: Jing Jin; Meihui Shen, 2015

2.6.2. Características

Algunos objetivos característicos de un modelo de seguridad incluyen:

- Verificar la identidad de los usuarios, proporcionada por los sistemas de autenticación que incluyen la seguridad de la contraseña y otros factores.
- Permitir a los usuarios autorizados acceder a recursos, proporcionados por sistemas de autorización que definen procesos basados en roles o solicitudes, y el aprovisionamiento relacionado. Los recursos, por ejemplo, incluyen cuentas, servicios, información del usuario y funciones. Un modelo de seguridad también requiere procesos de aprovisionamiento adicionales para seleccionar los recursos a los que los usuarios pueden acceder.
- Administrar qué operaciones y permisos se otorgan para cuentas y usuarios.
- Delegar la lista de actividades de un usuario a otros usuarios, por solicitud o por asignación.
- Proteger la información confidencial, como listas de usuarios o atributos de cuenta.
- Garantizar la integridad de las comunicaciones y los datos.

Un **modelo de seguridad** es un modelo de computadora que se utiliza para identificar e imponer políticas de seguridad.

No requiere ninguna formación previa, puede basarse en el modelo de derecho de acceso o en el modelo de computación de distribución o modelo de computación.

Un modelo de seguridad es un marco en el que se desarrolla una política de seguridad. El desarrollo de esta política de seguridad está orientado a una configuración o instancia particular de una política, por ejemplo, una política de seguridad basada en la autenticación, pero construida dentro de los límites de un modelo de seguridad. Por ejemplo, al diseñar un modelo de seguridad basado en autenticación y autorización, uno consideraría el modelo de seguridad de 4 factores, es decir, autenticación, autorización, disponibilidad y autenticidad.

Generalmente, un modelo de seguridad es un "sistema formal" utilizado para especificar y razonar sobre la política de seguridad (es decir, se utiliza como base para las pruebas formales de especificación). Por lo tanto, se pretende abstraer la política de seguridad y manejar su complejidad; representar los estados seguros de un sistema, así como la forma en que el sistema puede evolucionar, verificar la coherencia de la política de seguridad, detectar y resolver posibles conflictos.

2.7. Análisis de las principales vulnerabilidades

A continuación, se encuentran descritas las consideraciones de seguridad de infraestructuras y servicios de la nube, de los líderes del sector como: Trend Micro, la organización internacional CSA (Cloud Security Alliance), y GARTNER Inc.

Trend Micro líder mundial en ciberseguridad, público un informe denominado "Mapeo del futuro: Cómo lidiar con amenazas omnipresentes y persistentes", donde evalúa la falta de seguridad en los sistemas tecnológicos privados incluidos los de la nube, como se presenta a continuación en la Tabla 7-2: (TREND MICRO, 2019)

Tabla 7-2 Vulnerabilidades de la Infraestructura Cloud

VULNERABILIDADES	DESCRIPCIÓN
Configuraciones de seguridad mal configuradas durante la migración de la nube dará como resultado más violaciones de datos	Se predice que se verá más casos importantes de violación de datos que serán un resultado directo de configuraciones incorrectas durante la migración a la nube. Transición de datos en la nube local o privada a un proveedor de servicios en la nube puede abrir la empresa a riesgos de seguridad a menos que la empresa tenga un buen control de lo que está sucediendo exactamente con sus datos.
Se utilizarán instancias en la nube para la minería de criptomonedas	Los ciberdelincuentes intentarán secuestrar las cuentas en la nube para minar criptomonedas o mantener el control sobre otras alternativas. No es un juicio único por parte de ciberdelincuentes ya que las herramientas de escáner en el almacenamiento de nube ya están disponibles; añadir dificultad de obtener la configuración de seguridad múltiple para cada implementación en la nube correctamente será una opción. También se espera más malware de cryptojacking para minimizar el riesgo de detección al limitar el uso de recursos.

Más vulnerabilidades de software relacionadas con la nube será descubierto	Tanto Docker como Kubernetes son ampliamente adoptados para su uso en implementaciones basadas en la nube, misma que ya han presentado vulnerabilidades. Por lo que a medida que crece la adopción de la nube, se verá que la investigación de vulnerabilidad de la infraestructura de la nube comienza a ganar terreno.

Realizado por: Tenelema Arias

Cloud Security Alliance es una organización internacional sin ánimo de lucro para promover el uso de mejores prácticas para garantizar la seguridad en cloud. En octubre de 2015 publicó un informe denominado "Informe de Percepción de Proveedores de cloud computing" que incluye una encuesta a 200 profesionales / usuarios de servicios de Cloud durante los eventos InfoSecurity y CIBER 2015 en Argentina. (CSA, Cloud Security Alliance (CSA), 2015)

En la primera encuesta relacionada con las características de seguridad obtuvo los siguientes resultados

- **Prueba de Vulnerabilidad**

Gráfico 1-2 Prueba de vulnerabilidades en la nube

Fuente: CSA; 2015

En el Gráfico 1-2 se verifica que de los 80 profesionales / usuarios de servicios de Cloud afirman que su proveedor evalúa posibles vulnerabilidades en los recursos ofrecidos. Otro dato importante en el parámetro de prueba de vulnerabilidad es que 160 profesionales /usuarios afirman que el proveedor verifica las nuevas versiones ante posibles vulnerabilidades. También se denota que casi 80 profesionales / usuarios mencionan que no se les permiten realizar pruebas de vulnerabilidades, ni tampoco ver los resultados de las misma. 160 profesionales / usuarios admiten que el proveedor realiza cambios para mitigar vulnerabilidades

- **Manejo de los incidentes de seguridad**

Gráfico 2-2 Manejo de incidentes de seguridad en la nube

Fuente: CSA; 2015

En el Gráfico 2-2 se verifica que en un promedio de 45 profesionales / usuarios de servicios de Cloud afirman que su proveedor define procedimientos, controles y canales de comunicación ante incidentes de seguridad.

- **Encriptación de datos y redes**

Gráfico 3-2 Encriptación de Datos y redes en la nube

Fuente: CSA; 2015

En el Gráfico 3-2 se verifica que en un promedio de 150 profesionales de servicios de Cloud afirman que su proveedor encripta sus datos y redes, pero un promedio de 80 usuarios comparte dicha opinión.

- **Auditorias**

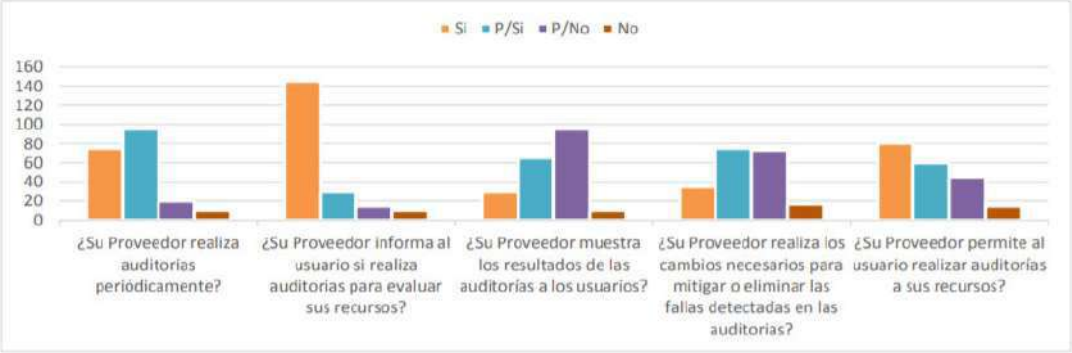


Gráfico 4-2 Auditorias en la nube

Fuente: CSA; 2015

En el Gráfico 4-2 se verifica que en un promedio de 45 profesionales/usuarios de servicios de Cloud mencionan en las auditorias el proveedor no muestra los resultados, no realiza los cambios necesarios para mitigar o eliminar faltas detectadas, así como no permite realizar al usuario auditorías a sus recursos.

- **Administración de accesos de los usuarios**

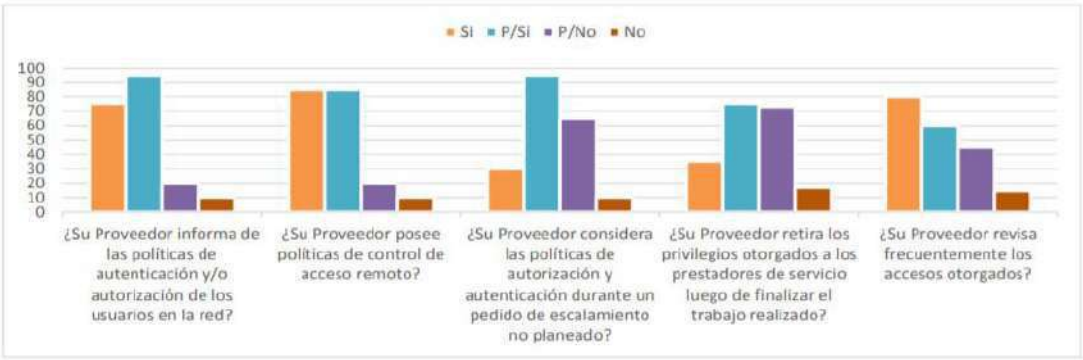


Gráfico 5-2 Administración de accesos de los usuarios en la nube

Fuente: CSA; 2015

En el Gráfico 5-2 se verifica que en un promedio de 50 profesionales de servicios de Cloud afirman que no se considera la política de autorización y autenticación durante un pedido de escalamiento, retira los privilegios otorgados a los prestadores de servicio, revisa frecuentemente los accesos otorgados.

La segundad encuesta relacionada con las características de Técnicas obtuvo los siguientes resultados:

- **Lock-In / Dependencia de los productos de un Proveedor específico**

Gráfico 6-2 Lock-In / Dependencia de los productos de un Proveedor específico en la nube

Fuente: CSA; 2015

En el Gráfico 6-2 se verifica que en un promedio de 80 profesionales de servicios de Cloud afirman que no se considera la dependencia de los productos de un proveedor especifico.

- **Aplicación de parches**

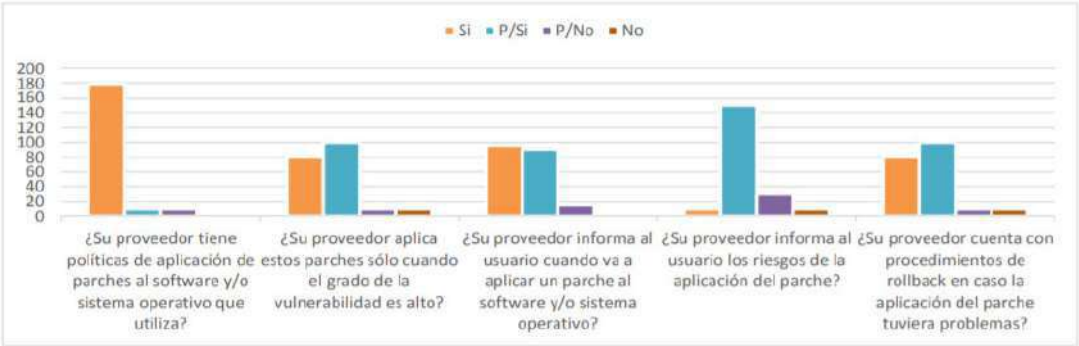


Gráfico 7-2 Aplicación de parches en la nube

Fuente: CSA; 2015

En el Gráfico 7-2 se verifica que en un promedio de 60 profesionales/usuarios de servicios de Cloud afirman que no gestiona la aplicación de parches.

- **Desarrollo de soluciones**

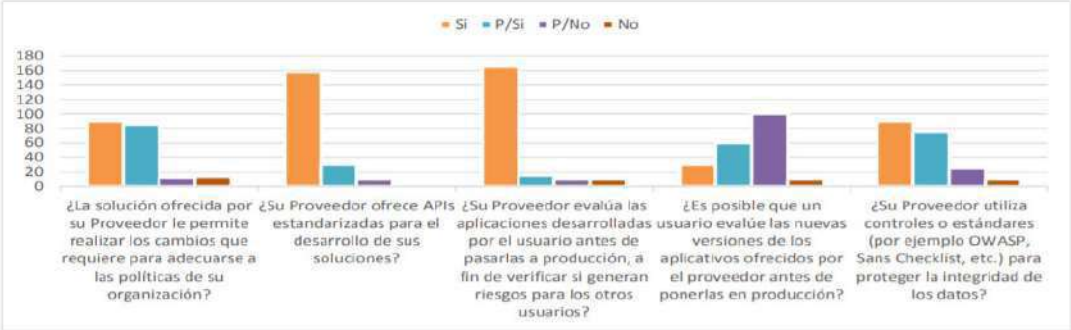


Gráfico 8-2 Desarrollo de Aplicaciones en la nube

Fuente: CSA; 2015

En el Gráfico 8-2 se verifica que en un promedio de 80 profesionales/usuarios de servicios de Cloud afirman que si gestiona el desarrollo de soluciones.

- **Almacenamiento de datos**

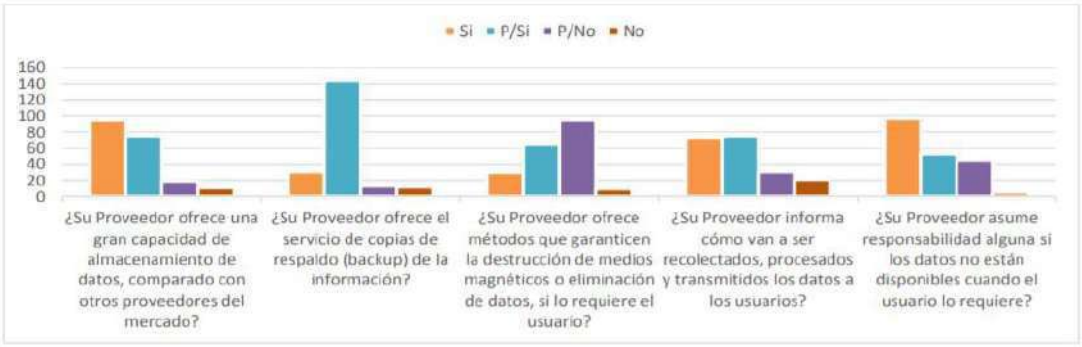


Gráfico 9-2 Almacenamiento de datos en la nube

Fuente: CSA; 2015

En el Gráfico 9-2 se verifica que en un promedio de 35 profesionales/usuarios de servicios de Cloud afirman que si se informa como van hacer recolectados, procesados y transmitidos los datos a los usuarios.

GARTNER Inc. es una empresa internacional consultora y de investigación de las tecnologías de la información. En junio de 2019 publicó un artículo denominado "¿Vulnerability Management in DevOps-style IT?" que trata sobre la nube pública (principalmente IaaS, pero quizás algunos PaaS) y contenedores en general: (GARTNER, 2019)

Las vulnerabilidades presentadas como preguntas del artículo son:

1. ¿Incluye de alguna manera la evaluación de vulnerabilidad (VA) en sus procesos?

2. ¿Cómo se ve el proceso? ¿Quién es el propietario de este proceso y cómo logró la seguridad agregarse a esto?
3. ¿La seguridad tiene "poderes de veto" para rechazar implementaciones debido a vulnerabilidades?
4. ¿Evalúa imágenes (contenedores, máquinas virtuales, etc.) antes de la producción?
5. Si es así, ¿utiliza métodos estáticos (sin código de ejecución) o dinámicos (iniciar y luego conectar / escanear)?
6. ¿Evalúa las imágenes en ejecución durante la producción?
7. ¿Confía en las herramientas de contenedor (Docker) o de proveedor de la nube o en herramientas de evaluación de vulnerabilidad dedicadas para la evaluación?
8. ¿Utiliza herramientas específicas de contenedor o herramientas VA de propósito general que tienen funcionalidad de evaluación de contenedor?

Todas las preguntas mencionadas anteriormente sirven como pauta para solventar las vulnerabilidades en la nube.

2.8. Determinación de la plataforma para almacenamiento en la nube

Se procede a realizar una búsqueda de información de estudios primarios acerca de la plataforma para almacenamiento en la nube más utilizados, se seleccionará la plataforma de acuerdo a sus características.

Las plataformas para almacenamiento en la nube seleccionados son:

- ✓ Nextcloud: software para nubes descentralizadas y federadas como alternativa a los servicios de nube centralizados. (Nextcloud, 2020)
- ✓ Google Drive: es un servicio de almacenamiento en la nube, y como cualquier servicio de almacenamiento en la nube, su objetivo principal es ampliar su capacidad de almacenar archivos más allá de los límites de su disco duro. (Cloudwards, 2020)
- ✓ Office 365: es un servicio de Microsoft que ofrece acceso a herramientas ofimáticas, como Excel, Word, Powerpoint, Outlook, Exchange online a través de la nube y puede ser utilizado mediante diferentes dispositivos como móviles, tablets, MAC. (CISET, 2020)
- ✓ OwnCloud: es una solución de colaboración de contenido, sincronización y archivos de código abierto, con la cual los equipos pueden acceder fácilmente a los datos desde cualquier lugar y desde cualquier dispositivo. (Owncloud, 2020)
- ✓ Box: solución almacenar cualquier tipo de archivo en línea y acceder a él fácilmente desde su computadora, teléfono o tablet, en cualquier momento y lugar. (Box, 2020)

- ✓ Citrix: es una plataforma que aloja y administra los servicios de Citrix. Se conecta a sus recursos a través de conectores en cualquier nube o infraestructura que elija (local, nube pública, nube privada o nube híbrida). (Citrix, 2019)
- ✓ Dropbox: solución que mantiene todos los archivos seguros con un potente almacenamiento en la nube en línea. (Dropbox, 2020)

Posteriormente, se procede con la síntesis para determinar la plataforma para almacenamiento en la nube que será utilizado como base, para lo cual se realiza la comparación entre las plataformas antes descriptas con base en los siguientes factores; se toma la información recopilada y la del artículo "Nextcloud vs. OwnCloud vs Seafile: The Best Self-Hosted File-Syncing Service" (NCC, 2018) y del "Nextcloud compares to these popular closed-source services" (NCC, 2018):

- Almacenamiento ilimitado
- Soporte de archivos grandes
- 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
- Metadatos de archivo
- Ver Pdf, imágenes, video
- 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 video
- 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
- Con el atributo de cookie del mismo sitio
- Control de acceso a archivos
- Derechos de acceso a la aplicación

Tabla 8-2 Tabla comparativa entre plataformas 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

Realizado por: Tenelema Esthela, 2019

De los resultados de la comparación realizada, se puede determinar que la plataforma para almacenamiento en la nube Nextcloud es el más adecuado debido a sus ventajas en relación a las otras plataformas ya que permite texto integrado, video y chat de voz, notificaciones en tiempo real, etc. Por lo que será utilizado como base para la elaboración e implementación del modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube con base en las normas ISO 27017 y 27018 para demostrar la hipótesis.

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

En este Capítulo, se detalla el tipo de investigación, diseño, métodos, técnicas, instrumentos con su respectiva validación, modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube, los prototipos (integran las mejores prácticas en seguridad informática con base en las normas ISO 27017 y 27018) y se definen los escenarios de pruebas.

3.1. Tipo de investigación

La presente investigación puede dividirse de dos tipos: aplicativa y experimental.

- **Aplicativa:** ya que se basa en conocimientos existentes, derivados de investigaciones previas, dirigida su interés en la aplicación y en las consecuencias prácticas de los conocimientos que se han obtenido
- **Experimental:** ya que se basa en pruebas realizadas en escenarios de laboratorio, en las que se observa los elementos más importantes del objeto de estudio que se investiga para entender los procesos causales.

3.2. Diseño de la investigación

El tipo de la investigación será cuasi-experimental debido a que, se escoge las normas ISO 27017 y 27018 que serán la base al modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube. El diseño será transversal debido a que los resultados obtenidos en las pruebas realizadas en base a la muestra determinada serán comparados.

3.3. Métodos y técnicas

Los métodos y técnicas utilizados para la investigación son:

3.3.1. Métodos

- **Método analítico:** porque se realizará un análisis de los controles de seguridad para almacenamiento en la nube, considerando las normas ISO 27017 y 27018 las cuales permitirán tener un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube
- **Método inductivo:** a partir de los controles de seguridad para almacenamiento en la nube, se obtendrá e implementará un modelo de seguridad que mejore el nivel de seguridad de la información para almacenamiento en la nube.

3.3.2. Técnicas

Las técnicas que serán utilizadas en la presente investigación son:

- **Búsqueda de información:** permite obtener la información necesaria de las metodologías existentes, norma ISO 27017 y 27018, utilizando las fuentes primarias y secundarias disponibles.
- **Pruebas:** permita realizar experimentos en escenarios de laboratorio, en el primer escenario utilizando el modelo de seguridad propuesto y en el segundo escenario las que no la considere para almacenamiento en la nube.
- **Observación:** permita determinar resultados de las pruebas realizadas en los escenarios de laboratorio.
- **Análisis:** permite determinar los resultados de la investigación

3.4. Instrumentos

Los instrumentos que apalancan o son la base en la recopilación los datos de los indicadores son los siguientes:

- **VirtualBox:** es un potente producto de virtualización x86 y AMD64 / Intel64 para uso empresarial y doméstico. VirtualBox no solo es un producto extremadamente rico en funciones y de alto rendimiento para clientes empresariales, sino que también es la única solución profesional que está disponible gratuitamente como software de código abierto. (BOX, 2019)
- **NextCloud:** es un software de código abierto para la sincronización y el uso compartido de archivos para todos, desde individuos que operan el servidor gratuito Nextcloud en la privacidad de su propio hogar, hasta grandes empresas y proveedores de servicios compatibles con la suscripción empresarial de Nextcloud. (NEXTCLOUD, 2019)

- **CentOS** es una distribución de Linux (derivada de Red Hat Enterprise Linux) que es popular entre los administradores de sistemas, ingenieros de DevOps y usuarios domésticos por igual. También es utilizado por muchas organizaciones para servidores de desarrollo y producción. (Simpson, 2019)
- **PostgreSQL:** es un poderoso sistema de base de datos relacional de objetos de código abierto que usa y extiende el lenguaje SQL combinado con muchas características que almacenan y escalan de manera segura las cargas de trabajo de datos más complicadas. (Postgresql, 2020)
- **Apache:** popular servidor web multiplataforma de código abierto que, según los números, es el servidor web más popular que existe. Lo mantiene activamente la Apache Software Foundation. (Kinsta, 2020)
- **PHP:** es un lenguaje de script de uso general de código abierto ampliamente utilizado que es especialmente adecuado para el desarrollo web y puede integrarse en HTML (El Grupo PHP, 2020)

3.5. Validación de instrumentos

Los instrumentos software que han sido utilizados en la investigación fueron seleccionados debido a sus características y ventajas que se mencionan a continuación:

- **Kali:** Kali Linux es una distribución de Linux basada en Debian dirigida a pruebas avanzadas de penetración y auditoría de seguridad. Kali contiene varios cientos de herramientas orientadas a diversas tareas de seguridad de la información, como Pruebas de penetración, Investigación de seguridad, Informática forense e Ingeniería inversa. Kali Linux está desarrollado, financiado y mantenido por Offensive Security, una empresa líder en capacitación en seguridad de la información. (KALI, 2019)
- **Openvas o Greenbone:** OpenVAS es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas no autenticadas, pruebas autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad. (OPENVAS, 2020)

3.6. Elaboración del modelo de seguridad

Luego del análisis de las principales vulnerabilidades, y plataforma de almacenamiento en la nube que han sido considerados como base en el Capítulo II, además de la naturaleza de los ataques cibernéticos que están en constante evolución; se presenta el 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 mismo que se basa en tres objetivos generales:

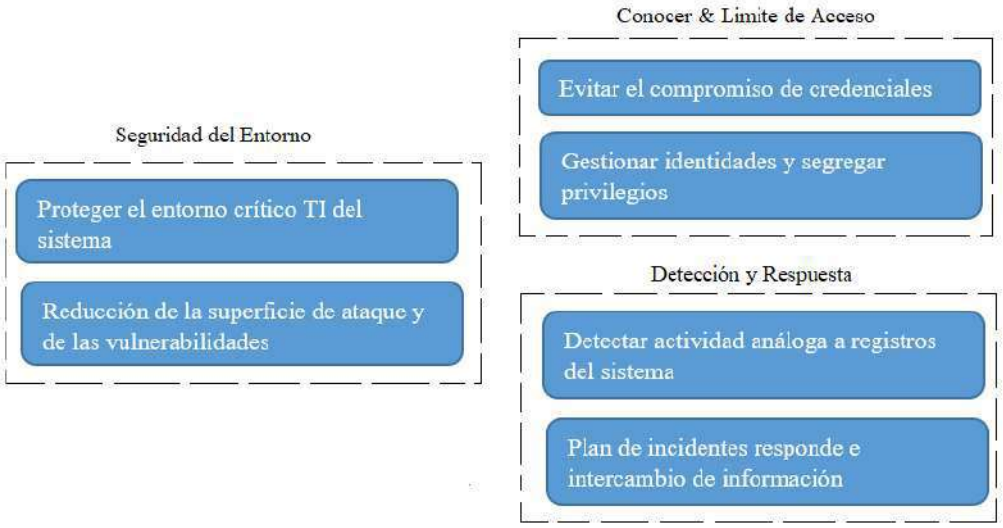


Figura 1- 3 Objetivos generales del Modelo de Seguridad

Realizado por: Tenelema Esthela, 2019

3.6.1. Estructura del modelo de seguridad

El modelo se basa en controles, cada control de seguridad está estructurado en tres partes: información general del control, definición del control y guía de implementación, como se describe a continuación.

Información general del control

- **Número y nombre del control -** Cada control tiene un número y nombre único.
- **Tipo de control -** Identifica el control como "Obligatorio" o "Recomendado". Los usuarios deberán priorizar todos los controles obligatorios que les resulten aplicables, tomando en cuenta su tipo de almacenamiento en la nube. Los controles recomendados se consideran buenas prácticas de seguridad y se sugiere enfáticamente su implementación adicional.

Definición del control

- **Objetivo del control -** Indica el objetivo de seguridad que debe alcanzarse, independientemente del método de implementación.
- **Componentes dentro del alcance -** Componentes específicos relacionados con el almacenamiento en la nube que abarca ese control en particular.
- **Factores de riesgo -** Explica a detalle los riesgos específicos que aborda este control de seguridad.

Guía de implementación

- **Planteamiento del control -** Los medios sugeridos mediante los cuales puede alcanzarse el objetivo del control.
- **Contexto del control -** Información adicional de antecedentes acerca de este control.
- Directrices para la implementación

3.6.1.a Protección de la Plataforma de Virtualización

Tipo de Control **Obligatorio**

Objetivo del control: 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.

Componentes dentro del alcance:

• Plataforma de virtualización (también denominada hipervisor) y VMs utilizadas para hospedar cualquiera de los componentes relacionados con el almacenamiento en la nube que se indican a continuación:

- Interfaz de almacenamiento en la nube
- Interfaz de comunicación
- GUI
- Servidor de salto
- Firewalls

Factores de riesgo:

Acceso no autorizado al hipervisor y sus módulos de configuración

- Proliferación incontrolada de VMs, que lleva a máquinas inmanejables, sin parches y no contabilizadas.
- Proliferación incontrolada de VMs, que lleva a un acceso no autorizado a datos.
- Falta de visibilidad en la separación de redes y el control sobre redes virtuales cuando no se utiliza protección de seguridad de redes (como firewalls físicos o sistemas de detección de intrusiones)

Guía de implementación

Planteamiento del control: Proteger la plataforma de virtualización, las máquinas virtualizadas y la infraestructura virtual de soporte (p.ej., *firewalls*) al mismo nivel que los sistemas físicos.

Contexto del control: La virtualización en sí misma proporciona otra capa de defensa contra los atacantes, ya que cada máquina virtual está por sí misma aislada del resto.

Por lo tanto, si un atacante es capaz de poner en peligro una máquina virtual, está operando en un entorno aislado. Aún más, la virtualización también proporciona la posibilidad de almacenar la copia corrupta de la máquina virtual para su posterior análisis forense.

Directrices para la implementación:

- Los mismos requisitos de seguridad se aplican a la plataforma de virtualización (a veces también llamada hipervisor), a las máquinas virtuales y a la infraestructura virtual de soporte que a todos los demás sistemas y componentes de la infraestructura (que cubren, por ejemplo, restricciones de acceso privilegiado, inicio de sesión, instalación de parches de seguridad, etc.).
- El anfitrión o sistema de la plataforma de virtualización está sujeto a protección física que impide el acceso físico no autorizado.
- La plataforma de virtualización debería fortalecerse de acuerdo a una o más de las siguientes guías:
    - Guía de configuración de seguridad del proveedor,
    - Guía de configuración de seguridad estándar de la industria (por ejemplo, DISA STIG, NIST),
    - Una configuración o serie de controles de seguridad estándar a nivel local o de una autoridad reguladora con el mismo rigor que la guía del proveedor o de la industria.

3.6.1.b Protección del entorno de almacenamiento en la nube

Tipo de Control: **Obligatorio**

Objetivo del control: 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.

Componentes dentro del alcance:

- Interfaz de comunicación (red de comunicación)
- GUI
- Módulo de seguridad Hardware.
- Servidor de salto

Factores de riesgo:

- Comprometer el sistema de autenticación de los usuarios
- Comprometer las credenciales del usuario
- Repetición de credenciales
- Acceso no autorizado

Guía de implementación

Planteamiento del control: Una zona segura independiente protege a la infraestructura de almacenamiento en la nube de ataques y amenazas que pudieran poner en compromiso a los entornos generales externos y de la organización o entidad que la utilice.

Contexto del control: La segmentación efectiva incluye la separación de niveles de red, restricciones de acceso y restricciones de conectividad del entorno de almacenamiento en la nube.

Directrices para la implementación:

- Implementar una "zona segura" para separar y proteger la infraestructura de almacenamiento en la nube de la amenaza que pudiera poner en compromiso los sistemas y servicios ubicados fuera de la zona segura.
- Todos los componentes dentro de la zona segura deberán estar protegidos en un nivel igual o equivalente de seguridad, control de acceso y confianza y pueden comunicarse libremente

dentro de la zona. Los usuarios pueden considerar la implementación de separación adicional entre componentes de la zona segura.

- Crear una infraestructura de próxima generación que posea la flexibilidad requerida para escalar instantáneamente y para integrarse con los sistemas existentes en varios entornos, mezclando los datos de la nube de forma transparente.
- Crear una infraestructura hiperconvergente que hace que implementar una nube sea fácil mediante la gestión con un único panel de control de computación, almacenamiento y red de todas las aplicaciones críticas para la organización.

3.6.1.c Protección contra Malware

Tipo de Control: **Obligatorio**

Objetivo del control: Asegurar que la infraestructura de almacenamiento de la nube esté protegida en contra de malware.

Componentes dentro del alcance:

- Servidor de salto
- Servidor o servidores de almacenamiento en la nube

Factores de riesgo:

- Ejecución de código malicioso
- Aprovechamiento de vulnerabilidades de seguridad conocidas

Guía de implementación

Planteamiento del control: Se instala y se mantiene actualizado en la plataforma o en la infraestructura que la apalanca un software antimalware de un proveedor reconocido.

Contexto del control: Malware es un término general que incluye muchos tipos de programas invasivos no deseados, incluyendo virus. La tecnología antimalware (un término más amplio para antivirus) resulta efectivo en la protección contra el código malicioso que tiene un perfil digital o de comportamiento conocido.

Directrices para la implementación:

- Se realiza un escaneo antimalware en acceso (también conocido como escaneo de tiempo real o en segundo plano) en la plataforma o en la infraestructura que le atañen al control. El escaneo completo a solicitud se programa cuando menos una vez a la semana. Por motivos de rendimiento, se realizan escaneos completos en momentos de poco uso y/o fuera de horas hábiles.
- Se instala el software antimalware de un proveedor reconocido en todas las plataformas informáticas y se actualiza en función de la frecuencia de escaneo
- Debe asegurarse que la transferencia del contenido de cualquier archivo no contenga ningún tipo de virus u otros datos que pudieran generar riesgos para el remitente, o para el receptor.
- Se realizan pruebas de compatibilidad del software antimalware con el entorno operativo.
- Invertir en un firewall de aplicaciones web (WAF) para analizar todas las conexiones entrantes a su servicio de nube para tendencias sospechosas, malware, denegación de servicio distribuida (DoS) y riesgos de Botnet.

3.6.1.d Integridad de la Base de Datos

Tipo de Control **Obligatorio**

Objetivo del control: Asegurar la integridad de los registros de la base de datos para el almacenamiento en la nube.

Componentes dentro del alcance:

- Bases de datos dedicada para el almacenamiento en la nube, desagregada.

Factores de riesgo:

- Pérdida de integridad de datos sensibles

Guía de implementación

Planteamiento del control: Se realiza una comprobación de la integridad de la base de datos a intervalos regulares para las bases de datos de almacenamiento en la nube.

Contexto del control: Las comprobaciones de la integridad de la base de datos brindan un control para detectar la modificación imprevista de registros almacenados dentro de dicha base.

Directrices para la implementación:

• La funcionalidad de comprobación de integridad de la base de datos se activa para asegurar la integridad a nivel de los registros (suma de verificación o firma de los registros) y confirmar que no existen brechas en los archivos almacenados en la nube. Opciones para la implementación:

- Integrada a la aplicación de interfaz de almacenamiento en la nube,
- Integrada al producto de la base de datos.

3.6.1.e Monitor de integridad de archivos

Tipo de Control **Recomendado**

Objetivo del control: Detectar, prevenir actividad irregular en el sistema para contrarrestar una manipulación de los archivo o directorios monitorizados.

Componentes dentro del alcance:

• Sistema Operativo (Servidor de alojamiento de la plataforma de almacenamiento en la nube).

Factores de riesgo:

• Anomalías no detectadas o actividad sospechosa.

Guía de implementación

Planteamiento del control: Se implementa el monitoreo de intrusiones con el fin de descubrir acceso no autorizado a archivos o directorios del sistema (actividades irregulares).

Contexto del control: Permite a las organizaciones salvaguardar mejor la información confidencial contra robos, pérdidas y ataques de malware supervisando o monitoreando quién accede y modifica los archivos. El ámbito del monitoreo de integridad no se limita al contenido de los archivos y las carpetas, sino también a la integridad de los directorios del sistema, las claves de registro y los valores del sistema operativo.

Directrices para la implementación:

- El sistema debe contar con un proceso que brinde visibilidad acerca de qué archivo cambió, cuándo se cambió y quién lo cambió.
- Si se detecta una intrusión, se activa una alarma y, si la herramienta lo permite, se activa un mecanismo de rastreo (acceso a archivos y directorios, movimientos y usos compartidos).
- Las intrusiones detectadas se gestionan mediante el proceso estándar de respuesta a incidentes.

3.6.1.f Planeación de Respuesta a Incidentes Cibernéticos

Tipo de Control **Obligatorio**

Objetivo del control: Asegurar un enfoque congruente y efectivo para la gestión de incidentes cibernéticos.

Componentes dentro del alcance:

- Control de la organización

Factores de riesgo:

- Daño excesivo derivado de la preparación cibernética deficiente

Guía de implementación

Planteamiento del control: El usuario cuenta con un plan de respuesta a incidentes cibernéticos definido y comprobado.

Contexto del control: La disponibilidad y resiliencia adecuada resultan fundamentales para el negocio. A este respecto, definir y probar un plan de respuesta a incidentes cibernéticos es una forma muy efectiva de reducir el impacto y duración de un incidente cibernético real.
Debido a que las lecciones se aprenden ya sea al probar este plan o a través de incidentes reales, es crucial que se aplique lo aprendido y se mejore el plan. Además, la planeación del intercambio de información relacionada con amenazas e incidentes resulta crucial para ayudar.

Directrices para la implementación:

• El usuario ha desarrollado y cada año actualiza un plan de respuesta a incidentes cibernéticos. Existe un plan formal de respaldo y recuperación para todas las líneas críticas para brindar soporte a las actividades de respuesta a incidentes.

– El plan de respuesta a incidentes cibernéticos incluye detalles de contacto actualizados (interno y externo), así como programadores de escalamiento. Dicho plan tiene que incorporar:

o El plan de recuperación ante Incidentes de Seguridad Cibernética, proporciona una lista no exhaustiva de pasos o acciones que un cliente debe seguir en caso de violación de la seguridad cibernética y remitirse al servicio de soporte técnico que se encargue de la gestión de la plataforma de almacenamiento en la nube.

o Las políticas, leyes y reglamentos de seguridad interna dentro de la jurisdicción de un usuario deben acatarse y tenerse en cuenta en la planeación de la respuesta ante incidentes cibernéticos.

• Como mínimo, el plan se revisa en forma anual y se prueba cuando menos cada dos años, garantizando la recuperación segura de operaciones críticas con un tiempo de interrupción mínimo después de un incidente de ciberseguridad.

• El plan de respuesta ante incidentes cibernéticos incluye pasos a seguir para: – Notificar de inmediato a los actores y directivos internos relevantes.

– Notificar de inmediato a los actores y directivos de organizaciones externas relevantes (normalmente, regulador(es), supervisor(es) y autoridades de los cuerpos de seguridad),

– Notificar de inmediato al Centro de Atención al Cliente de la plataforma de almacenamiento en la nube a través del canal predeterminado y cumplir con otras obligaciones aplicables a los usuarios en caso de un incidente de seguridad, incluida la obligación de cooperar y proporcionar material forense que pueda requerir,

– Contener de inmediato; identificando y reduciendo la exposición del ataque,

– Realizar un análisis del problema posterior al incidente para identificar y solucionar vulnerabilidades,

– Documentar por completo el incidente.

3.6.1.g Pruebas de Penetración

Tipo de Control **Recomendado**

Objetivo del control: Validar la configuración de seguridad operativa e identificar brechas de seguridad al realizar pruebas de penetración.

Componentes dentro del alcance:

- Todo el hardware, software y red
- Capa de intercambio de datos

Factores de riesgo:

- Vulnerabilidades de seguridad o configuraciones de seguridad incorrectas desconocidas

Guía de implementación

Planteamiento del control: Se realizan pruebas de penetración a la aplicación, anfitrión y red a la zona segura es decir a la infraestructura que compone el almacenamiento en la nube.

Contexto del control: Las pruebas de penetración se basan en ataques simulados que utilizan tecnologías similares a aquellas que se despliegan en ataques reales. Se utilizan para determinar las rutas que los atacantes podrían utilizar y la profundidad a la que podrían acceder al entorno objetivo del ataque. Llevar a cabo dichos simulacros es una herramienta efectiva para identificar las debilidades del entorno que pudiera requerir corrección, mejora o controles adicionales.

Directrices para la implementación:

- La organización utiliza un enfoque basado en los riesgos con el fin de determinar el alcance preferido (por ejemplo, la zona segura o un servidor específico, incluyendo otros servicios potenciales que sirven de soporte a la zona segura), el método (por ejemplo, pruebas de caja blanca y de caja negra) y el origen del ataque (por ejemplo, ataque interno, desde el interior o el exterior de la zona segura, o externo) para la prueba.
- Las pruebas de penetración se realizan por lo menos cada 2 años, así como después de que ocurran cambios significativos en el entorno (por ejemplo, nuevos dispositivos del servidor o de la red, cambio al diseño de la red).
- Las pruebas de penetración se planean y realizan cuidadosamente para evitar posibles impactos en la disponibilidad o integridad.
- Las pruebas de penetración son realizadas por personal experto independiente del equipo responsable de la infraestructura.
- Las pruebas de penetración a los componentes y anfitrión de la red (por ejemplo, revisión de configuración y bases de reglas) se llevan a cabo en el entorno de producción de servicios.

• Se cuenta con suficientes protecciones para reducir al mínimo cualquier impacto operativo que pudiera surgir de la realización de la prueba de penetración.
• El resultado de las pruebas de penetración se documenta (con acceso restringido) y se utiliza como contribución para el proceso de actualización de la seguridad.

3.6.1.h Política de Contraseñas

Tipo de Control **Obligatorio**

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

Componentes dentro del alcance:

• Inicio de sesión a la plataforma de almacenamiento en la nube
• Tokens personales y dispositivos móviles personales utilizados como factor de posesión para una autenticación de múltiples factores

Factores de riesgo:

• Descifrado o adivinación de contraseñas u otra amenaza informática

Guía de implementación

Planteamiento del control: Todas las cuentas de aplicaciones y sistema operativo exigen contraseñas con parámetros adecuados tales como longitud, complejidad, validez y el número de intentos fallidos de inicio de sesión. Del mismo modo, los tokens y dispositivos móviles personales exigen contraseñas o un Número de Identificación Personal (PIN) con parámetros correspondientes.

Contexto del control: Implementar una política de contraseñas que brinde protección contra ataques comunes a las mismas (por ejemplo, adivinación y fuerza bruta) resulta efectivo para protegerse contra amenazas que pongan en compromiso las cuentas. A menudo, los atacantes utilizan los privilegios de una cuenta afectada para moverse lateralmente dentro de un entorno y realizar el ataque. Otro riesgo es que se vean comprometidas las claves de autenticación local para alterar la integridad de las transacciones. Sin embargo, resulta importante reconocer que las contraseñas por sí solas por lo general no son suficientes en el contexto actual de las

amenazas cibernéticas. Los usuarios deben considerar este control en estrecha relación con el requisito de autenticación de múltiples factores.

Directrices para la implementación:

• Se establece una política de contraseñas que cubre también la configuración del PIN, de conformidad con los estándares o mejores prácticas actuales de la industria y define los siguientes criterios:

– Vencimiento de contraseñas,

– Longitud, composición, complejidad y otras restricciones de las contraseñas,

– Reutilización de contraseñas,

– Bloqueo después de intentos fallidos de autenticación y medidas correctivas.

– Los requisitos de contraseñas podrán modificarse según resulte necesario para casos específicos de uso:

o En combinación con un segundo factor (por ejemplo, contraseña por única ocasión)

o Objeto de la autenticación (por ejemplo, sistema operativo, aplicación, dispositivo móvil, token),

o Tipo de cuenta (operador general, operador privilegiado, cuenta de aplicación a aplicación o claves de autenticación local).

3.6.1.i Fortalecimiento del Sistema

Tipo de Control **Obligatorio**

Objetivo del control: Reducir la superficie de ciberataque de los componentes relacionados con el almacenamiento en la nube al realizar el fortalecimiento del sistema.

Componentes dentro del alcance:

• Sistemas operativos para aplicaciones relacionadas con la plataforma de almacenamiento en la nube

• Infraestructura de soporte dentro de la zona segura (por ejemplo, firewalls, routers)

Factores de riesgo:

• Superficie de ataque excesiva

• Aprovechamiento de la configuración insegura del sistema

Guía de implementación

Planteamiento del control: El fortalecimiento del sistema se realiza y se mantiene en todos los componentes que le atañen.

Contexto del control: El fortalecimiento del sistema se aplica al concepto de seguridad de "privilegios mínimos" a un sistema al desactivar funciones y servicios que no se requieren para las operaciones normales del mismo. Este proceso reduce las capacidades, funciones y protocolos del sistema que una persona maliciosa puede utilizar durante un ataque

Directrices para la implementación:

• Todos los sistemas que le atañen se fortalecen conforme a una o más de las siguientes: – Guía de configuración de seguridad del proveedor, – Guía de configuración de seguridad estándar de la industria (por ejemplo, DISA STIG, NIST), – Una configuración o serie de controles estándar local o de autoridad reguladora del mismo rigor que la guía del proveedor o de la industria.
• Como mínimo, el proceso de fortalecimiento deberá:
– Cambiar contraseñas por defecto,
– Desactivar o eliminar cuentas de usuario innecesarias,
– Desactivar o restringir servicios, puertos y protocolos innecesarios,
– Eliminar software innecesario,
– Ajustar las configuraciones por defecto conocidas por ser vulnerables. Los estándares del proveedor y de la industria arriba indicados pueden proporcionar una guía detallada para lograr esos objetivos mínimos.
• Las desviaciones del estándar de fortalecimiento seleccionado se documentan junto con la justificación de la desviación y las mitigaciones potenciales aplicadas.
Los sistemas se mantienen protegidos:
- Comprobando los sistemas regularmente, al menos dos veces al año, contra los ajustes de seguridad identificados según las directrices anteriores para tomar las medidas correctivas pertinentes.
- O aplicando regularmente los ajustes de seguridad identificados.

3.6.1.j Autenticación de Múltiples Factores

Tipo de Control **Obligatorio**

Objetivo del control: 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.

Componentes dentro del alcance:

Dependiendo de la implementación:

- Acceso del operador al servidor de salto
- Proceso de inicio de sesión del usuario en la interfaz de almacenamiento en la nube (incluyendo base de datos hospedada) y la interfaz de comunicación
- Sistema operativo que hospeda la interfaz de almacenamiento en la nube (incluyendo base de datos hospedada) y la interfaz de comunicación

Factores de riesgo:

- Repetición de credenciales
- Descifrado o adivinación de contraseñas u otra amenaza informática
- Robo de contraseña

Guía de implementación

Planteamiento del control: La autenticación de múltiples factores se utiliza para el acceso del usuario interactivo a la plataforma de almacenamiento en la nube y a las cuentas del sistema operativo que las apalanque.

Contexto del control: La autenticación de múltiples factores requiere la presentación de dos o más factores comunes de autenticación que se mencionan a continuación:

- Factor del conocimiento (algo que el usuario o cliente sabe), por lo general, una contraseña.
- Factor de posesión (algo que el usuario o cliente tiene), normalmente:

– tokens conectados (por ejemplo, tokens USB, tarjetas inteligentes),

– tokens desconectados (por ejemplo, generadores de contraseña por única ocasión utilizando el teléfono celular, token RSA o Digipass del usuario o cliente).

- Factor de inherencia (algo que el operador es), generalmente, elementos biométricos tales como huella digital, escaneos de retina o reconocimiento de voz.

La implementación de la autenticación de múltiples factores brinda una capa adicional de protección contra ataques de autenticación comunes (por ejemplo, mirar por encima del hombro, reutilización de contraseña o contraseñas débiles) y proporciona una mayor protección contra la violación de cuentas. A menudo, los atacantes utilizan los privilegios de una cuenta afectada para moverse lateralmente dentro de un entorno y realizar el ataque.

Directrices para la implementación:

• Al implementar una autenticación de múltiples factores, se aplican los siguientes principios:
- Cuando se basa en un factor de conocimiento (normalmente una contraseña) combinado con un factor de posesión (un dispositivo móvil), el dispositivo utilizado para el segundo factor no debe ser el mismo que el dispositivo utilizado para introducir el primer factor.
- Las soluciones de segundo factor basadas en un factor de posesión incluyen (no es una lista exhaustiva): TOTP, RSA SecurID, Digipass, Mobile App, Tabla de Números de Autenticación de Transacciones (TAN), token personal de USB. La solución se elige en función de la propia gestión de riesgos del usuario
• Los sistemas de autenticación de múltiples factores están considerablemente más expuestos si las credenciales de autenticación se almacenan fuera de la zona segura (por ejemplo, dentro de un Directorio activo de la empresa). De ser viable, el sistema de autenticación que soporta la solución de múltiples factores se ubica dentro de la zona segura.
• Los factores de autenticación que se presentan se asignan en forma individual y soportan la rendición de cuentas individual con respecto al acceso a los servicios, sistema operativo y aplicación.
• Si se implementa un inicio de sesión único (por ejemplo, SAML), aún se requiere un segundo factor en dicho inicio de sesión único o en una etapa posterior

3.6.1.k Compromisos de las partes

Tipo de Control **Obligatorio**

Objetivo del control: 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.

Componentes dentro del alcance:

• Tipo de servicio en la nube:

- IaaS: consiste en ofrecer capacidad de cómputo, almacenamiento y servicios de red.

- PaaS: ofrecen servicios a todas las fases del ciclo de desarrollo o puede especializarse en un área en particular.
- SaaS: Ofrece aplicaciones completas, bajo demanda.

• Legislación de protección de la información o de datos personales (depende de cada jurisdicción).

Factores de riesgo:

- No control en la calidad de las actividades que se realice, el cumplimiento de los niveles de servicio y la consistencia entre los pagos pactados (si es de pago).
- La no protección de privacidad de la información.

Guía de implementación

Planteamiento del control: Protección legal de las partes involucradas (cliente-proveedor) en la contratación del servicio de almacenamiento en la nube.

Contexto del control: Poseer un contrato de voluntades que generé derechos y obligaciones legales para cada una de las partes que lo componen. Cuando existe un contrato es fundamental que, como mínimo, se conserve el grado de cuidado original con respecto a la seguridad con el fin de asegurar que no se introduzcan nuevas debilidades o vulnerabilidades.

Directrices para la implementación:

- Establecer SLA para el servicio.
- El prestador del servicio deberá respetar las instrucciones impartidas para el tratamiento de datos por el contratante.
- El prestador del servicio no podrá disponer ni hacer uso de los datos que se le proveen en calidad de tratamiento a menos que sea autorizado fehacientemente por el cliente.
- Prohibición de modificaciones unilaterales por el contratista a los términos del servicio para evitar la cautividad del cliente.
- El proveedor deberá establecer mecanismos seguros de acceso a la información.
- Auditar el contrato de servicio que permita transparencia, mejora en la comunicación, los procesos, los controles internos del servicio.

3.7. Implementación del modelo de seguridad

De acuerdo a la plataforma de almacenamiento en la nube que ha sido considerado como base en el Capítulo II, las directrices de implementación del modelo de seguridad señalado en el ítem 3.6, y los siguientes requerimientos del sistema:

Tabla 1-3 Requerimientos del sistema - Nextcloud

Plataforma	Opciones
Sistema Operativo	• Ubuntu 18.04 LTS (recomendado) • Red Hat Enterprise Linux 7 (recomendado) • Debian 8 (Jessie), 9 (Stretch) • SUSE Linux Enterprise Server 11 with SP3 & 12 • openSUSE Leap 42.1+ • CentOS 7
Base de Datos	• MySQL 5.x or MariaDB 5.5+ (recomendado) • Oracle Database 11g (solo como parte de una suscripción empresarial) • PostgreSQL 9.5/9.6/10 • SQLite (solo recomendado para pruebas e instancias mínimas)
Servidor Web	✓ Apache 2.4 with mod_php or php-fpm (recomendado) ✓ nginx with php-fpm
PHP Runtime	• 7.1 • 7.2 (recomendado • 7.3 (recomendado)

Realizado por: Tenelema Esthela, 2019

Se establece los componentes a emplear en la implementación base de la plataforma de almacenamiento en la nube:

- ✓ Virtual Box 6.0
- ✓ CentOS 7.5
- ✓ PostgreSQL 9.5
- ✓ Apache 2.4
- ✓ PHP 7.2
- ✓ Paquete de instalación de Nextcloud.

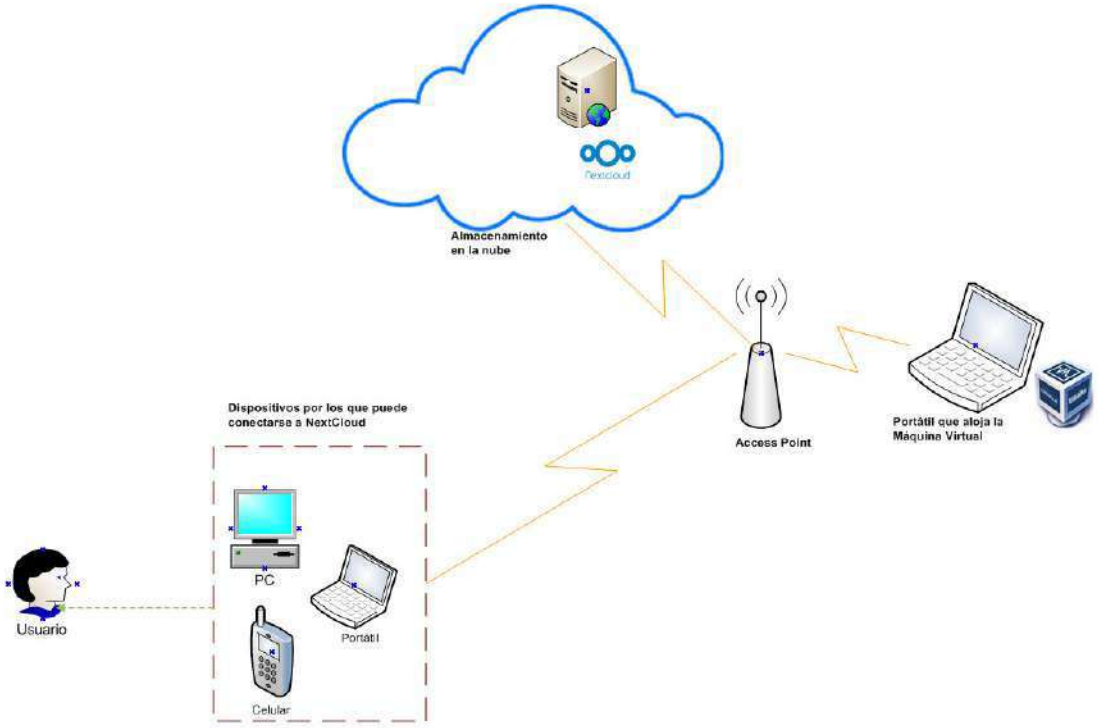


Figura 2 -3 Diagrama base de la plataforma de almacenamiento en la nube

Realizado por: Tenelema Esthela, 2019

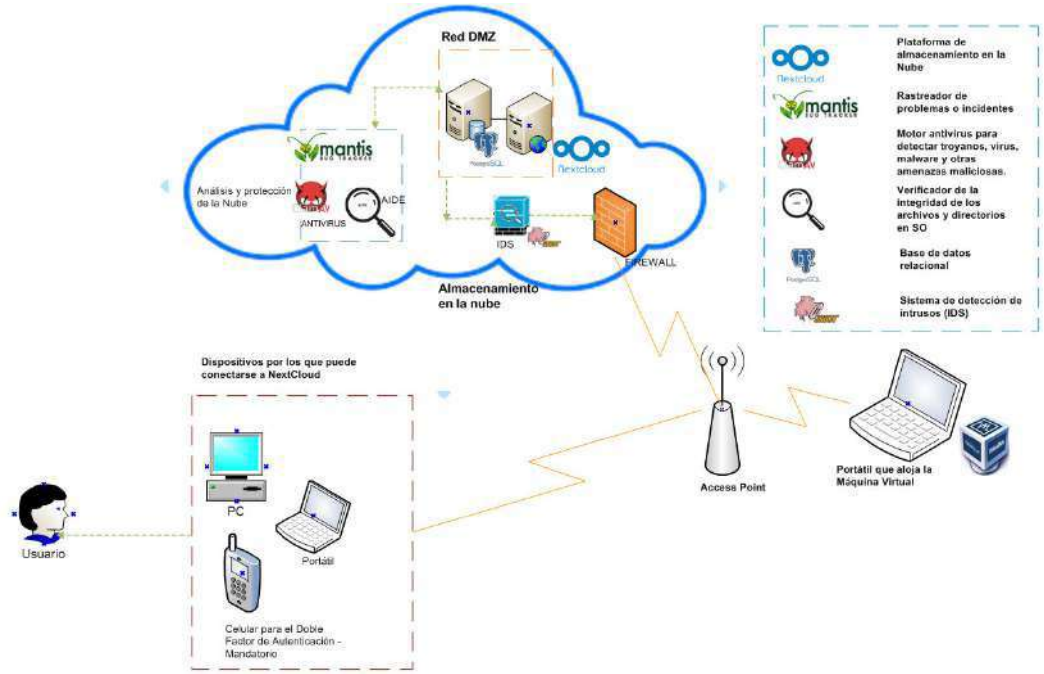


Figura 3 -3 Diagrama con el modelo de seguridad en la plataforma de almacenamiento en la nube

Realizado por: Tenelema Esthela, 2019

- **Primer Control del Modelo de seguridad:**

Nombre: Protección de la Plataforma de Virtualización

Implementación: Como protección del entorno virtual en el cual se encuentra alojada la plataforma de almacenamiento en la nube, se cifra el disco de la máquina virtual que utiliza un algoritmo de cifrado simétrico AES, y clave de 256 bits como se muestra en la Figura 4-3 y 5-3:

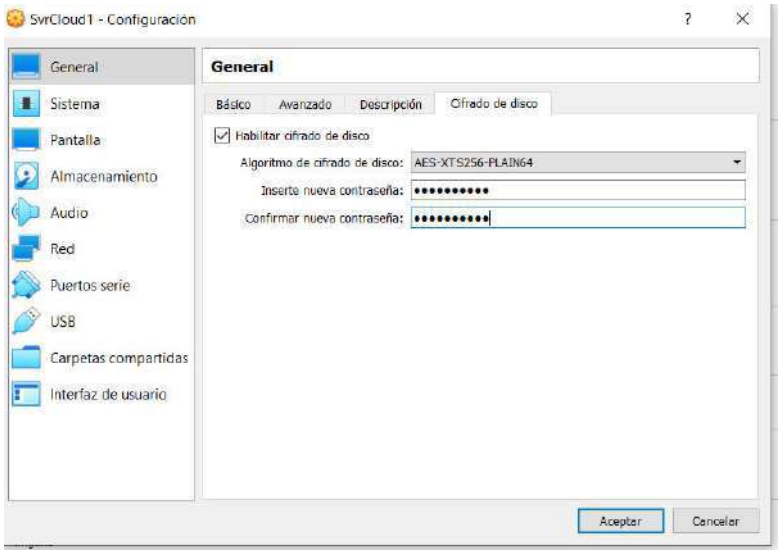


Figura 4 -3 Habilitación cifrado de disco VM

Realizado por: Tenelema Esthela, 2019

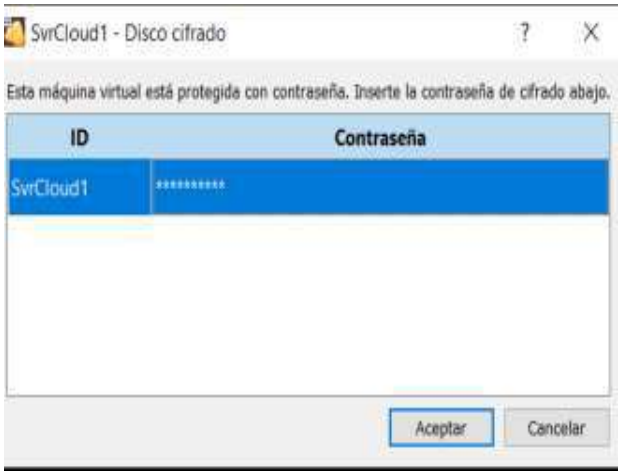


Figura 5-3 Solicitud de clave de cifrado de disco de la VM

Realizado por: Tenelema Esthela, 2019

- **Segundo Control del Modelo de seguridad:**

Nombre: Protección del entorno de almacenamiento en la nube

Implementación: Como protección del entorno de almacenamiento en la nube se crea una zona desmilitarizada (dmz) a nivel de firewall del sistema operativo (Centos 7), el cual brindará un acceso público con restricción a la red interna:

```
[root@cloudmsc ~]# sudo firewall-cmd --set-default-zone=dmz
success
```

Figura 6-3 Activación zona dmz a nivel del firewall
Realizado por: Tenelema Esthela, 2019

Se habilita el servicio https en la zona dmz mediante el siguiente comando:

sudo firewall-cmd --zone=dmz --permanent --add-service=https

Se establece un mecanismo de seguridad de control de acceso obligatorio (MAC) implementado en el kernel para protección de la data de la plataforma de almacenamiento en la nube (políticas en SELinux).

```
semanage fcontext -a -t httpd_sys_rw_content_t '/ var / www / html / nextcloud / data'
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/config(/.*)?'
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/apps(/.*)?'
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/3rdparty(/.*)?'
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/.htaccess'
semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/.user.ini'
```

Figura 7-3 Mecanismo SELinux a nivel de la plataforma de almacenamiento en la nube
Realizado por: Tenelema Esthela, 2019

Instalación y configuración de un IDS: En este caso se instala Snort que es un Sistema de Detección de Intrusos potente basado en red (IDSN) de código abierto, con reglas y filtros para un análisis de posibles amenazas a la infraestructura de almacenamiento en la nube:

```
[root@cloudmsc snort]# snort -A console -c /etc/snort/snort.conf -D
[root@cloudmsc snort]#
```

Figura 8-3 Configuración de snort para el análisis de vulnerabilidades
Realizado por: Tenelema Esthela, 2019

- **Tercer Control del Modelo de seguridad:**

Nombre: Protección contra Malware

Implementación: Se instala el antivirus **clamav** en el SO Centos, que aloja la plataforma de almacenamiento en la nube, ya que es un excelente analizador y obstructor de *malware*.

* Se actualiza la base de antivirus para prevenir ataques nuevos.

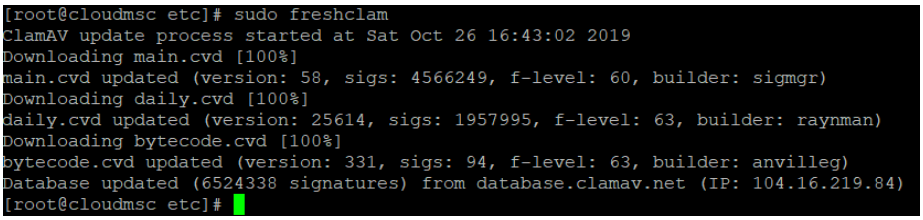


Figura 9 -3 Actualización de base de datos clamav
Realizado por: Tenelema Esthela, 2019

Se corre en segundo plano un análisis a las 23:59, como se presenta a continuación:

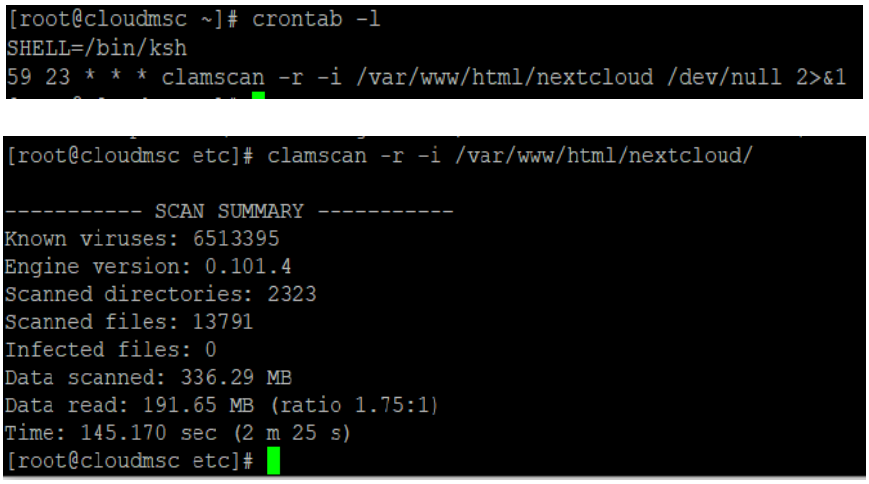


Figura 10-3 Ejecución en segundo plano del análisis de posibles virus
Realizado por: Tenelema Esthela, 2019

- **Cuarto Control del Modelo de seguridad:**

Nombre: Integridad de la Base de Datos

Implementación: Se crea un script para copia de seguridad incremental de la base de datos como se muestra:

```
[root@cloudmsc ~]# more /etc/backup.sh
#!/bin/bash
# vars
backups_path="/var/lib/pgsql/backups"
database="nextclouddb"
current_date_time="'date +%Y%m%d%H%M%S'";
# dump
pg_dump $database > $backups_path/$current_date_time.sql;
# get size of dump
size="'wc -c $backups_path/$current_date_time.sql'";
# get oldest backup
first_backup="'ls $backups_path | sort -n | head -1'"
echo 'first backup '$first_backup
# get size of oldest backup
size_first="'wc -c $backups_path/$first_backup'"
echo 'size_first '$size_first
# get backups count
backups_count="'find  $backups_path/*.sql -type f | wc -l'"
echo 'backups_count '$backups_count
# printing subject for email
echo 'Subject:'$size >  $backups_path/$current_date_time.txt
# condition for remove if there is more than 4 backups
if [ $backups_count -ge 5 ] ; then
 echo 'Greather than 5'
# removing backup
 rm $backups_path/$first_backup
 first_text="'ls $backups_path | sort -n | head -1'"
# removing text of backup
 rm $backups_path/$first_text
# printing body explaining removed backup
 printf "\nArchivo borrado: "$first_backup >>  $backups_path/$current_date_time.
txt
 printf "\nPeso: "$size_first >>  $backups_path/$current_date_time.txt
fi
```

Figura 11-3 Script para respaldo de la base de datos
Realizado por: Tenelema Esthela, 2019

Nota: Se asigna la ejecución del script como una tarea en segundo plano

```
[root@cloudmsc ~]# crontab -l
SHELL=/bin/ksh
00 22 * * * clamscan -r -i /var/www/html/nextcloud /dev/null 2>&1
00 23 * * * root /etc/backup.sh
0 0 * * * root /usr/sbin/aide --check
```

Figura 12-3 Ejecución en segundo plano de respaldo de la base de datos
Realizado por: Tenelema Esthela, 2019

- **Quinto Control del Modelo de seguridad:**

Nombre: Monitor de integridad de archivos

Implementación: Después del análisis de los diferentes monitores de integridad de archivos, se escoge, instala y configura **aide;** cuya función principal es permite de forma rápida y sencilla la detección de intrusos que puedan manipular los archivos o directorios monitorizados, como se muestra a continuación:

```
Instalado:
  aide.x86_64 0:0.15.1-13.el7

¡Listo!
[root@cloudmsc ~]#
```

Figura 13-3 Instalación de aide
Realizado por: Tenelema Esthela, 2019

Pruebas utilizando aide:

Escenario1: Sin cambios en la infraestructura.

```
[root@cloudmsc aide]# aide --check
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2019-10-27 18:58:51

Summary:
  Total number of files:        185928
  Added files:                  0
  Removed files:                0
  Changed files:                2


---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /etc/cups/subscriptions.conf
changed: /etc/cups/subscriptions.conf.O

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------


File: /etc/cups/subscriptions.conf
 SHA256   : G+gbAnJ5A8bYG/E29AjzTOVcKVDfN1S1 , SyJ1kqv8g3Z9H3wHPiCUHW55bcXgiGlH

File: /etc/cups/subscriptions.conf.O
 SHA256   : c7sSZW4Z3z6vdHQfGlBVl3LaQ+JS5mFN , G+gbAnJ5A8bYG/E29AjzTOVcKVDfN1S1
[root@cloudmsc aide]#
```

Figura 14-3 Chequeo mediante aide a nivel del sistema operativo
Realizado por: Tenelema Esthela, 2019

Escenario2: Con cambios en la infraestructura (añadiendo un archivo).

```
File: /etc/cups/subscriptions.conf
 SHA256   : G+gbAnJ5A8bYG/E29AjzTOVcKVDfN1S1 , SyJ1kqv8g3Z9H3wHPiCUHW55bcXgiGlH

File: /etc/cups/subscriptions.conf.O
 SHA256   : c7sSZW4Z3z6vdHQfGlBVl3LaQ+JS5mFN , G+gbAnJ5A8bYG/E29AjzTOVcKVDfN1S1
[root@cloudmsc aide]# touch /usr/sbin/testbinary
[root@cloudmsc aide]# aide --check
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2019-10-27 19:03:09

Summary:
  Total number of files:        185930
  Added files:                  2
  Removed files:                0
  Changed files:                2


---------------------------------------------------
Added files:
---------------------------------------------------

added: /sbin/testbinary
added: /usr/sbin/testbinary

---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /etc/cups/subscriptions.conf
changed: /etc/cups/subscriptions.conf.O

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------


File: /etc/cups/subscriptions.conf
 SHA256   : G+gbAnJ5A8bYG/E29AjzTOVcKVDfN1S1 , SyJ1kqv8g3Z9H3wHPiCUHW55bcXgiGlH

File: /etc/cups/subscriptions.conf.O
 SHA256   : c7sSZW4Z3z6vdHQfGlBVl3LaQ+JS5mFN , G+gbAnJ5A8bYG/E29AjzTOVcKVDfN1S1
```

Figura 15-3 Dos archivos añadidos y modificados que lo detecto aide
Realizado por: Tenelema Esthela, 2019

- **Sexto Control del Modelo de seguridad:**

Nombre: Planeación de Respuesta a Incidentes Cibernéticos

Implementación: De acuerdo a lo planteado en el control, se implementa la herramienta Mantis Bug Tracker (uno de los más populares sistemas de seguimiento de problemas) para gestionar tareas o incidencias que se presenten en la plataforma de almacenamiento en la nube como se presenta a continuación:

Figura 16-3 Inicio de sesión de Mantis Bug Tracker
Realizado por: Tenelema Esthela, 2019

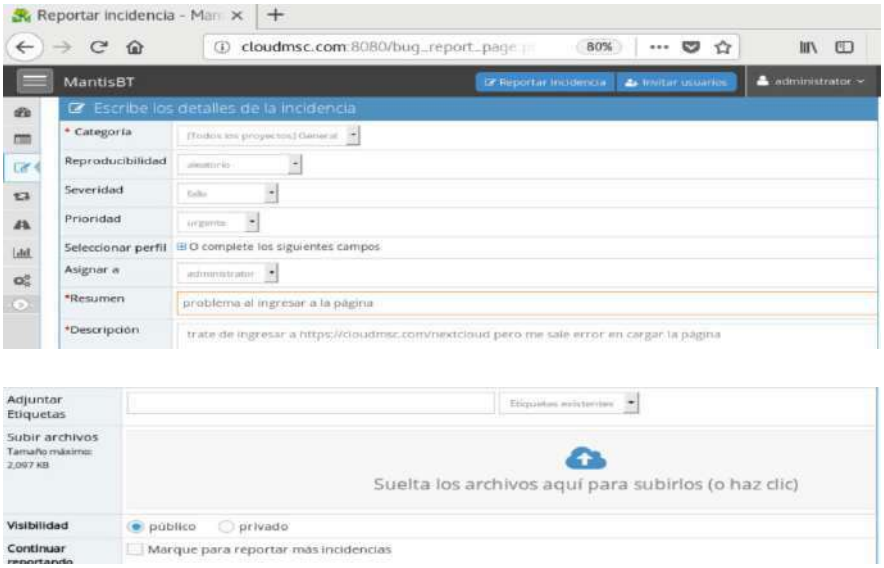


Figura 17-3 Creación de un incidente en Mantis Bug Tracker
Realizado por: Tenelema Esthela, 2019

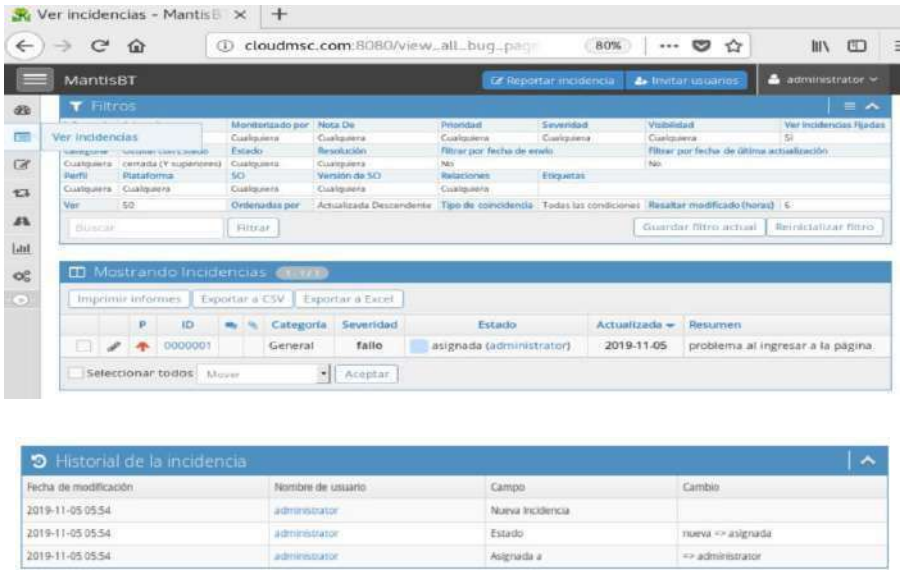


Figura 18-3 Seguimiento al incidente reportado en Mantis Bug Tracker
Realizado por: Tenelema Esthela, 2019

Nota: El usuario tiene disponible el manual para el correcto uso de la herramienta de incidentes (en la página inicial de nextcloud).

- **Séptimo Control del Modelo de seguridad:**

Nombre: Pruebas de Penetración

Implementación: Se utiliza para esta ocasión la aplicación **Metasploit framework** de Kali Linux, para análisis de vulnerabilidades de la plataforma de almacenamiento en la nube, como se muestra a continuación:

- Identificación de la IP del almacenamiento en la nube:

```
[root@cloudmsc ~]# ifconfig
br-fb3d79ee8ff3: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:23:50:52:b2  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:6b:a8:4a:af  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.30  netmask 255.255.255.192  broadcast 192.168.1.63
        inet6 fe80::a00:27ff:fe28:f41f  prefixlen 64  scopeid 0x20<link>
        inet6 2800:370:134:23d0:a00:27ff:fe28:f41f  prefixlen 64  scopeid 0x0
```

Figura 19-3 Identificación de IP (almacenamiento en la nube)
Realizado por: Tenelema Esthela, 2019

- Con esa información se procede al análisis de las vulnerabilidades:

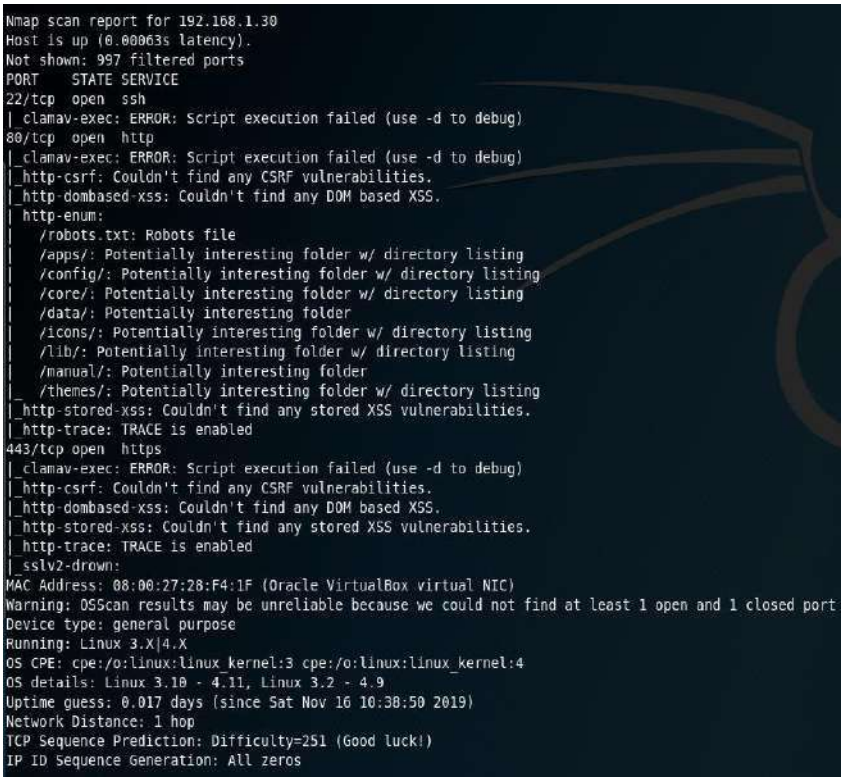


Figura 20-3 Análisis de vulnerabilidades con Metasploit
Realizado por: Tenelema Esthela, 2019

- Con la información provista en el escaneo de vulnerabilidades, el siguiente paso es corregir la vulnerabilidad de las carpetas que son visibles o fáciles de acceder desde la web:

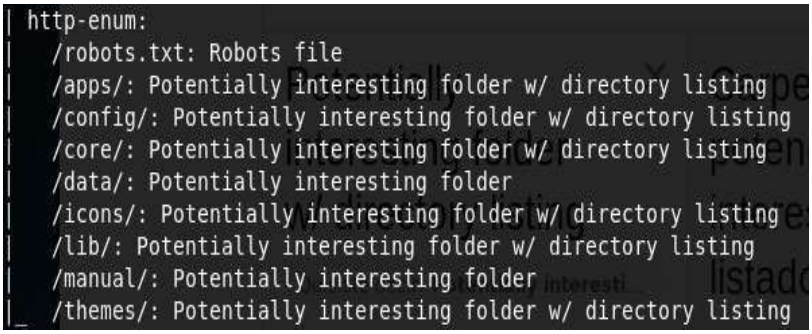


Figura 21-3 Directorios visibles y fáciles de vulnerar
Realizado por: Tenelema Esthela, 2019

Nota: La configuración predeterminada o mal configurada en los servidores web puede provocar una serie de problemas que pueden ayudar a los piratas informáticos malintencionados a crear un ataque de piratería. Un problema común del servidor web es el listado de directorios

- Se corrige con la siguiente línea en el archivo de configuración del apache:

```
rectory "/var/www/html">
 #
 # Possible values for the Options directive are "None", "All",
 # or any combination of:
 #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
 #
 # Note that "MultiViews" must be named *explicitly* --- "Options All"
 # doesn't give it to you.
 #
 # The Options directive is both complicated and important.  Please see
 # http://httpd.apache.org/docs/2.4/mod/core.html#options
 # for more information.
 #
 Options FollowSymLinks
```

Figura 22-3 Corrección del archivo de configuración
Realizado por: Tenelema Esthela, 2019

- Se reinicia el apache y se procede a realizar un nuevo análisis:

```
Nmap scan report for 192.168.1.30
Host is up (0.00069s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp  open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /robots.txt: Robots file
|   /icons/: Potentially interesting folder w/ directory listing
|_  /manual/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
443/tcp open  https
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /icons/: Potentially interesting folder w/ directory listing
|_  /manual/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_sslv2-drown:
MAC Address: 08:00:27:28:F4:1F (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
Uptime guess: 0.053 days (since Sat Nov 16 10:38:51 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
```

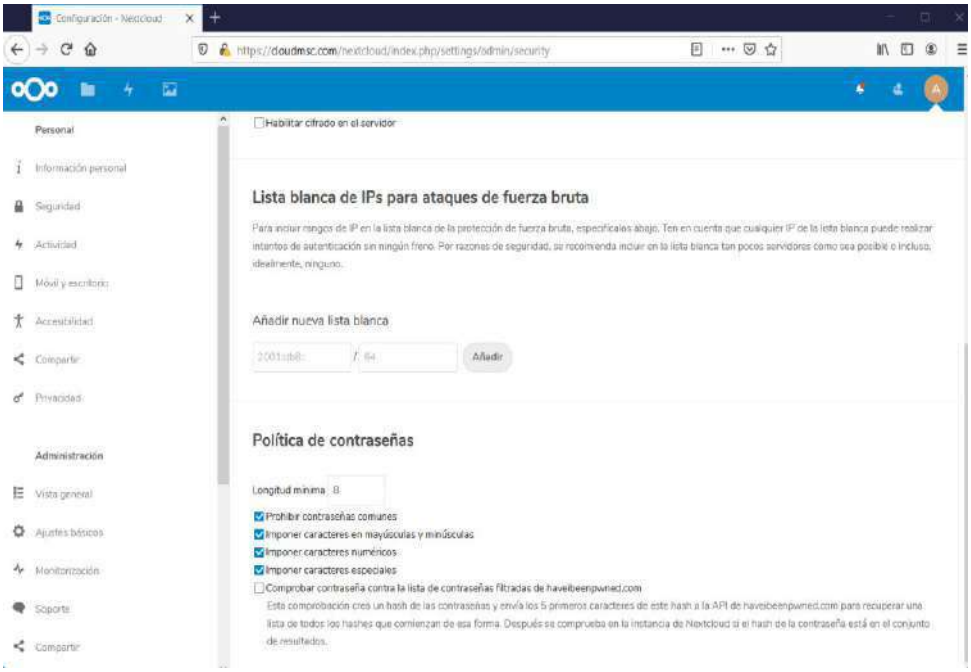
Figura 23-3 Nuevo análisis de vulnerabilidades
Realizado por: Tenelema Esthela, 2019

Nota: Como se muestra en la imagen anterior los directorios que son parte del servidor apache, se encuentra protegidos y no se presenta como vulnerabilidad

- **Octavo Control del Modelo de seguridad:**

Nombre: Política de Contraseñas

Implementación: Se configura la política de contraseña en la plataforma de almacenamiento en la nube como se muestra:



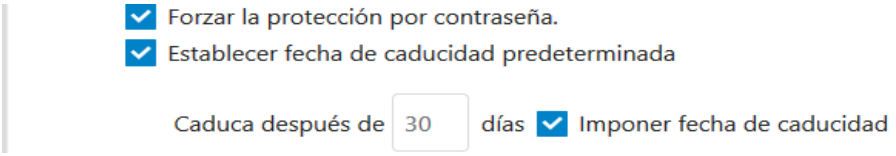


Figura 24-3 Habilitación de políticas de contraseñas en nextcloud
Realizado por: Tenelema Esthela, 2019

Nota: Con la configuración realizada en el próximo inicio de sesión, la clave o contraseña del usuario deberá cumplir con las directrices señalada en la política.

- **Noveno Control del Modelo de seguridad:**

Nombre: Fortalecimiento del Sistema
Implementación: Mediante el método de doble factor de autenticación, se procede a fortalecer la conexión remota del cliente **ssh** (herramienta más usada para la gestión de sistemas basados en Linux), como se muestra a continuación:

1. Instalar Google Authenticator

```
Instalado:
  google-authenticator.x86_64 0:1.04-1.el7
```

Figura 25-3 Instalación de Google Authenticator
Realizado por: Tenelema Esthela, 2019

2. Realizar la lectura del QR desde el teléfono:

Figura 26-3 Lectura de QR para los clientes OTP
Realizado por: Tenelema Esthela, 2019

3. Validación de la autenticación remota hacia el servidor que aloja la plataforma de almacenamiento en la nube:

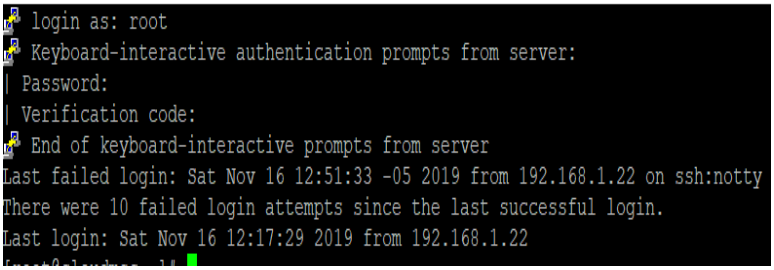


Figura 27-3 Autenticación ssh mediante dos factores
Realizado por: Tenelema Esthela, 2019

✓ Se restringe la modificación de los directorios que forman parte de la plataforma de almacenamiento en la nube (realizar archivos inmutables):

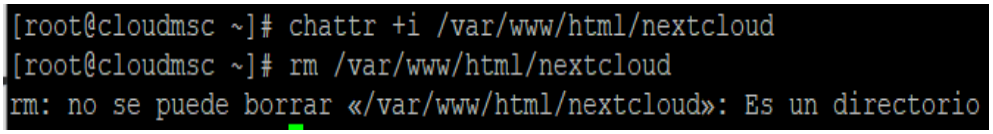


Figura 28-3 Comando para convertir archivos en inmutables
Realizado por: Tenelema Esthela, 2019

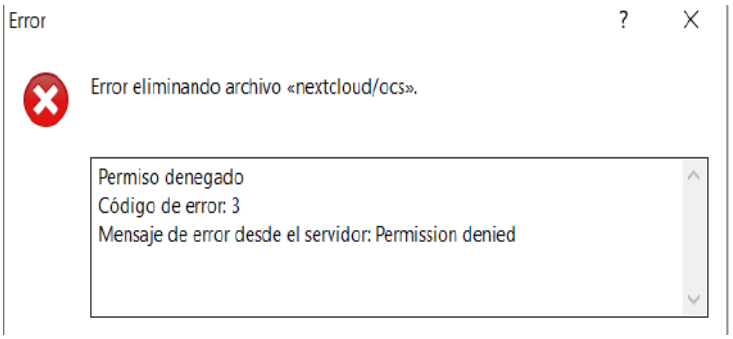


Figura 29-3 Error al tratar de modificar un archivo inmutable
Realizado por: Tenelema Esthela, 2019

Nota: Los archivos inmutables no pueden sobrescribirse por ningún usuario, incluso el root.

- **Décimo Control del Modelo de seguridad:**

Nombre: Autenticación de Múltiples Factores

Implementación: Se implementa el doble factor de autenticación en la plataforma de almacenamiento en la nube (Primer factor: mediante una clave que contempla políticas de seguridad; segundo factor con OTP de Google Authenticator)

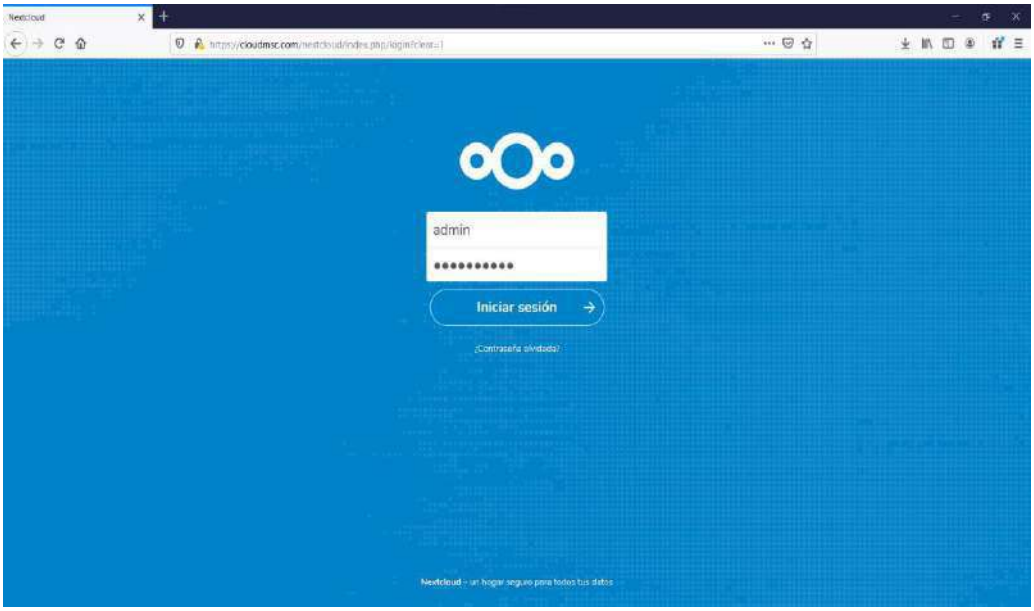


Figura 30-3 Inicio de sesión con el primer factor de autenticación
Realizado por: Tenelema Esthela, 2019

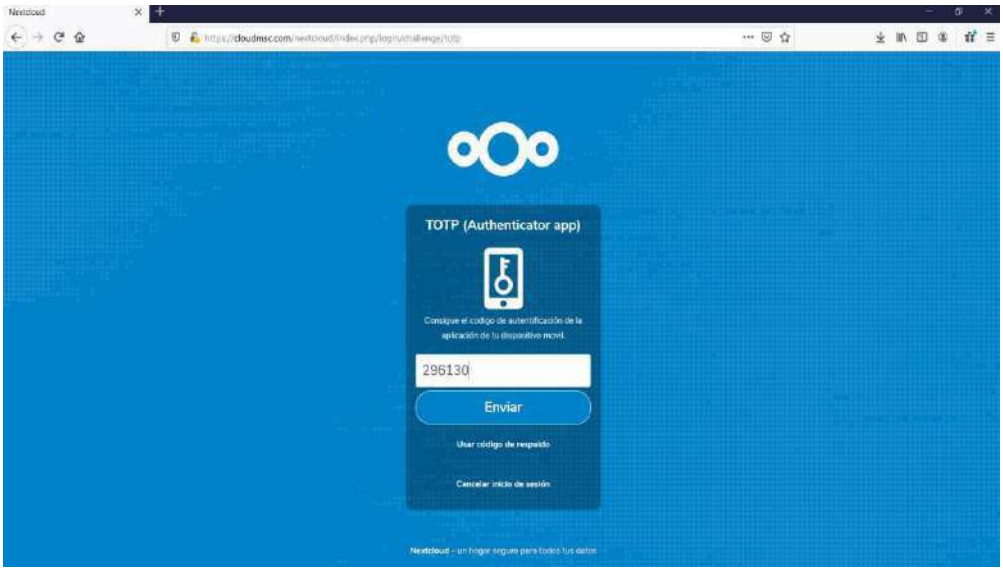


Figura 31-3 Inicio de sesión con el segundo factor de autenticación
Realizado por: Tenelema Esthela, 2019

- **Onceavo Control del Modelo de seguridad:**

Nombre: Compromisos de las partes

Implementación: Se establece un contrato de servicio (cliente-proveedor) para delinear acuerdos sobre la utilización de la plataforma de almacenamiento en la nube mediante una aplicación dinámica propia de la plataforma llamado **Terms of service**:

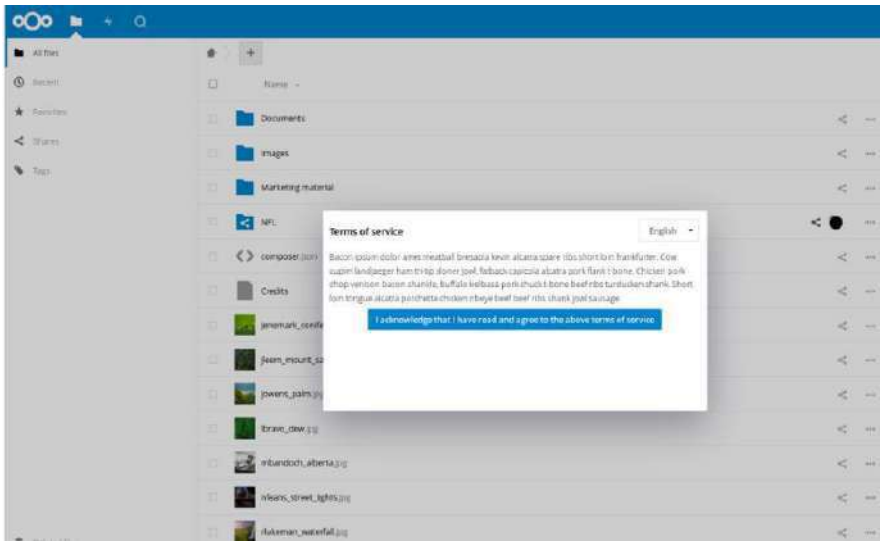


Figura 32-3 Aplicación Terns of service
Realizado por: Tenelema Esthela, 2019

3.8. Definición de los escenarios de prueba

Se establece escenarios de pruebas para análisis de vulnerabilidades de almacenamiento en la nube con base en las normas ISO 27017 y 27018:

- **Escenario 1**

En el primer escenario se utilizará un Prototipo I, que contempla las directrices del modelo de seguridad en la nube propuesto (se encuentra ya implementado en el ítem 3.7 de este capítulo).

- **Escenario 2**

En el segundo escenario se utilizará el Prototipo II, que no tiene o contempla las directrices de implementación del modelo de seguridad en la nube propuesto.

Resultados

Consecutivamente se realizan las pruebas en los dos escenarios planteados con la finalidad de demostrar la mejora de la seguridad de acuerdo al modelo de seguridad propuesto en este capítulo, para lo cual se compararán los resultados obtenidos entre:

- Prototipo I que incluye el modelo de seguridad para ambientes de almacenamiento en la nube.
- Prototipo II que no incluye un modelo de seguridad para ambientes de almacenamiento en la nube.

3.9. Hipótesis

¿La implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube, mejorará el nivel de seguridad de la misma?

3.9.1. Determinación de variables

De acuerdo a la hipótesis planteada, se determinan las siguientes variables:

- Modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube.

- Seguridad de la información

3.9.2. Operacionalización conceptual

La Tabla 2-3, muestra la operacionalización conceptual de las variables determinadas.

Tabla 2-3 Operacionalización conceptual

VARIABLE	TIPO	DEFINICIÓN
Implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube.	Independiente	• Modelo de seguridad es aquel que se fundamenta en lineamientos otorgados por las normas y estándares internacionales del área; lo cual permite ser una base para cualquier tipo de organización. • La mitigación de vulnerabilidades es un proceso continuo y consciente que ayuda a contrarrestar las debilidades de TI. • El ambiente de almacenamiento en la nube es un servicio que permiten guardar información y trabajarla de forma colaborativa.
Seguridad de la información	Dependiente	• La seguridad de la información se relaciona con el nivel de protección de: la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización.

Realizado por: Tenelema Esthela, 2019

3.9.3. *Operacionalización metodológica*

La Tabla 3-3, muestra la operacionalización metodológica de las variables determinadas.

Tabla 3-3 Operacionalización metodológica

VARIABLE	INDICADOR	TÉCNICA	INSTRUMENTO/ FUENTE
Implementación de un modelo de seguridad en ambientes de almacenamiento en la nube.	- Complejidad - Facilidad de diseño e implementación - Tiempo de diseño e implementación - Recursos necesarios	- Búsqueda de información - Pruebas - Observación	- Matrices de control de riesgo - Encuestas - Entrevistas
Seguridad de la información	- Número de vulnerabilidades - Número de riesgos mitigados. - Número de Logs encontrados	- Pruebas - Observación - Análisis	- Matrices de control de riesgo - Kali Linux - Openvas

Realizado por: Tenelema Esthela, 2019

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

En este Capítulo, se desarrollan las pruebas en los escenarios establecidos, se analizan, comparan los resultados obtenidos y se comprueba la hipótesis planteada.

4.1. Desarrollo de las pruebas

4.1.1. Indicadores de la variable independiente

Con base en los siguientes indicadores:

- **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.

Se realiza un análisis y calificación del Prototipo I y II implementados con una escala de:

Tabla 1-4 Escala de calificación de la complejidad

COMPLEJIDAD	CÓDIGO
Muy Poco	5
Poco	4
Bastante	3
Mucho	2
Demasiado	1

Realizado por: Tenelema Esthela, 2019

Tabla 2-4 Escala de calificación de facilidad de diseño e implementación

FACILIDAD DE DISEÑO E IMPLEMENTACIÓN	CÓDIGO
Muy Poco	5
Poco	4
Bastante	3
Mucho	2
Demasiado	1

Realizado por: Tenelema Esthela, 2019

Tabla 3-4 Escala de calificación de tiempo de diseño e implementación (días)

TIEMPO DE DISEÑO E IMPLEMENTACIÓN (DÍAS)	CÓDIGO
1 a 5	5
6 a 10	4
11 a 15	3
16 a 20	2
>= 20	1

Realizado por: Tenelema Esthela, 2019

Tabla 5-4 Escala de calificación recursos necesarios

RECURSOS NECESARIOS	CÓDIGO
3 a 5	5
6 a 8	4
9 a 11	3
12 a 14	2
>=15	1

Realizado por: Tenelema Esthela, 2019

Con las escalas ya definidas para cada uno de los indicadores, se evalúa los controles de seguridad que forman parte de la variable independiente "Modelo de seguridad en ambientes de almacenamiento en la nube" que se muestra en la Tabla 6-4:

Tabla 6-4 Evaluación Prototipo I y II respecto a la variable independiente

Nº Ítem	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**

Realizado por: Tenelema Esthela, 2019

Gráfico 1-4 Variable independiente en relación al Prototipo I
Realizado por: Tenelema Esthela, 2019

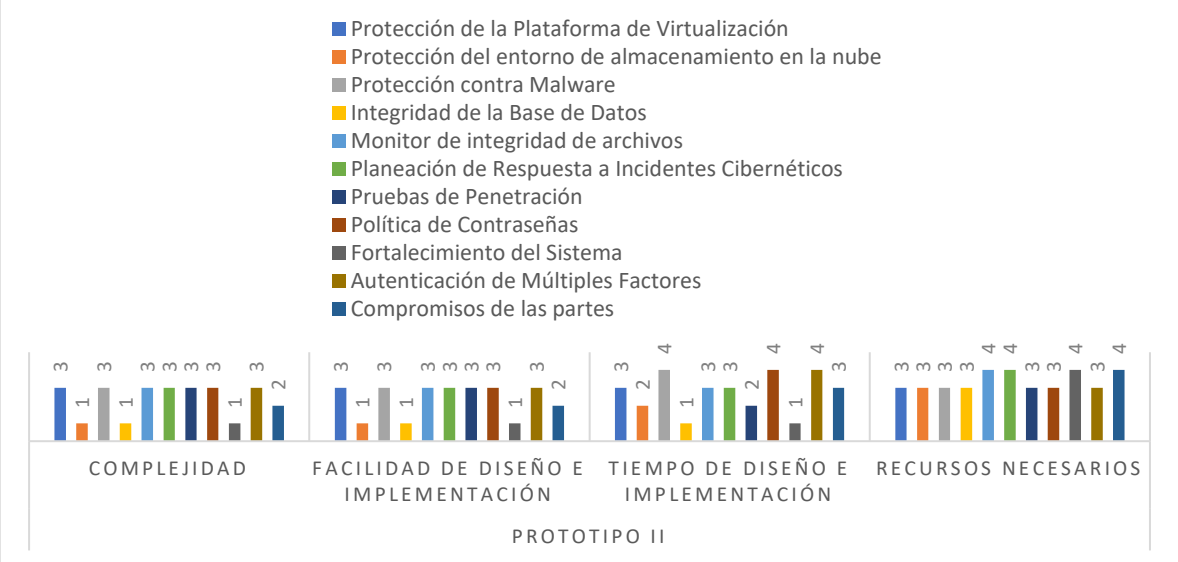


Gráfico 2-4 Variable independiente en relación al Prototipo II
Realizado por: Tenelema Esthela, 2019

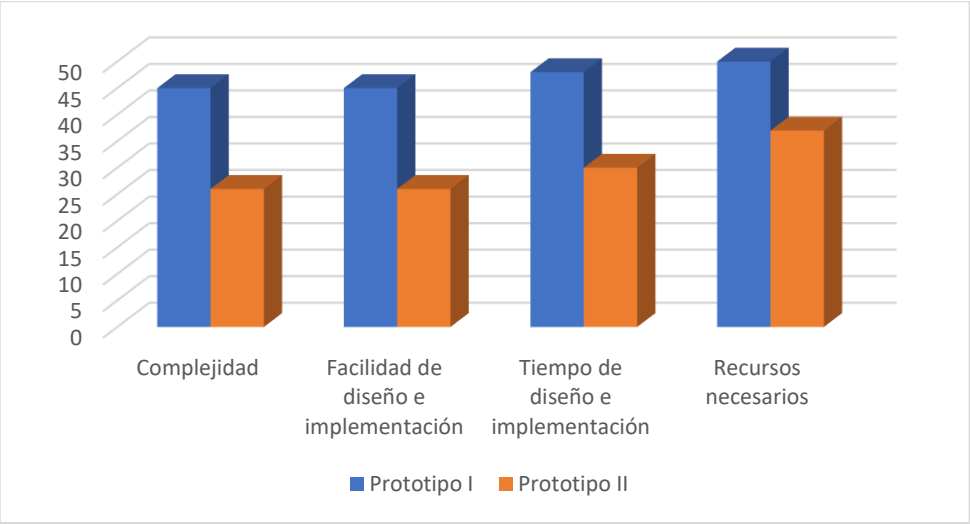


Gráfico 3-4 Variable independiente en relación a los Prototipos I y II
Realizado por: Tenelema Esthela, 2019

Interpretación de los indicadores (variable independiente)

- **Complejidad**

De acuerdo a los datos que se muestran en el Gráfico 1-4 y 2-4, se puede denotar que el nivel de complejidad en relación a la variable del Prototipo I a la II, es poco. 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**

De acuerdo a los datos que se muestran en el Gráfico 1-4 y 2-4, se puede denotar que la facilidad en el diseño e implementación en 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**

De acuerdo a los datos que se muestran en el Gráfico 1-4 y 2-4, se puede denotar que el tiempo de diseño e implementación en relación a la variable del Prototipo I es muy 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**

De acuerdo a los datos que se muestran en el Gráfico 1-4 y 2-4, se puede denotar que los recursos necesarios en 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.

4.1.2. Indicadores de la variable dependiente

Con base en los siguientes indicadores:

- **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.

Se realiza un análisis y calificación del Prototipo I y II implementados, con ayuda de Kali Linux y su aplicación Greenbone que es un framework con una base de servicios y herramientas para la evaluación de vulnerabilidades. A demás, de ser un escáner que ejecuta las denominadas NVT (Network Vulnerability Tests), es decir, las pruebas de vulnerabilidades de red, conformadas por rutinas que comprueban la presencia de un problema de seguridad específico conocido o potencial en los sistemas, como se muestra en el Grafico 3-4 y 4-4.

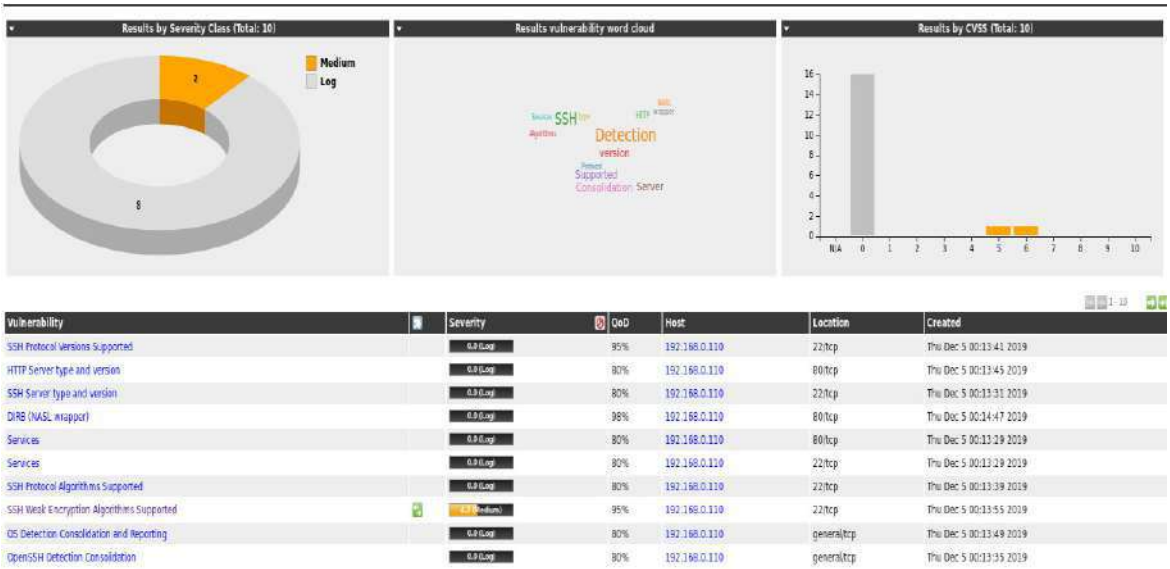
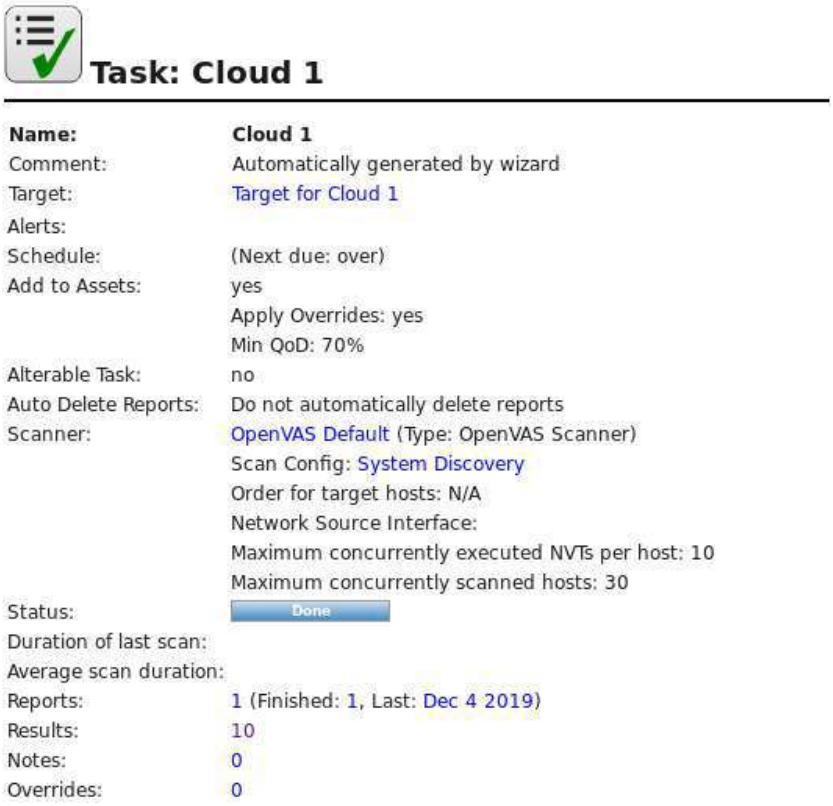


Gráfico 4-4 Análisis de vulnerabilidades por la herramienta Greenbone en el Prototipo I que considera el modelo de seguridad
Realizado por: Tenelema Esthela, 2019



Task: Cloud 1

Name:	**Cloud 1**
Comment:	Automatically generated by wizard
Target:	Target for Cloud 1
Alerts:	
Schedule:	(Next due: over)
Add to Assets:	yes
	Apply Overrides: yes
	Min QoD: 70%
Alterable Task:	no
Auto Delete Reports:	Do not automatically delete reports
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)
	Scan Config: System Discovery
	Order for target hosts: N/A
	Network Source Interface:
	Maximum concurrently executed NVTs per host: 10
	Maximum concurrently scanned hosts: 30
Status:	Done
Duration of last scan:	
Average scan duration:	
Reports:	1 (Finished: 1, Last: Dec 4 2019)
Results:	10
Notes:	0
Overrides:	0

Figura 1-4 Reporte de análisis de vulnerabilidades Prototipo I
Realizado por: Tenelema Esthela, 2019

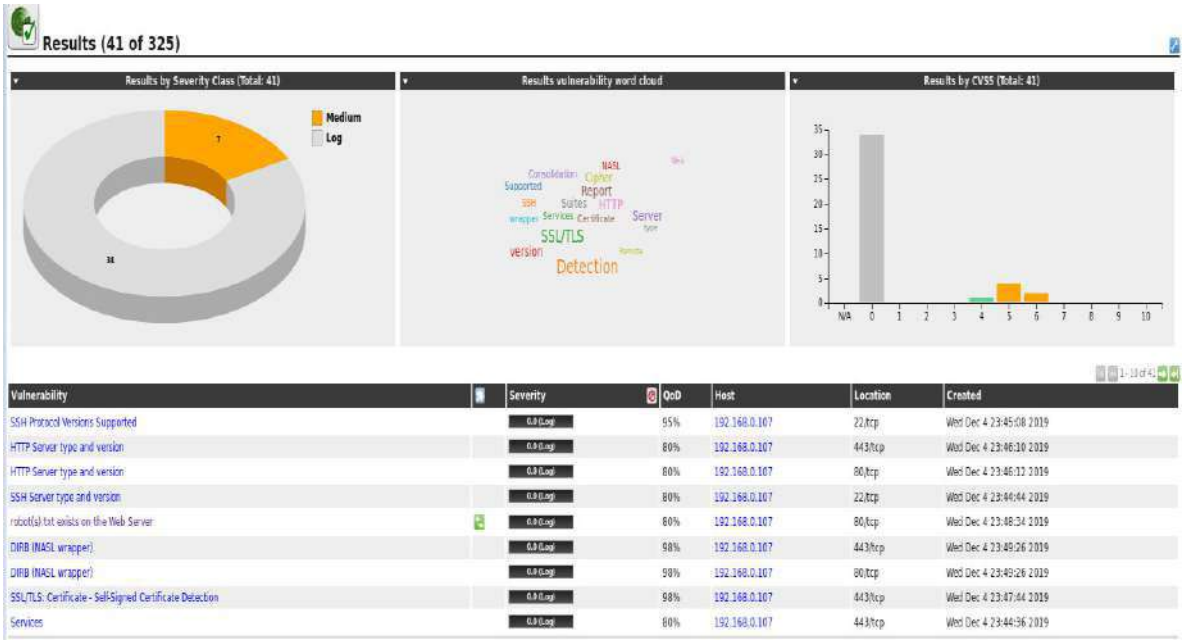


Gráfico 5-4 Análisis de vulnerabilidades por la herramienta Greenbone en el Prototipo II que no considera el modelo de seguridad
Realizado por: Tenelema Esthela, 2019

Figura 2-4 Reporte de análisis de vulnerabilidades Prototipo II
Realizado por: Tenelema Esthela, 2019

Tabla 7-4 Resultados de los indicadores de la variable dependiente

INDICADORES	PROTOTIPO I	PROTOTIPO II
Número de vulnerabilidades	10	41
Número de riesgos mitigados	2	7
Número de logs	8	34

Realizado por: Tenelema Esthela, 2019

4.1.2.a Escalas de calificación

Para realizar la comparación de los resultados obtenidos se utilizará la escala de Likert para cada uno de los indicadores de la variable independiente.

Indicador 1: Número de vulnerabilidades

Para medir el Indicador 1: Número de vulnerabilidades, se utilizará la escala mostrada en la Tabla 8-4.

Tabla 8-4 Tabla de escalas para el Indicador 1: Número de vulnerabilidades

NÚMERO DE VULNERABILIDADES	CÓDIGO
<=10	5
11 a 20	4
21 a 30	3
31 a 40	2
> 40	1

Realizado por: Tenelema Esthela, 2019

Indicador 2: Número de riesgos mitigados

Para medir el Indicador 2: Número de riesgos mitigados, se utilizará la escala mostrada en la Tabla 9-4.

Tabla 9-4 Tabla de escalas para el Indicador 2: Número de riesgos mitigados

NÚMERO DE RIESGOS MITIGADOS	CÓDIGO
<=2	5
3 a 4	4
5 a 6	3
7 a 8	2
> 8	1

Realizado por: Tenelema Esthela, 2019

Indicador 3: Número de logs

Para medir el Indicador 3: Número de riesgos mitigados, se utilizará la escala mostrada en la Tabla 10-4.

Tabla 10-4 Tabla de escalas para el Indicador 3: Número de logs

NÚMERO DE RIESGOS MITIGADOS	CÓDIGO
<=9	5
10 a 19	4
20 a 29	3
30 a 39	2
>= 40	1

Realizado por: Tenelema Esthela, 2019

4.1.3. Ponderación de indicadores

Los resultados obtenidos en las pruebas para cada Indicador en el punto 4.1.2 son cuantificados con las escalas definidas en el punto 4.1.2.1

4.1.3.a Indicador 1: Número de vulnerabilidades

Utilizando los valores promedios del Indicador 1: Número de vulnerabilidades, con cada prototipo se cuantifica los resultados de acuerdo a la escala definida, con lo que se obtiene los valores mostrados en la Tabla 11-4.

Tabla 11-4 Códigos del Indicador 1: Número de vulnerabilidades

No.	Indicador	Valor promedio		Código obtenido (de acuerdo a la escala)	
		Prototipo I	Prototipo II	Prototipo I	Prototipo II
1	Número de vulnerabilidades	10	41	5	1

Realizado por: Tenelema Esthela, 2019

En el Gráfico 6-4 se muestran los códigos obtenidos (de acuerdo a la escala) del Indicador.

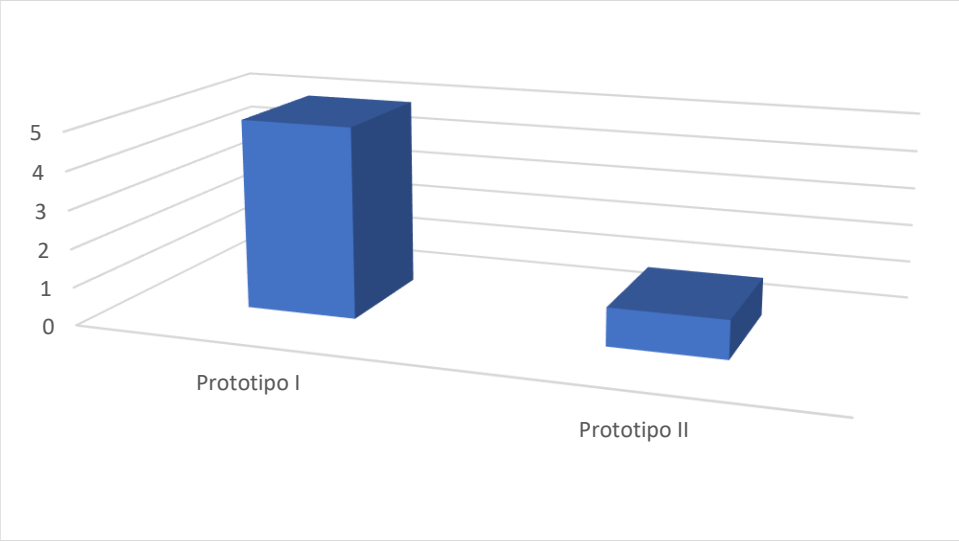


Gráfico 6-4 Resultados obtenidos (de acuerdo a la escala) del Indicador 1: Número de vulnerabilidades

Realizado por: Tenelema Esthela, 2019

4.1.3.b Indicador 2: Número de riesgos mitigados

Utilizando los valores promedios del Indicador 2: Número de riesgos mitigados, con cada prototipo se cuantifica los resultados de acuerdo a la escala definida, con lo que se obtiene los valores mostrados en la Tabla 12-4.

Tabla 12-4 Códigos del Indicador 2: Número de riesgos mitigados

No.	Indicador	Valor promedio		Código obtenido (de acuerdo a la escala)	
		Prototipo I	Prototipo II	Prototipo I	Prototipo II
1	Número de riesgos mitigados	2	7	5	2

Realizado por: Tenelema Esthela, 2019

En el Gráfico 7-4 se muestran los códigos obtenidos (de acuerdo a la escala) del Indicador.

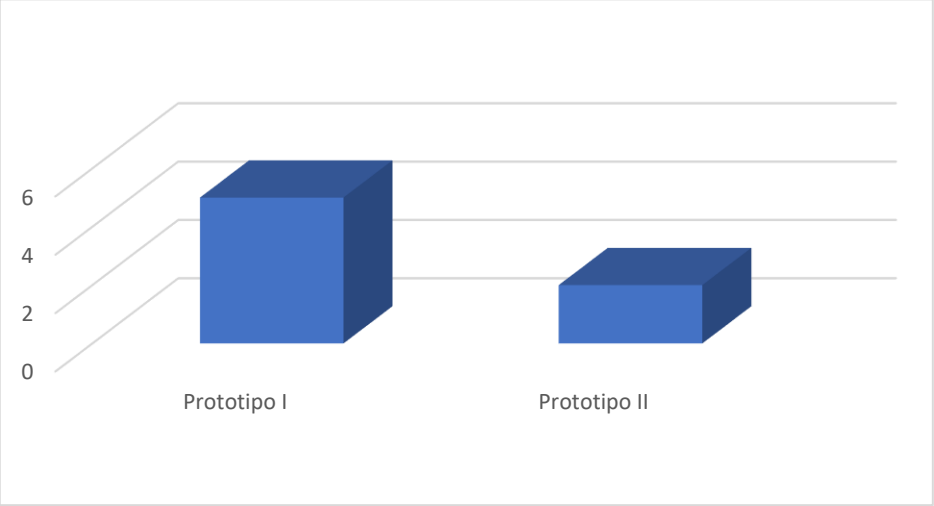


Gráfico 7-4 Resultados obtenidos (de acuerdo a la escala) del Indicador 2: Número de riesgos mitigados

Realizado por: Tenelema Esthela, 2019

4.1.3.c Indicador 3: Número de logs

Utilizando los valores promedios del Indicador 3: Número de logs, con cada prototipo se cuantifica los resultados de acuerdo a la escala definida, con lo que se obtiene los valores mostrados en la Tabla 13-4.

Tabla 13-4 Códigos del Indicador 3: Número de logs

No.	Indicador	Valor promedio		Código obtenido (de acuerdo a la escala)	
		Prototipo I	Prototipo II	Prototipo I	Prototipo II
1	Número de logs	8	34	5	2

Realizado por: Tenelema Esthela, 2019

En el Gráfico 7-4 se muestran los códigos obtenidos (de acuerdo a la escala) del Indicador.

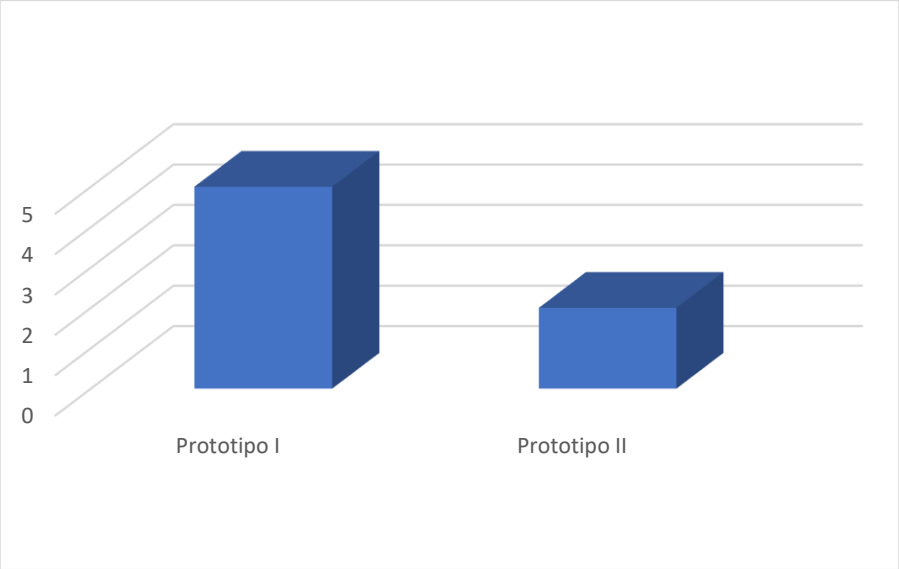


Gráfico 8-4 Resultados obtenidos (de acuerdo a la escala) del Indicador 3: Número de logs
Realizado por: Tenelema Esthela, 2019

4.2. Comprobación de hipótesis

La hipótesis definida en la presente investigación es: "La implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube, mejorará el nivel de seguridad de la misma"

Para la demostración de la hipótesis se utilizará la estadística descriptiva y la estadística inferencial, considerando con atenuantes:

- **Población:** número de vulnerabilidades
- **Muestra:** número de vulnerabilidades encontradas en base a la escala de Likert.

4.2.1. Estadística descriptiva

Para la comprobación de la hipótesis se utilizará la estadística descriptiva en la que se cuantifican los resultados obtenidos en las pruebas realizadas de cada uno de los indicadores definidos utilizando la escala de Likert, como se muestra en la Tabla 14-4.

Tabla 14-4. Resultados de indicadores

No.	Indicadores	Prototipo I	Prototipo II
1	Número de vulnerabilidades	5	1
2	Número de riesgos mitigados	5	2
3	Número de logs	5	2
	TOTAL	15	5

Realizado por: Tenelema Esthela, 2019

En el Gráfico 8-4 se muestran los resultados de la comparación realizada por cada uno de los indicadores.

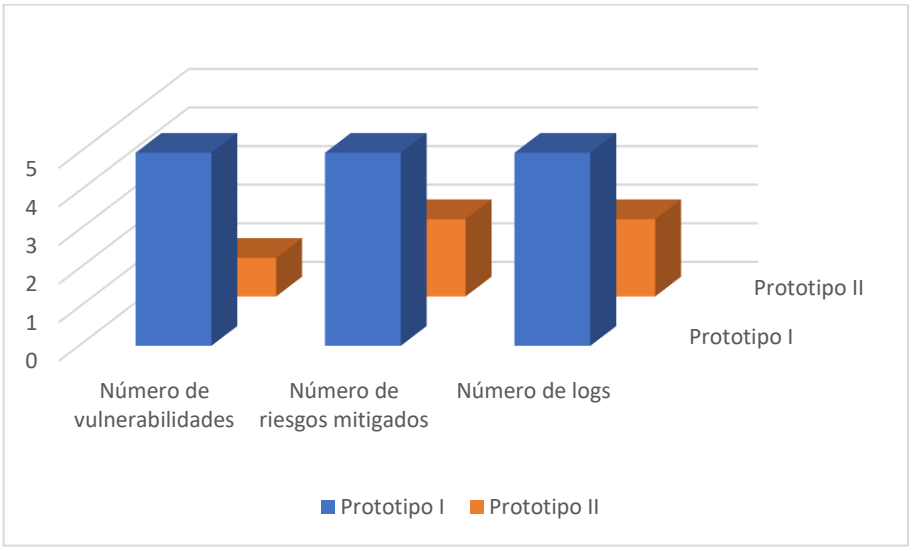


Gráfico 8-4 Resultados de la comparación por Indicador
Realizado por: Tenelema Esthela, 2019

En el Gráfico 9-4 se muestran los resultados totales de la comparación realizada por cada prototipo.

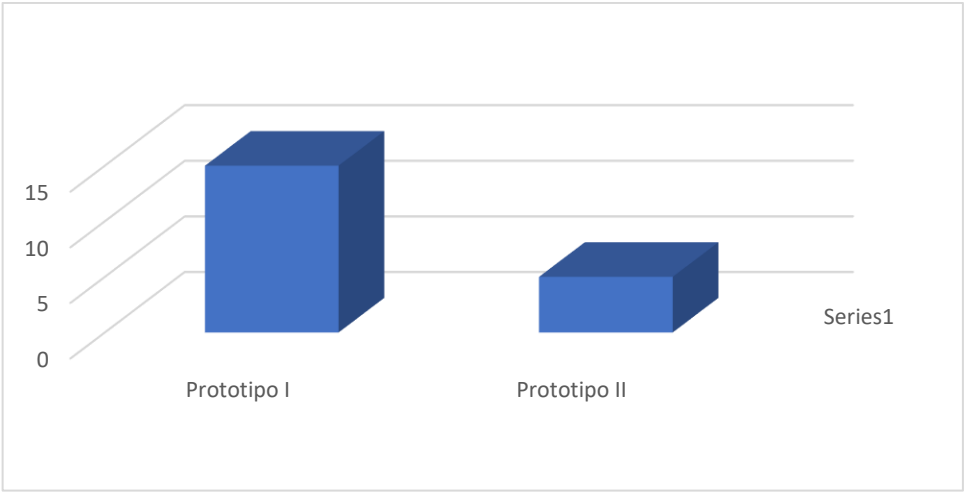


Gráfico 9-4 Resultados totales de la comparación
Realizado por: Tenelema Esthela, 2019

Se concluye que la implementación de un modelo de seguridad para almacenamiento en la nube implantado en el Prototipo I es más seguro en un 75% en comparación al Prototipo II que no la considera.

4.2.2. Estadística inferencial

Para la comprobación de la hipótesis de investigación se da los siguientes valores a la variable independiente X los siguientes valores:

X = Implementación del modelo de Seguridad
X_1 = Mejora la seguridad
X_2 = No mejora la seguridad

Los mismos en los que se comprobará 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 X^2, 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:** *La implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube,* ***mejorará el nivel de seguridad*** *de la misma.*
- **Ho:** *La implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambientes de almacenamiento en la nube,* ***no mejorará el nivel de seguridad*** *de la misma.*

La tabla de contingencia creada para el cálculo de chi cuadrado, se muestra en la Tabla 15-4, en la que se ubican las frecuencias observadas de cada Indicador.

Tabla 15-4 Tabla de contingencia de frecuencias observadas

	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**

Realizado por: Tenelema Esthela, 2019

La tabla de contingencia de frecuencias esperadas son 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.

$$fe = \frac{(total\_fil) * (total\_columna)}{N}$$

Dónde:

N: Número total de frecuencias observadas.

Aplicando la fórmula a los valores de la Tabla 15-4 se obtiene la tabla de contingencia de valores esperados, como se muestra en la Tabla 16-4.

Tabla 16-4 Tabla de contingencia de frecuencias esperadas

	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**

Realizado por: Tenelema Esthela, 2019

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

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

Dónde:

O: Frecuencia observada en cada celda

E: Frecuencia esperada en cada celda

En la Tabla 17-4 se calcula el valor de X^2

Tabla 17-4 Cálculo de X^2

			O	/E	O - E	$(O - E)^2$	$\frac{(O - E)2}{E}$
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 SEGURIDAD	PI	No mejora número de vulnerabilidades Prototipo I	0	0,75	-0,75	0,56	0,75
		No mejora número de riesgos mitigados Prototipo I	0	1,50	-1,50	2,25	1,50
		No mejora número de logs Prototipo I	0	1,50	-1,50	2,25	1,50
	PII	No mejora número de vulnerabilidades Prototipo II	1	0,25	0,75	0,56	2,25
		No mejora número de riesgos mitigados Prototipo II	2	0,50	1,50	2,25	4,50
		No mejora número de logs Prototipo II	2	0,50	1,50	2,25	4,50
							20,00

Realizado por: Tenelema Esthela, 2019

Interpretación

Para determinar si el valor de X^2 es o no significativo, se debe determinar los grados de libertad mediante la siguiente fórmula.

$$GI = (f - 1)(c - 1)$$

Dónde:

f: Número de filas de la tabla de contingencia

c: Número de columnas de la tabla de contingencia

Por lo tanto:

$$GI = (12 - 1)(2 - 1) = 11$$

De acuerdo la tabla de distribución X^2 que se muestra en la Tabla 18-4 y eligiendo como nivel de significancia de $\alpha = 5\% = 0.05$ para obtener un nivel de confianza del 95%, se obtiene como punto crítico de X^2 para 11 grados de libertad $X^2_{Crìtico} = 19.675$.

Tabla 18-4 Tabla de distribución de X^2

g.d.l	0,001	0,005	0,01	0,02	0,025	0,03	0,04	0,05	0,10	
1	10,828	7,879	6,635	5,412	5,024	4,709	4,218	3,841	2,706	
2	13,816	10,597	9,210	7,824	7,378	7,013	6,438	5,991	4,605	
3	16,266	12,838	11,345	9,837	9,348	8,947	8,311	7,815	6,251	
4	18,467	14,860	13,277	11,668	11,143	10,712	10,026	9,488	7,779	
5	20,515	16,750	15,086	13,388	12,833	12,375	11,644	11,070	9,236	
6	22,458	18,548	16,812	15,033	14,449	13,968	13,198	12,592	10,645	
7	24,322	20,278	18,475	16,622	16,013	15,509	14,703	14,067	12,017	1
8	26,124	21,955	20,090	18,168	17,535	17,010	16,171	15,507	13,362	1
9	27,877	23,589	21,666	19,679	19,023	18,480	17,608	16,919	14,684	1
10	29,588	25,188	23,209	21,161	20,483	19,922	19,021	18,307	15,987	1
11	31,264	26,757	24,725	22,618	21,920	21,342	20,412	19,675	17,275	1
12	32,909	28,300	26,217	24,054	23,337	22,742	21,785	21,026	18,549	1
13	34,528	29,819	27,688	25,472	24,736	24,125	23,142	22,362	19,812	1
14	36,123	31,319	29,141	26,873	26,119	25,493	24,485	23,685	21,064	1
15	37,697	32,801	30,578	28,259	27,488	26,848	25,816	24,996	22,307	2
16	39,252	34,267	32,000	29,633	28,845	28,191	27,136	26,296	23,542	2
17	40,790	35,718	33,409	30,995	30,191	29,523	28,445	27,587	24,769	2
18	42,312	37,156	34,805	32,346	31,526	30,845	29,745	28,869	25,989	2
19	43,820	38,582	36,191	33,687	32,852	32,158	31,037	30,144	27,204	2
20	45,315	39,997	37,566	35,020	34,170	33,462	32,321	31,410	28,412	2
21	46,797	41,401	38,932	36,343	35,479	34,759	33,597	32,671	29,615	2
22	48,268	42,796	40,289	37,659	36,781	36,049	34,867	33,924	30,813	2
23	49,728	44,181	41,638	38,968	38,076	37,332	36,131	35,172	32,007	2
24	51,179	45,559	42,980	40,270	39,364	38,609	37,389	36,415	33,196	3
25	52,620	46,928	44,314	41,566	40,646	39,880	38,642	37,652	34,382	3

Realizado por: Tenelema Esthela, 2019

El valor X^2 calculado $X^2_{Calculado}$ en esta investigación es de 20 que es superior al valor de la tabla de distribución de 19.675, como se muestra en la Figura 3-4.

$$X^2_{Crìtico}(19.675) < X^2_{Calculado}(20)$$

GRAFICO

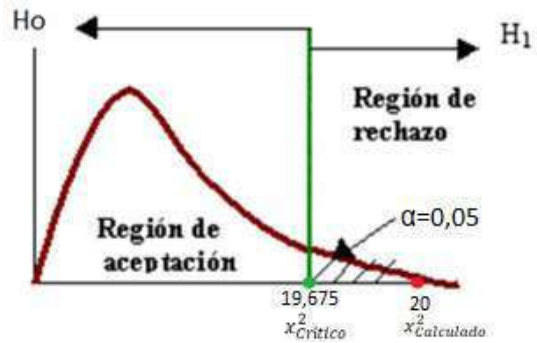


Figura 3-4 Curva de X2
Realizado por: Tenelema Esthela, 2019

Por lo que el valor calculado de X^2 se encuentra en el sector de rechazo de la hipótesis nula H_0, y se acepta la hipótesis de investigación que es significativa, con un nivel de significancia de $\alpha = 5\% = 0.05$ para obtener un nivel de confianza del 95%:

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

CONCLUSIONES

- Considerando las normas ISO 27017 y 27018, el análisis de los organismos internacionales más relevantes en seguridad de la información como: Trend Micro, la organización internacional CSA (Cloud Security Alliance), y GARTNER Inc, se logró definir once controles de seguridad para almacenamiento en la nube que son parte integra 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.
- En la elaboración, implementación del modelo de seguridad para ambientes de almacenamiento en la nube, la principal tarea fue encaminada a los proveedores de servicios, puesto 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 realizado a los prototipos planteados, se logra evidenciar que le modelo de seguridad elaborado e implantado en el Prototipo I ayuda a mejorar los niveles de seguridad de la nube, y mitigación de vulnerabilidades en un 75% en relación al Prototipo II, considerando que a posteriori podrían convertirse en amenazas o riesgos para la organización o cliente que la utilice.
- Se observa que una administración centralizada de seguridad de la información mejora el análisis y el filtrado del tráfico, agilizando el monitoreo de eventos de red y del sistema; importante para reducir la carga en el manejo de 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 un plus o ventaja competitiva para que las organizaciones operen a escala, reduzcan costos de tecnología y utilicen sistemas ágiles.
- Para la implementación del modelo de seguridad en la nube, se utilizó herramientas de software libre como: Clamav, Aide, Mantis bug tracker, Metasploit framework (Kali Linux), entre otros, con ello se simplifican costos, además que mejora la capacidad para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software.

RECOMENDACIONES

- 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. El proveedor con el que se contrate el servicio deberá estar en la capacidad de ofrecer la mejor seguridad de su clase y que sea adapte a las necesidades o requerimientos de su organización.
- Para tener una seguridad de que los datos depositados o almacenados en la nube están protegidos, se debe tomar en cuenta los siguientes factores: la ley de protección de datos del país o la zona en los que resida el servidor y el lugar en donde está registrada la sede social de la empresa, ya que ambos contribuyen a la determinación del grado de protección de la información frente a terceros.
- 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; ya que debido al constante crecimiento de amenazas se debería ir actualizando o complementando el mismo.
- Dentro de esta investigación, siempre que se desee que haya una mejora continua del mismo; se recomienda a futuros estudiantes que tengan interés en la investigación, la complementación del modelo de seguridad con más controles, y en la implementación se puede evaluar la utilización de otras herramientas dependiendo de las vulnerabilidades que sigan apareciendo.

BIBLIOGRAFÍA

Aisha Javed. (31 de 07 de 2017). *The Lessons of #CloudComputing – What Have We Learned So Far?* Obtenido de http://www.xorlogics.com/2017/07/31/the-lessons-of-cloudcomputing-what-have-we-learned-so-far/

Aisha, J. (31 de 7 de 2017). *What Have We Learned So Far?* Obtenido de http://www.xorlogics.com/2017/07/31/the-lessons-of-cloudcomputing-what-have-we-learned-so-far/

Andrews Jeyaraj. (2018). *Recent security challenges in cloud computing.* Obtenido de https://doi.org/10.1016/j.compeleceng.2018.06.006

Aranda Software. (1 de 4 de 2018). *América Latina piensa en la Nube*. Obtenido de https://arandasoft.com/america-latina-piensa-en-la-nube/

AWS. (2020). *¿Qué es el almacenamiento en la nube?* Obtenido de https://aws.amazon.com/es/what-is-cloud-storage/

Box. (2020). *Box.* Obtenido de https://www.box.com/es-419/cloud-storage

BOX, C. V. (2019). *Netbeans*. Obtenido de https://www.netbeans.org

Castro. (2019). *¿Qué es almacenamiento en la nube?* . Obtenido de https://www.aboutespanol.com/que-es-almacenamiento-en-la-nube-157946

CISET. (2020). *Microsoft Office 365.* Obtenido de https://www.ciset.es/glosario/468-office-365

Citrix. (12 de 12 de 2019). *Citrix Systems.* Obtenido de https://docs.citrix.com/en-us/citrix-cloud.html

Cloudwards. (22 de 05 de 2020). *What Is Google Drive and How Does it Work?* Obtenido de https://www.cloudwards.net/how-does-google-drive-work/

CSA. (2015). *Cloud Security Alliance (CSA).* Obtenido de https://aws.amazon.com/es/compliance/csa/

Dhamdhere, P. (2018). Data Access Security in Cloud Computing: A., (págs. 633-635).

Diaz et. al. (2014). *Almacenamiento en la nube.* Obtenido de http://polux.unipiloto.edu.co:8080/00001330.pdf

Dropbox. (2020). *Dropbox.* Obtenido de https://www.dropbox.com/features

El Grupo PHP. (2020). *¿Qué es PHP?* Obtenido de https://www.php.net/manual/en/intro-whatis.php

Evaluando Cloud. (2 de 7 de 2018). *ABC del Cloud Computing.* Obtenido de https://evaluandocloud.com/abc-del-cloud-computing/

GARTNER. (2019). *¿Gestión de vulnerabilidades en TI de estilo DevOps?* Obtenido de https://blogs.gartner.com/anton-chuvakin/2019/06/04/vulnerability-management-in-devops-style-it/

Gastón, L. (17 de 11 de 2017). *¿Qué es el almacenamiento en la nube?* Obtenido de BBVA: https://www.bbva.com/es/que-es-el-almacenamiento-en-la-nube/

GP Liaison. (1 de 05 de 2019). *GP Liaison Services está comprometido con el RGPD y sus principios.* Obtenido de https://gp-liaison.com/gdpr-committment

Institution The British Standards. (2019). *ISO/IEC 27017.* Obtenido de https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

ISO Tools. (16 de 3 de 2017). *ISO 27017: Controles de seguridad para servicios en la nube.* Obtenido de https://www.isotools.org/2017/03/16/iso-27017-controles-seguridad-servicios-la-nube/

ISO Tools. (23 de 3 de 2017). *ISO 27018 La primera normativa para la privacidad en la nube.* Obtenido de https://www.isotools.org/2017/03/23/iso-27018-la-primera-normativa-la-privacidad-la-nube/

Kalaiselvi, R. (2017). Survey of data and storage security in cloud computing. *ICCS 2017.* IEEE International Conference on Circuits and Systems. Obtenido de http://www.xorlogics.com/2017/07/31/the-lessons-of-cloudcomputing-what-have-we-learned-so-far/

KALI. (2019). *Latest Kali Linux News and Tutorials*. Obtenido de https://www.kali.org/

Kinsta. (2020). *What Is Apache Web Server? A Basic Look at What It Is and How It Works.* Obtenido de https://kinsta.com/knowledgebase/what-is-apache/

Lee, J.-H., Kim, Y. S., Kim, J. H., & Kim, I. K. (2017). Toward the SIEM architecture for cloud-based security services. *Toward the SIEM architecture for cloud-based security services* (págs. 398-399). Las Vegas, NV, USA: IEEE.

Marquina. (2017). Obtenido de Big Data y Cloud Computing: una apuesta de futuro: https://bes-h.com/es/big-data-y-cloud-computing-una-apuesta-de-futuro/

MICÓ. (4 de 5 de 2017). *En 2020 cada usuario de Internet almacenará 1,7 gigas en la nube al mes.* Obtenido de https://www.lavanguardia.com/tecnologia/20170504/422277704864/almacenamiento-en-la-nube-cloud-datos-aumenta.html

MICROSOFT. (15 de 05 de 2020). *Microsoft y la norma ISO/IEC 27017.* Obtenido de https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-27017?view=o365-worldwide

MINTIC. (03 de 2016). *Guía técnica de Información-Ciclo de vida del dato.* Obtenido de https://www.mintic.gov.co/arquitecturati/630/articles-9255_recurso_pdf.pdf

NCC, B. (02 de 09 de 2018). *Nextcloud compares to these popular closed-source services,*. Obtenido de Uqnic Network Pte Ltd: https://nextcloud.com/compare/

Nextcloud. (2020). *Nextcloud.* Obtenido de https://nextcloud.com/about/

NEXTCLOUD, C. (2019). *Nextcloud*. Obtenido de https://docs.nextcloud.com/server/16/user_manual/

OPENEXPO EUROPE. (2019). *LA IMPORTANCIA DE LA NORMATIVA DE SEGURIDAD ISO 27017*. Obtenido de https://openexpoeurope.com/es/normativa-seguridad-iso-27017/

OPENVAS. (2020). *OpenVAS - Escáner de evaluación de vulnerabilidad abierta*. Obtenido de https://www.openvas.org/

Ortíz et. al. (2016). *LA IMPORTANCIA DEL USO DE LAS CLOUD COMPUTING EN LAS EMPRESAS PÚBLICAS Y PRIVADAS.* Obtenido de https://www.eumed.net/ce/2016/2/icloud.html

Owncloud. (2020). *Owncloud.* Obtenido de https://owncloud.org/features/

Postgresql. (21 de 05 de 2020). *Postgresql.* Obtenido de https://www.postgresql.org/about/

Simpson, S. (14 de 03 de 2019). *¿What is CentOS?* Obtenido de https://www.lynda.com/Linux-tutorials/What-CentOS/797737/5043628-4.html

Sun, A., Gao, G., Ji, T., & Tu, X. (2018). One Quantifiable Security Evaluation Model for Cloud Computing Platform. *2018 Sixth International Conference on Advanced Cloud and Big Data (CBD)* (págs. 12-15). Lanzhou, China: IEEE.

TREND MICRO. (2019). *MAPPING THE FUTURE Dealing With Pervasive and Persistent Threats*. Obtenido de https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019

ANEXOS

Anexo A: Matriz de Riesgo para Ambientes de Almacenamiento en la nube con base en la ISO 27017 Y 27018.

MATRIZ DE RIESGO PARA AMBIENTES DE ALMACENAMIENTO EN LA NUBE CON BASE EN LA ISO 27017 Y 27018

SECCIÓN A. INFORMACIÓN GENERAL		SECCIÓN B. EVALUACIÓN DEL RIESGO								SECCIÓN C. EVALUACIÓN DE LOS CONTROLES DEL RIESGO						SECCIÓN D. PLAN DE MITIGACIÓN
					CRITERIOS						CRITERIOS					
CONDICIÓN (Si no se contempla)	NEXO	RIESGO EN LA NUBE	FACTOR EXTERNO	FACTOR INTERNO	REPUTACIONAL	PATRIMONIAL	I	P	NIVEL DE EXPOSICIÓN DE RIESGO INHERENTE	¿QUÉ CONTROLES TIENE?	REPUTACIONAL	PATRIMONIAL	I	P	NIVEL DE EXPOSICIÓN DE RIESGO RESIDUAL	OPCION DE MEJORA
Que el proveedor evalúe frecuentemente las posibles vulnerabilidades de la infraestructura que apalanca la solución en la nube	CAUSARIA	Afectación a Plataforma de Virtualización e infraestructura inmersa en ella.	Clientes	Tecnologías	5	2	4	4	ALTO	Protección de la Plataforma de Virtualización	3	1	2	5	MEDIO	La plataforma de virtualización debería fortalecerse de acuerdo a una o más de las siguientes guías: - Guía de configuración de seguridad del proveedor, - Guía de configuración de seguridad estándar de la industria (por ejemplo, DISA STIG, NIST), - Una configuración o serie de controles de seguridad estándar a nivel local o de una autoridad reguladora con el mismo rigor que la guía del proveedor o de la industria
Que el proveedor verifique que las nuevas versiones de las soluciones ofrecidas no tienen vulnerabilidades	CAUSARIA	Afectación al almacenamiento en la nube	Clientes	Tecnologías	4	3	4	3	ALTO	Protección del entorno de almacenamiento en la nube	3	1	2	5	MEDIO	Implementar una "zona segura" para separar y proteger la infraestructura de almacenamiento en la nube de la amenaza que pudiera poner en compromiso los sistemas y servicios ubicados fuera de la zona segura.
Que el proveedor ofrezca soluciones para protección contra malware	CAUSARIA	Afectación de malware, ataques DoS, etc	Clientes	Tecnologías	3	3	3	4	MEDIO	Protección contra Malware	2	2	2	3	BAJO	Se realiza un escaneo antimalware en acceso (también conocido como escaneo de tiempo real o en segundo plano) en la plataforma o en la infraestructura que le atañen al control. El escaneo completo a solicitud se programa cuando menos una vez a la semana. Por motivos de rendimiento, se realizan escaneos completos en momentos de poco uso y/o fuera de horas hábiles.
Que el proveedor informe cuál es la solución usada para encriptar los datos y redes y mejorar de integridad de la información almacenada en la nube	CAUSARIA	Afectación a la Base de datos y su integridad.	Clientes	Tecnologías	5	4	5	3	ALTO	Integridad de la Base de Datos	4	4	4	2	MEDIO	La funcionalidad de comprobación de integridad de la base de datos se activa para asegurar la integridad a nivel de los registros (suma de verificación o firma de los registros) y confirmar que no existen brechas en los archivos almacenados en la nube. Opciones para la implementación: – Integrada a la aplicación de interfaz de almacenamiento en la nube
Que el proveedor posea controles de seguridad para encriptar y monitorear los datos.	CAUSARIA	Afectación a los datos almacenamos en la nube.	Clientes	Tecnologías	5	4	5	3	ALTO	Monitor de integridad de archivos	3	1	2	5	MEDIO	Si se detecta una intrusión, se activa una alarma y, si la herramienta lo permite, se activa un mecanismo de rastreo (acceso a archivos y directorios, movimientos y usos compartidos).
Que el proveedor tenga definido procedimientos de comunicación con los usuarios en caso de algún incidente.	CAUSARIA	No tener un seguimiento, estadísticas y correcta reacción ante incidentes en la nube	Clientes	Procesos	3	3	3	4	MEDIO	Planeación de Respuesta a Incidentes Cibernéticos	2	2	2	3	BAJO	Cada año se actualice un plan de respuesta a incidentes cibernéticos. Existe un plan formal de respaldo y recuperación para todas las líneas críticas para brindar soporte a las actividades de respuesta a incidentes.

Que el proveedor evalúe las aplicaciones desarrolladas antes de pasarlas a producción, a fin de verificar si generan riesgos para los usuarios.	CAUSARIA	No estar con los ultimos parches de seguridad, fraude y error humano.	Clientes	Tecnologías	3	3	3	4	MEDIO	Pruebas de Penetración	2	2	2	3	BAJO	Las pruebas de penetración se realice por lo menos cada 2 años, así como después de que ocurran cambios significativos en el entorno (por ejemplo, nuevos dispositivos del servidor o de la red, cambio al diseño de la red).
Que el proveedor informe y establezca las políticas de autenticación y/o autorización de los usuarios en la red.	CAUSARIA	Suplantación de identidad, robo de información, etc.	Clientes	Tecnologías	3	3	3	4	MEDIO	Política de Contraseñas	2	2	2	3	BAJO	Se establece una política de contraseñas que cubre también la configuración del PIN, de conformidad con los estándares o mejores prácticas actuales de la industria y define los siguientes criterios: Vencimiento de contraseñas, Longitud, composición, complejidad y otras restricciones de las contraseñas, Reutilización de contraseñas, Bloqueo después de intentos fallidos de autenticación y medidas correctivas.
Que el proveedor realice auditorias periódicamente	CAUSARIA	No contar con una eficaz gestión de recursos informáticos, cumplimiento de la normatica, confianza del usuario.	Clientes	Tecnologías	3	4	4	4	ALTO	Fortalecimiento del Sistema	3	1	2	5	MEDIO	Comprobando los sistemas regularmente, al menos dos veces al año, contra los ajustes de seguridad identificados según las directrices anteriores para tomar las medidas correctivas pertinentes.
Que exista mas de un metodo para autenticar al usuario.	CAUSARIA	Suplantación de identidad, robo de información, etc.	Clientes	Tecnologías	3	3	3	4	MEDIO	Autenticación de Múltiples Factores	2	2	2	3	BAJO	Las soluciones de segundo factor basadas en un factor de posesión incluyen (no es una lista exhaustiva): TOTP, RSA SecurID, Digipass, Mobile App, Tabla de Números de Autenticación de Transacciones (TAN), token personal de USB. La solución se elige en función de la propia gestión de riesgos del usuario
Que exista un contrato firmado de servicio entre las partes tanto el físico como en digital (subido a la nube)	CAUSARIA	Que si implemente normas o procedimientos que no esten de acuerdo con alguna de las partes. Uso de la información sin concentimiento del usuario.	Clientes	Personas	3	3	3	4	MEDIO	Compromisos de las partes	2	2	2	3	BAJO	Auditar el contrato de servicio que permita transparencia, mejora en la comunicación, los procesos, los controles internos del servicio

Anexo B: Modelo de Contrato de servicio para el almacenamiento en la nube

CONDICIONES DEL CONTRATO PARA EL SERVICIO CLOUDMSC

CLÁUSULAS:

PRIMERA - CALIFICACIÓN JURÍDICA Y OBJETO.

Por el presente contrato el cliente contrata a TI, S.L. (en adelante Cloudmsc) para que realice la prestación de los servicios que se relacionan en la cláusula tercera y que se especifican en la factura correspondiente y para el número de usuarios especificado en la misma.

Cloudmsc otorga al cliente el derecho no exclusivo, no transferible para utilizar el Servicio y realizar sus propósitos relacionados con los términos y las condiciones de este Contrato.

Todos los derechos que no le sean otorgados de forma explícita se los reservarán Cloudmsc y sus licenciatarios.

SEGUNDA - DEFINICIONES.

SaaS: Software como Servicio. Proveedor de Servicios de Aplicación, proporciona la capacidad de utilizar una aplicación Web exclusivamente a través de Internet.

Aplicación Web: Toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación. El interfaz es un navegador Web, y la ejecución se produce en el proveedor de Servicios de Aplicación.

Datos del cliente / Base de datos: Recopilación de datos dispuestos demanera sistemática o metódica y accesible individualmente únicamente por el cliente a través de la aplicación Web.

Usuario: Persona que tiene derecho a utilizar el programa por estar autorizada para ello exclusivamente a través de Internet, utilizando un navegador Web.

TERCERA - CONTENIDO DE SERVICIO.

-El servicio incluirá:

a) Acceso a través de Internet al servicio, aplicaciones y usuarios contratados, utilizando un navegador y permitiendo el acceso mediante la utilización de una clave de acceso, para cada uno de los usuarios, estas claves serán facilitadas por Cloudmsc.

b) Acceso al servicio de soporte dentro de horas hábiles de trabajo, según el calendario laboral de Cloudmsc.

En el caso de que sea un Distribuidor Autorizado de Cloudmsc quién facture la prestación de servicios, los servicios relacionados en esta cláusula serán prestados directamente por éste.

c) El cliente recibirá, a título meramente informativo, el texto de las novedades relacionadas con el servicio contratado y un breve resumen del contenido de las mismas, utilizándose a tal efecto como canal de comunicación exclusivamente el correo electrónico.

Cloudmsc no se hace responsable de la información suministrada, pues los únicos textos que tienen validez son los publicados a través de la web www.cloudmsc.com.

d) Administración del sistema Servidor en Internet: incluyendo sus actualizaciones.

- NO quedará incluido en el contrato de arrendamiento de servicio:

a) La adaptación de la aplicación Web, las circunstancias especiales del Cliente o a las nuevas necesidades surgidas con el uso.

b) La incorporación de los elementos necesarios para adaptarse a la evolución tecnológica en el dispositivo del usuario: últimas versiones de sistemas operativos, navegador de Internet, conexión a Internet, etc.

c) Los gastos de desplazamiento de los técnicos, si se acordase como consecuencia de la prestación del servicio.

d) Las tareas necesarias para restablecer la situación anterior derivada de operaciones incorrectas por parte del Cliente o de terceros que ocasionen pérdidas de información, destrucción o desorganización de los datos.

e) La corrección de anomalías que no guarden ninguna relación de causalidad con el servicio.

CUARTA - DESCRIPCIÓN Y CONDICIONES DE ACCESO AL SERVICIO.

a) Condiciones de acceso: El cliente recibirá los datos de acceso para poder utilizar el servicio.

Adicionalmente el cliente dispondrá de un código y una clave adicional para administrar los datos de su cuenta cliente, tales como asignar derechos de acceso a los usuarios, consultar los registros de acceso, etc.

b) Los usuarios podrán, a través de la aplicación Web tratar todos los datos facilitados conforme a las cláusulas anteriores, pudiendo realizar todos los cálculos y procesos relacionadas con este contrato.

c) El cliente no podrá otorgar licencias, sublicenciar, vender, revender, transferir, asignar, distribuir, explotar comercialmente de otro modo ni poner el Servicio o El Contenido a disposición de terceros.

d) El cliente no podrá modificar el servicio o el contenido ni realizar trabajos derivados de ellos.

e) La información de la base de datos del servicio Web de Cloudmsc, pertenecerá exclusivamente al cliente.

QUINTA - GARANTÍA, RESPONSABILIDAD CIVIL Y CONFIDENCIALIDAD.

a) El servicio Web proporcionado a través de Internet puede verse sometido a fallos en las infraestructuras del servidor, de la red Internet y de otros programas instalados en el dispositivo del cliente desde donde se conecten al servicio.

Dichos errores también pueden tener su origen en el elevado número de casuísticas diferentes que pueden producirse y de la necesidad del Cliente de utilizar el servicio de forma inmediata, de manera que no exista un lapso de tiempo suficiente entre la publicación de la norma y su incorporación a las nuevas versiones, para probar todas las posibilidades o casuísticas.

Cloudmsc. Garantiza la corrección gratuita, para los clientes que tengan suscrito el presente contrato de servicio, de todos aquellos errores demostrables de modo fehaciente que le sean comunicados. Las correcciones serán incorporadas automáticamente y por lo tanto puestas a disposición de los clientes en la aplicación Web.

b) Tampoco será imputable a Cloudmsc, la alteración de la velocidad y calidad de las comunicaciones.

c) En todo caso, Cloudmsc no será responsable de aquellos daños o perjuicios, que no sean única y exclusivamente imputables a Cloudmsc, ni del lucro cesante dejado de obtener por el cliente.

Por este motivo, queda bajo responsabilidad y la debida diligencia del cliente la contratación de las pólizas de seguros que entienda necesarias para cubrir las situaciones citadas anteriormente.

d) Cloudmsc se obliga por tiempo indefinido a guardar secreto y mantener la más estricta confidencialidad sobre toda la información, propiedad del Cliente, a que tenga acceso como consecuencia de este contrato.

e) Cloudmsc sin el previo consentimiento expreso del Cliente, se abstendrá de efectuar actividad alguna ya se trate de reproducción, uso, conservación, modificación o de cualquier otra

índole, con la información recibida, propiedad del Cliente, para finalidades distintas del estricto cumplimiento de este contrato.

f) En ningún caso podrán acceder terceros a los datos, propiedad del cliente, a que Cloudmsc tenga acceso, sin el consentimiento expreso del Cliente.

g) Fuera de lo dispuesto anteriormente, la responsabilidad de Cloudmsc por los daños imputables directamente a la prestación de servicio contratada se limitará al precio cuota inicial en concepto de alta y cuotas equivalentes al periodo de un año.

h) En cualquier caso el usuario acepta que el servicio contratado constituye una herramienta destinada a complementar, pero no a sustituir la labor humana, por esta razón es obligación del usuario realizar un muestreo sobre los resultados obtenidos con el uso de la aplicación. En caso de que el usuario detectara algún error deberá comunicarlo a la compañía Cloudmsc quién lo solucionará de forma gratuita para aquellos clientes que tengan suscrito el contrato de mantenimiento. El Cliente será el único responsable del buen funcionamiento de sus equipos y sistemas, no pudiendo imputar a Cloudmsc ninguna responsabilidad por estos motivos.

SEXTA - FUERZA MAYOR.

Ninguna de las partes será responsable frente a la otra parte o terceros por los daños y perjuicios ocasionados o pérdidas que resulten de la demora o imposibilidad de cumplimiento de sus obligaciones legales o contractuales, en el supuesto de que se produzca cualquier circunstancia imprevista o que, estando prevista, fuera inevitable al estar fuera de su control.

En relación con el uso del servicio Cloudmsc no garantiza:

a) Que el mismo será siempre seguro, oportuno, ininterrumpido, que carecerá de errores o que funcionará en combinación con cualquier otro hardware, software, sistema o con otros datos.

b) Que cumplirá los requisitos o expectativas del Cliente.

c) Que los datos almacenados serán exactos y fiables.

d) Que la calidad de los productos, los servicios, la información u otro material adquirido u obtenido por el Cliente a través del servicio SaaS cumplirán los requisitos o las expectativas del usuario

e) Que el servicio/s prestado por otros operadores de telecomunicaciones, que hacen que el servicio de Cloudmsc esté disponible, no tendrá vicios u otros componentes dañinos.

Los servicios de Cloudmsc pueden ser objeto de limitaciones, retrasos y otras incidencias inherentes al uso de Internet. Cloudmsc no será responsable de los daños derivados de dichas incidencias.

SÉPTIMA - PROTECCIÓN DE DATOS PERSONALES.

A) TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL.

En la página de www.cloudmsc.com, se recoge la política de privacidad de Cloudmsc.

B) TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL DEL CLIENTE.

El servicio permite introducir documentos e información propia, que pertenecen y son responsabilidad exclusiva del cliente. Cloudmsc como proveedor de servicios de la aplicación, tiene la obligación de cumplir con las obligaciones previstas conforme a la LOPD y el régimen legal vigente en la materia.

C) CLOUD COMPUTING.

Cloudmsc o en su caso, sus Proveedores, para prestar servicios de cloud computing pueden conllevar un acceso a datos de carácter personal. Se trata de una modalidad mixta de cloud computing, un cloud privado, donde se crean redes independientes para los clientes dentro de una plataforma de alta disponibilidad.

A través de Cloudmsc se ofrece a los clientes un servicio SaaS (modelo de Servicio Software As a Service). Para prestar el servicio Cloudmsc tiene subcontratado parte del mismo con varios proveedores.

OCTAVA - RESPONSABILIDAD DEL CLIENTE.

a) Facilitar el trabajo de mantenimiento. El Cliente facilitará el acceso y claves a los especialistas de Cloudmsc a sus páginas de la aplicación Web durante la vigencia del presente contrato, con el fin de facilitar los servicios de soporte contratados.

b) El cliente será responsable de todas las actividades realizadas con sus cuentas de usuario y con su utilización. Por este motivo, el cliente será el único responsable de la exactitud, la calidad, la integridad, legalidad y fiabilidad de sus datos, así como de la propiedad intelectual o el derecho de utilizar los mismos, y Cloudmsc no será en ningún caso responsable de la eliminación, corrección, destrucción, los daños ni la pérdida de los datos del cliente ni de que dichos datos no hayan sido guardados. Una vez rescindido el contrato debido a un motivo justificado, el Cliente perderá inmediatamente el derecho a acceder a los datos del mismo y a utilizarlos. Cloudmsc no tendrá la obligación de conservar ni enviar dichos datos. Cloudmsc se reserva el derecho de retener, suprimir y/o descartar los Datos del cliente sin previo aviso si se produce algún incumplimiento por parte del mismo, incluida sin limitación, la falta de pago.

NOVENA - PRECIO Y FORMA DE PAGO.

Los precios de los servicios contratados por el Cliente se encuentran en la factura correspondiente. A dicha cantidad deberá añadirse el impuesto sobre valor añadido vigente:

a) El pago de los servicios del presente contrato, realizados por Cloudmsc será efectuado en los periodos indicados en el documento comercial y por anticipado por domiciliación bancaria.

b) Correrán por cuenta del Cliente los gastos que se ocasionen con motivo del servicio encargado, tales como desplazamientos y gastos de envío.

DECIMA - DURACION DEL CONTRATO, SUSPENSIÓN DEL CONTRATO.

Este contrato tendrá una vigencia de un año o dos años de acuerdo a la opción que haya escogido el Cliente durante el proceso de compra/suscripción.

En caso de impago de cualquier plazo o cuota emitida por Cloudmsc a cargo del cliente, Cloudmsc queda facultada, para suspender el servicio contratado, sin necesidad de comunicación previa alguna, hasta que el cliente no abone los importes pendientes. Por lo tanto, durante el tiempo que dure la situación de impago Cloudmsc no estará obligada a prestar el servicio contratado.

UNDECIMA - EXTINCION DEL CONTRATO.

Este contrato se extinguirá por las causas generales establecidas por la Ley y en especial, por incumplimiento de las obligaciones contempladas en el mismo.

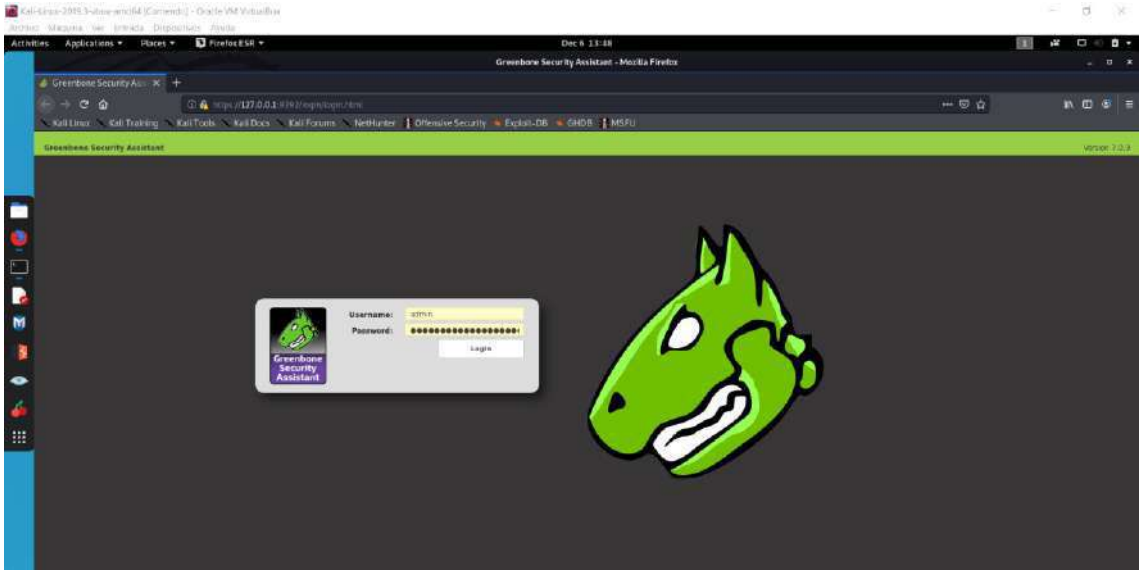
DUODECIMA - COMPETENCIA JURISDICCIONAL.

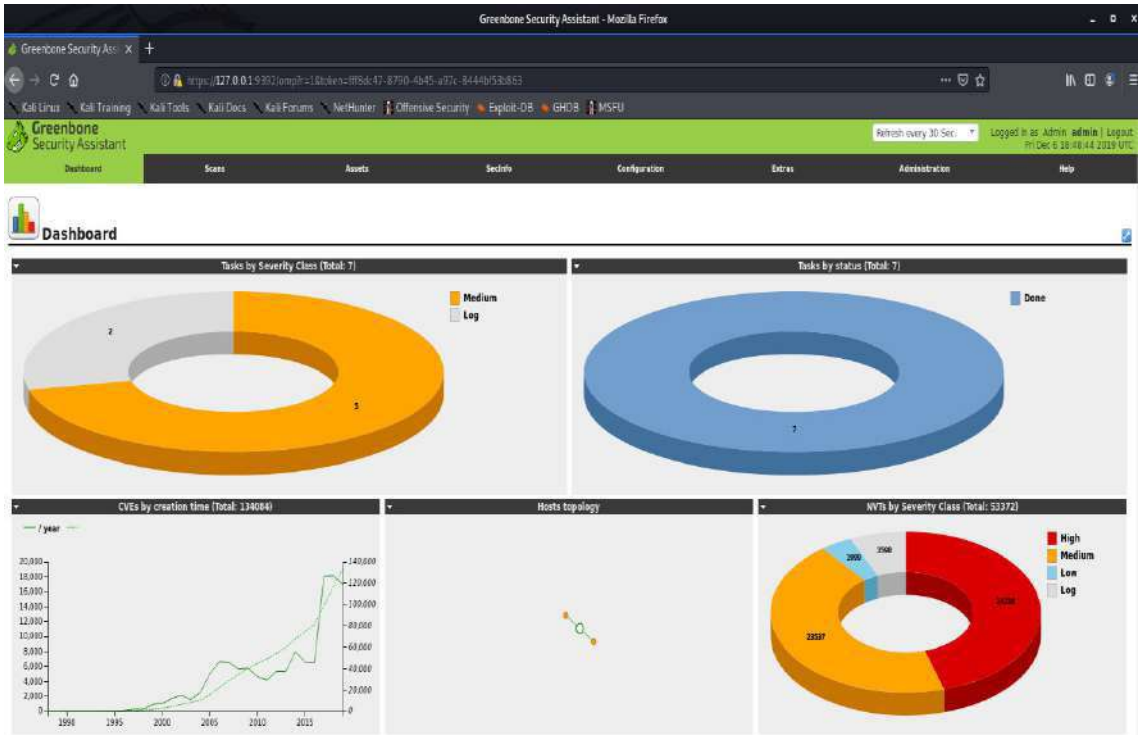
Las partes, con renuncia a su fuero propio, si lo tuvieren, se someten expresamente a los Juzgados y Tribunales de la Ciudad de Ecuador, para dirimir en ellos cuantas cuestiones pudieran derivarse de la interpretación y ejecución presente contrato.

DECIMOTERCERA - DISPOSICIÓN DEROGATORIA.

Las presentes Condiciones Generales derogan lo dispuesto en cualquier otro documento suscrito entre el cliente y Cloudmsc, referente al servicio de mantenimiento contratado.

Anexo C: Herramienta Openvas o Greenbone para análisis de vulnerabilidades.





Anexo D: Estructura o esquema del modelo de seguridad

Tipo de Control	Obligatorio /Recomendado
Objetivo del control: Indica el objetivo de seguridad que debe alcanzarse, independientemente del método de implementación. **Componentes dentro del alcance:** Componentes específicos relacionados con el almacenamiento en la nube que abarca ese control en particular. **Factores de riesgo:** Explica a detalle los riesgos específicos que aborda este control de seguridad.	
Guía de implementación **Planteamiento del control:** Los medios sugeridos mediante los cuales puede alcanzarse el objetivo del control. **Contexto del control:** Información adicional de antecedentes acerca del control. **Directrices para la implementación:** Conjunto de normas o condiciones a valorar en la implementación.	

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS PARA EL APRENDIZAJE Y LA INVESTIGACIÓN

DBRAI

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 24 / 08 /2020

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: Esthela Nataly Tenelema Arias
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: Magister en Seguridad Telemática
f. Analista de Biblioteca responsable: Lic. Luis Caminos Vargas Mgs.

UNIDAD DE PROCESOS TÉCNICOS DBRAI ESPOCH

24-08-2020

0209-DBRAI-UPT-2020