Diseño de un instrumento de ciberseguridad para la migración a la nube en entidades militares : caso de estudio Fuerza Aérea colombiana FAC

Khristian Jaffet Morales Vargas

Trabajo de grado para optar al título profesional:

Maestría en Estrategia y Geopolítica

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

DISEÑO DE UN INSTRUMENTO DE CIBERSEGURIDAD PARA LA MIGRACIÓN A LA NUBE EN ENTIDADES MILITARES. CASO DE ESTUDIO FUERZA AÉREA COLOMBIANA FAC

TENIENTE (FAC) KHRISTIAN JAFFET MORALES VARGAS

DIRECTOR: MSC LUIS CARLOS HERRERA VELÁSQUEZ

ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO"

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2020

Dedicatoria

A mi amada familia y a todas aquellas personas que me apoyaron y acompañaron en el camino hacia el logro de este nuevo peldaño.

Agradecimientos

En primera instancia quiero agradecer a Dios, por regalarme la vida y la sabiduría necesaria para culminar con éxito la realización de este proyecto de investigación.

A mi Fuerza Aérea Colombiana, por darme la oportunidad de realizar mis estudios de maestría, proyectándome como una mejor persona y profesional hacia un mejor futuro, pensando siempre en su personal como el activo más valioso de la Institución.

A mi esposa y a mi hijo, por su amor, comprensión y apoyo incondicional en todo momento, siendo mi soporte y motor de vida para culminar mis metas y llevar a feliz término mis estudios.

A mi asesor, el señor Mayor (FAC) Luis Carlos Herrera Velásquez y todas aquellas personas que, con sus conocimientos y consejos, aportaron en gran medida para poder desarrollar el presente documento.

Resumen

La tecnología de *clouding computing* o la nube, es una realidad que las organizaciones a todo nivel están afrontando y las Fuerzas Militares no son ajenas a ello. Por eso en el presente trabajo, se realiza un instrumento que sirva como guía para la migración hacia los tipos de nube privada o comunitaria para una entidad militar haciendo énfasis en el esquema de ciberseguridad. Para lograr este objetivo, se analiza documentación relacionada con la temática, tal como la legislación aplicable para Colombia respecto a la materia, los lineamientos a nivel del sector defensa, los diferentes modelos de despliegue y servicio de la tecnología *clouding computing*, estándares aplicables, consideraciones para las migraciones hacia la nube, características de los diferentes tipos de nubes, consideraciones de ciberseguridad y ciclo de vida de los datos; todo esto, con el fin de documentar las ventajas y desventajas que podría traer la migración a la nube de los sistemas de información de una entidad militar. Posteriormente se realiza una entrevista a personal experto en estrategias de ciberseguridad y tecnologías de información, donde se recolectan datos cuantitativos y cualitativos acerca de su experiencia en procesos de migración hacia infraestructuras en nube, obteniendo información de las dificultados e inconvenientes afrontados en dichos procesos y recomendaciones acerca de las modelos de despliegue y servicio de nube a utilizar por una entidad militar, a la vez que opiniones sobre qué aspectos deberían ser incluidos en la construcción del presente instrumento. Finalmente, se crea un instrumento basado en fases, aplicable para las entidades de índole militar, donde se indica que pasos se deberían considerar para migrar los sistemas de información de la organización hacia la tecnología *clouding computing* bajo los modelos de despliegue conocidos como nube privada o comunitaria, dada la complejidad de la información de las Fuerzas Militares y haciendo énfasis en el esquema de ciberseguridad que debería contemplarse para contar con una infraestructura robusta y segura.

Palabras claves: Ciberseguridad, migración, *clouding computing*, modelos de nube, instrumento, fases de migración.

Abstract

Clouding computing technology or the cloud, is a reality that organizations at all levels are facing and the Military Forces are no stranger to it. That is why in this document, an instrument is made to serve as a guide for migration to the types of private or community cloud for a military organization with an emphasis on the cybersecurity scheme. To achieve this goal, documentation related to the subject is analyzed, such as the applicable legislation for Colombia regarding the matter, the guidelines at the defense sector, the different deployment and service models of clouding computing technology, applicable standards, considerations for migration to the cloud, characteristics of the different types of clouds, cybersecurity considerations and data life cycle; all this, in order to document the advantages and disadvantages thar the migration to the cloud of the information systems of a military entity cloud brings. Subsequently, and interview ins conducted with expert personnel in cybersecurity strategies and information technologies, where quantitative and qualitative data is collected about their experience in migration processes to the cloud infrastructures, obtaining information of the difficulties and inconveniences faced in said processes and recommendations about the deployment and cloud service models to be used by a military entity, as well as opinions on what aspects should be included in the development of this instrument. Finally, an instrument based on phases is created, applicable for entities of a military nature, where it is indicated what steps should be considered to migrate de organization´s information systems towards clouding technology under the deployments models known as private or community cloud, due the complexity of the information of the Military Forces and emphasizing the cybersecurity scheme that should be considered in order to have a hardy and secure infrastructure.

Keywords: Cybersecurity, migration, clouding computing, cloud models, instrument, migrations phases.

Tabla de Contenidos

Índice de Figuras

Índice de Tablas

Lista de Apéndices

Listado de Siglas y Abreviaturas

AES	Advanced Encryption Standard
API	Application Programming Interface
BYOND	Bring Your Own Device
CASB	Cloud Acces Security Broker
CDMI	Cloud Data Management Interface
CONPES	Consejo Nacional de Política Económica y Social.
CPU	Central Processing Unit
CRM	Customer Relationship Management
CVE	Common vulnerabilities and Exposures
DDOS	Distributed Denial of Service
DLP	Data Lost Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DRP	Disaster Recovery Plan
DSS	Digital Signature Standard
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resources Planning
FAC	Fuerza Aérea Colombiana.
FFMM	Fuerzas Militares de Colombia.
GRC	Gobierno Riesgo y Cumplimiento
HTTP	HyperText Transfer Protocol
HTTPS	HyperTex Transfer Protocol Secure

IAAS	Infrastructure as a Service
IAM	Identity Access Management
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IOT	Internet of Things
IPS	Intrusion Prevention Systems
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Versión 6
ISO	International Organization for Standardization.
IT	Infraestructura Tecnológica.
ITIL	Information Technology Infraestructure Library.
ITU	International Telecomunications Union
KMIP	Key Management Interoperability Protocol
MFA	Multi Factor Autentication
MINTIC	Ministerio de Tecnologías de la Información y Comunicaciones
MSPI	Modelo de Seguridad y Privacidad de la Información
NAC	Network Access Control
NIST	Instituto Nacional de Estándares y Tecnología
NTP	Network Time Protocol
OAUTH	Open Authorization Protocol
OCCI	Open Cloud Computing Interface
OVF	Open Virtualization Format
PAAS	Platform as a Service

PIV	Personal Identity Verification
PKI	Public Key Infraestructure
RAM	Random Access Memory
ROI	Return On Investment
SAAS	Software as a Service
SAML	Security Assertion Markup Language
SCAP	Security Content Automation Protocol
SDLC	Systems Development Life Cycle
SENA	Servicio Nacional de Aprendizaje
SHS	Secure Hash Standard
SLA	Service Level Agreement
SNIA	Storage Networking Industry Association
SNMP	Simple Network Management Protoco
SOA	Servicio Orientado a Arquitectura
SOC	Security Operations Center
SPML	Service Provisioning Markup Language
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single Sign On
TCP	Transmission Control Protocol
TI	Tecnologías de la Información
TIC´s	Tecnologías de la Información y Comunicaciones.
TLS	Transport Layer Security

UDP	User Datagram Protocol
WAF	Web Application Firewall
WAN	Wide Area Network

Introducción

El uso de la tecnología es algo intrínseco a la naturaleza humana antes de la existencia de las Tecnologías de la Información y la Comunicación. Sin embargo, como menciona Grande, Cañón y Catón (2016) el alcance y las consecuencias de su uso hoy en día nos permite modificar nuestro entorno de forma favorable o desfavorable para las organizaciones, provocando vertiginosas transformaciones en los diferentes campos como el social, políticos, económico y académico al igual que en nuestra forma de pensar, entender y acceder a los recursos informativos (De Aguilera & Casero-Ripollés, 2018).

Todo esto ocurre a una gran velocidad y su impacto es igual o superior a otros grandes desarrollos tecnológicos como la imprenta, la máquina de vapor o el uso del petróleo (Salvat & Serrano, 2011). Estos avances tecnológicos han contribuido a lo largo de la historia de la humanidad a mejorar procesos y hacer más eficiente el uso de los recursos (materias primas, maquinaria y mano de obra), impulsando las sociedades hacia una evolución a pasos agigantados (Grande et al., 2016).

El auge del uso de las tecnologías de la información ha fomentado la aparición de nuevas tendencias de computación. La computación en la nube es una de ellas, abordando principalmente el uso de los recursos computacionales. Colombia no ha sido ajena a esta tendencia, lo que ha llevado a diferentes organizaciones en los diversos sectores del país a abordar el uso de la tecnología de computación en la nube, invirtiendo recursos importantes en su implementación (Ramírez, De la Hoz & Gómez, s. f.).

La adopción y el desarrollo de nuevas tecnologías en las entidades gubernamentales y más específicamente en el sector militar, es una constante que se deriva desde el Ministerio de la Tecnologías de la Información y Comunicaciones, y se consolida y orienta a través del Ministerio

de Defensa. Como parte de estos lineamientos se encuentra el CONPES 3854 Política Nacional de Seguridad Digital (Ministerio de Tecnologías de la Información y las Telecomunicaciones - MinTic, 2016b), diferentes guías de computación en la nube emitidas por el MinTic (2018) y un proyecto de resolución del Ministerio de Defensa Nacional por la cual se emite la política de tecnologías en la nube del sector defensa y seguridad. Estos lineamientos aunados a la necesidad misional de la Fuerza Aérea Colombiana (FAC) de aumentar su índice de disponibilidad de servicios tecnológicos, haciendo eficiente el uso de los recursos y manteniendo la seguridad de su información.

Dadas estas consideraciones y la necesidad de la Institución de ofrecer unos servicios tecnológicos de forma eficiente, escalable y con una alta disponibilidad, se ve la computación en la nube como una alternativa para migrar muchos de sus sistemas de información. Es por esto, que nace la necesidad de realizar el presente trabajo de investigación, el cual le otorgará a la FAC una herramienta de ciberseguridad para migrar hacia la nube sus servicios tecnológicos procurando por la integridad, confidencialidad y disponibilidad de la información y sus recursos tecnológicos.

El desarrollo de la presente monografía se contempla en 4 capítulos, como se describen a continuación:

En el Capítulo 1, se realiza el análisis de información académica, estándares internacionales, lineamientos institucionales y gubernamentales, que permitan identificar las ventajas y desventajas de la migración a la nube de la plataforma tecnológica para entidades militares.

En el Capítulo 2, se aplica un instrumento de recolección de información con personal experto en ciberseguridad, lo cual permite establecer los requerimientos funcionales de un sistema de computación en la nube para entidades militares, al mismo tiempo que recopilar opiniones

expertas que puedan ayudar a solucionar nuevas dudas que se presenten durante el desarrollo del trabajo de investigación.

En el capítulo 3, se ilustra un instrumento de ciberseguridad aplicable para la migración a la nube de la plataforma tecnológica de una entidad militar, tomando como caso de estudio la Fuerza Aérea Colombiana.

Finalmente, en el Capítulo 4, se da respuesta al objetivo de la investigación y a la pregunta de investigación, generando a su vez las conclusiones obtenidas luego del desarrollo del presente trabajo de investigación. De igual forma, se establecen los trabajos futuros que puedan desarrollar nuevos conocimientos y extiendan lo realizado en el presente documento.

Antecedentes

Hoy en día, la mayoría de las organizaciones hacen uso de las Tecnologías de Información y las diferentes herramientas que ofrece para la administración de sus negocios. Los sistemas de información abarcan diversas áreas de las organizaciones como la administración de sistemas, publicidad, ventas en línea, mantenimiento y comunicaciones. Pero a medida que la organización crece, también lo hace la complejidad de los sistemas de información, lo que demanda unos altos requerimientos de recursos (Sefraoui, Aissaoui & Eleuldj, 2014). Por lo cual, las organizaciones a diario realizan grandes inversiones en la obtención, soporte y proyección de dichos recursos, entre los que encontramos el equipo tecnológico, actualización de software, capacitación de personal y por supuesto adquisición de tecnología para asegurar dichos sistemas.

Como alternativa de solución de esta problemática, aparece la computación en la nube, que como concepto envuelve la facilidad y rapidez de acceso a los sistemas, redes, datos de multimedia y servicios vía Internet haciendo uso de un mínimo de recursos (Reddy & Monika, 2012). Pero como toda tecnología tiene sus ventajas y desventajas, métodos de implementación, mejores prácticas para adopción y un aspecto que hoy por hoy reviste gran importancia que es la ciberseguridad, la cual es una de las razones fundamentales para adoptar o no una tecnología.

Es por esto que, en el desarrollo de la presente monografía, se realiza un análisis de las distintas formas de la computación en la nube, desde los puntos de vista documental, práctico y en opinión de expertos, lo cual permite realizar un instrumento para llevar a cabo una migración hacia la nube basada en las mejores prácticas, funcional y con las medidas de seguridad digital requeridas.

Alcance

El alcance de esta monografía es la creación de un instrumento de ciberseguridad para la migración hacia la nube de una institución militar, la cual podrá ser utilizada por la Fuerza Aérea Colombiana o cualquier institución militar. Este instrumento se desarrolla basado en un análisis conceptual de referencias bibliográficas, reglamentaciones y metodologías; igualmente el análisis de información obtenida de fuentes primarias y secundarias relacionadas con el objetivo del presente trabajo.

Justificación

Los sistemas de información son herramientas utilizadas por las organizaciones para optimizar la administración de su negocio y envuelven diferentes áreas como publicidad, ventas en línea, mantenimiento, comunicaciones y producción, entre otros. La arquitectura de estos sistemas depende de muchos componentes y parámetros de la organización, al igual que del tipo de tecnología que este en uso. Un sistema de información generalmente se compone de hardware y software, donde a nivel físico se pueden encontrar estaciones de trabajo, equipos portátiles, tabletas, celulares inteligentes y servidores, entre otros y a nivel de software se encuentra desde el sistema operativo hasta diferentes aplicaciones como ERP, CRM, CMMS y ofimática, etc. Por último, se encuentra el componente humano que administra los dos componentes antes mencionados (Sefraoui et al., 2014).

Ahora bien, estos sistemas de información y todos sus componentes, son susceptibles a ataques cibernéticos que comprometen la información. Para ilustrar un caso, tenemos el caso en 2007 donde Estonia fue afectado por un ciberataque donde sus páginas web de gobierno, sistemas bancarios y periódicos resultaron bloqueados durante horas, igualmente el caso de un ataque al Departamento de Defensa de los Estados Unidos, al parecer lanzado por hackers chinos, donde se habrían comprometidos una cantidad aún desconocida de información confidencial (Sánchez, 2010).

En consecuencia de la complejidad de los ataques, el crecimiento acelerado de los sistemas de información y la necesidad de racionalizar los recursos, se han desarrollado nuevas tecnologías como la computación en la nube, donde todos los componentes de un sistema de información como el hardware y software o la infraestructura física, son considerados como un servicio entregado de acuerdo a la necesidad del usuario, incorporando los conceptos de elasticidad, escalabilidad,

accesibilidad y virtualización, con modelos de seguridad adaptados y acordes a la sensibilidad de la información del sistema (Sefraoui et al., 2014).

Para hablar de la tecnología de computación en la nube, se deben tener en cuenta las ventajas y desventajas de su adopción en el sector defensa, donde las principales ventajas serían la escalabilidad, la eficiencia de los recursos mediante los modelos de pago bajo demanda, un ahorro significativo en tiempo y costos y facilidad para el trabajo colaborativo, sin embargo las desventajas podrían traer la propiedad sobre los datos subidos a la nube, la dependencia con la infraestructura contratada y la dependencia de la seguridad de la infraestructura según el modelo de computación en la nube que se seleccione (pública, privada, comunitaria o híbrida) lo cual es parte del propósito del presente trabajo (Instituto Nacional de Tecnología de la Comunicación, 2011

La adopción de nuevas tecnologías y el desarrollo tecnológico de las entidades gubernamentales y más específicamente el sector militar, es una constante que se deriva desde el Ministerio de la Tecnologías de la Información y Comunicaciones y se consolida y orienta a través del Ministerio de Defensa. Como parte de estos lineamientos se encuentra el CONPES 3854 Política Nacional de Seguridad Digital, diferentes guías de computación en la nube emitidas por el MINTIC y un proyecto de resolución del Ministerio de Defensa Nacional por la cual se emite la política de tecnologías en la nube del sector defensa y seguridad. Estos lineamientos aunados a la necesidad misional de las Fuerzas Militares de aumentar su índice de disponibilidad de servicios tecnológicos, haciendo eficiente el uso de los recursos y manteniendo la seguridad de su información aumentan la cabida de este tipo de tecnologías (Departamento Nacional de Planeación (2016).

La seguridad también juega un papel fundamental, puesto que los grandes costos que se invierten para proteger un sistema en sitio son cada vez más crecientes y la amenaza cambiante hace que muy a menudo se deban adquirir nuevos sistemas de defensa haciendo de esto un círculo vicioso que resulta demandando grandes costos en infraestructura tecnológica, administración, capacitación y aun así, las brechas de seguridad nunca estarán totalmente cerradas y se mantendrá un índice de inseguridad bastante elevado en muchos casos.

Formulación del Problema

Ahora bien, las organizaciones militares que proyectan una migración hacia cualquier modelo de servicio y despliegue de la tecnología *clouding computing*, no cuentan con un instrumento que les apoye como guía técnica y procedimental para realizar una migración exitosa y conservando siempre los estándares de ciberseguridad, teniendo en cuenta el punto de vista de las Fuerzas Militares, los procesos que se manejan, la información, las particularidades, los tipos de usuarios, sedes y geografía, que las hacen diferentes de una empresa u organización de cualquier otro tipo en el escenario nacional.

El hecho de realizar una migración hacia una infraestructura en nube, sin contar con un instrumento guía, puede traer diferentes tipos de afectaciones a una organización militar, como incumplimiento sobre estándares y reglamentaciones al respecto, descalabros financieros y técnicos, selección errada del modelo de despliegue y servicio de nube, equivocaciones en la selección de los sistemas a migrar o realizar dicha migración con fallas en la seguridad digital, sea por un dimensionamiento corto o un sobre dimensionamiento en las capacidades de ciberseguridad que podría ocasionar la afectación a la información y por ende a todos los procesos Institucionales; de igual forma, se podrían perder de vista aspectos importantes como la evaluación y el proceso

de mejora que se deben llevar para mantener una infraestructura tecnológica sostenible en todos los ámbitos, que apoye de forma transversal el cumplimiento de la misión de las Fuerzas Militares.

Dadas estas razones y sabiendo que las Fuerzas Militares Colombianas en este momento aún no han incursionado de forma masiva en la tecnología de la nube, con excepción de la Fuerza Aérea Colombiana, quien ya maneja algunas herramientas en dicha tecnología, es el momento oportuno para crear este instrumento de migración a la nube que apoye también desde el punto de vista de la ciberseguridad, para que cuando sea el momento en que por la evolución natural de la tecnología y las organizaciones, sea necesario adoptar las bondades de la nube, se realicen de la mejor forma, desde los puntos de vista técnicos, financieros, funcionales y de seguridad, que deben imperar siempre en una organización de seguridad y defensa Nacional.

Por esta razón, en el desarrollo del presente trabajo de investigación, se proyecta dar respuesta a la siguiente pregunta:

Pregunta de Investigación

¿Cómo diseñar un instrumento de ciberseguridad para la migración a la nube en entidades militares?

La presente monografía tiene como objetivo resolver esta pregunta, desarrollando ese instrumento de ciberseguridad para apoyar los procesos de migración a la nube para lo cual se deberán cumplir los objetivos propuestos, haciendo uso de la metodología seleccionada para tal fin.

Objetivos

Objetivo de la Investigación

Diseñar un instrumento de ciberseguridad para la migración a la nube en entidades militares. Caso de estudio: Fuerza Aérea Colombiana.

Objetivos Específicos

1. Analizar la documentación académica, estándares internacionales, lineamientos institucionales y gubernamentales, que permitan identificar ventajas y desventajas de la migración a la nube de la plataforma tecnológica de entidades militares.
2. Aplicar un instrumento de recolección de información con personal experto en ciberseguridad, que permita establecer los requerimientos funcionales de un sistema de computación en la nube para entidades militares.
3. Ilustrar un diseño de un instrumento de ciberseguridad aplicable para la migración a la nube de la plataforma tecnológica de una entidad militar, caso de estudio Fuerza Aérea Colombiana.

Metodología

Tipo de Investigación

En el desarrollo del presente trabajo de investigación se elige una metodología mixta (Cualitativa – Cuantitativa) en la cual se utiliza evidencia de datos numéricos, verbales, textuales, visuales, simbólicos y de otras clases para entender problemas (DeCuir-Gunby & Schutz, 2017) y (Creswell, 2013). Con este enfoque se busca resolver la pregunta problema y por consiguiente el cumplimiento de los objetivos planteados durante el proceso. Para lograr el cumplimiento de lo antes mencionado, se llevarán a cabo los siguientes pasos:

Análisis Conceptual

El análisis y la revisión de literatura, se constituye en un referente teórico que sirve de guía indicativa y provisional en apoyo a la construcción de conceptos. Por consiguiente, la lectura se debe realizar de forma crítica y selectiva, extrayendo propias conclusiones y manteniendo la atención sobre los aspectos relevantes y que aporten directamente a la investigación y a los hallazgos que puedan darse durante el proceso, evitando que se constituya en un único marco teórico y que produzca un sesgo en el direccionamiento del proceso del presente trabajo (Hernández et al., 2018). Conforme a lo anterior, en el desarrollo de la presente monografía, se analizan documentos de fuentes primarias, secundarias, lineamientos sobre tecnología de computación en la nube y normatividad existente, que permita identificar el estado del arte de la tecnología de computación en la nube, evidenciando a su vez casos de éxito o dificultades en la adopción de la tecnología.

Realización de Entrevistas a Expertos

A través de las entrevistas se analizan las experiencias de los individuos, relacionándolas con prácticas profesionales, con lo cual se busca enfatizar en tener acceso a las prácticas e

interacciones en su cotidianidad, evitando alteraciones que puedan desviar el juicio en un entorno artificial (Hernández, 2014). Es así como la presente monografía hace uso de la entrevista a expertos en materia de ciberseguridad de diferentes sectores, entre ellos el académico, técnico y militar, con el propósito de establecer puntos comparativos de experiencias en implementaciones de tecnología de computación en la nube, ventajas y desventajas y guías que permitan adoptar las mejores prácticas para la adopción exitosa de la tecnología de computación en la nube para una entidad militar.

Capítulo 1

Análisis del Estado del Arte, Estándares, Legislación, Ventajas y Desventajas del Uso del Clouding Computing

En este capítulo se realiza una revisión y análisis de literatura referente a la evolución de los sistemas de información, aparición de la tecnología de computación en la nube, ventajas y desventajas en la adopción de dicha tecnología según diversos autores y modelos de aplicación en diferentes organizaciones. De igual forma se realiza revisión de los estándares y normatividad nacional e internacional que es aplicable, con los aspectos relevantes a tener en cuenta para la migración a la nube y un análisis de la ciberseguridad sobre el *clouding computing*. Esta información servirá para realizar una correcta evaluación de las técnicas y métodos aplicables para la migración a la nube de la plataforma tecnológica de la FAC, que permita desarrollar la herramienta de ciberseguridad para migrar una Institución militar a esta tecnología.

Ciber-Infraestructura

Definida como los componentes de la red que se vinculan a través de diversos nodos replicadores y aseguradores de la transmisión del flujo de información, imprescindible para que puedan acceder los usuarios y consumidores de los servicios; esta infraestructura suministra las capacidades de almacenamiento, integración, virtualización de los datos y recursos informáticos y puede ser accedida a través de internet o una red interna (Casero, Loose & Piemonti, 2019).

Virtualización

La virtualización es una tecnología que como lo menciona Cedeño (2016) combina el hardware y software para fusionar múltiples recursos, presentando un subconjunto de recursos físicos agrupados de forma lógica, permitiendo que se obtengan beneficios sobre la configuración inicial. Actualmente alcanza otras áreas donde se originan grandes avances, entre las que se

encuentran la virtualización de redes, almacenamiento y servidores. Es así, que la virtualización cobra una gran relevancia, pues garantiza la optimización de los recursos, minimizando el uso de software, hardware y personal entre otros, proporcionando capacidades importantes de elasticidad y facilidad de administración.

Mallas Computacionales

Este concepto es muy utilizado para la resolución de problemas computacionales de gran escala y se basa en el aprovechamiento de una gran cantidad de computadores distribuidos y organizados. La computación en la nube hace uso de este término, pues se requiere un soporte robusto en la parte física de la infraestructura, de modo que si uno de los nodos llegara a fallar, el proceso de sustitución, réplica, sustitución para el procesamiento y almacenamiento de la información permita que los usuarios sigan trabajando si siquiera notar que algo ha fallado (Ibagué Camacho & Espindola, 2011).

La Web

La web es básicamente un conjunto de documentos interconectados por enlaces de hipertexto disponibles en internet, a los que se puede acceder a través de tecnología digital. Claramente se ha tenido una evolución de la web, desde su etapa incipiente con la primera versión de la misma denominada Arpanet hasta el nacimiento de lo que hoy se conoce como internet, pasando por versiones desde la 1.0 que aparece hacia los años 1990 limitada a la publicación de información de organizaciones y solo destinada al consuno de la misma, es decir, de forma unidireccional, la web 2.0 que aparece en 2004 con foros y blogs y posteriormente redes sociales, la web 3.0 que estuvo disponible en 2010 y se asocia con una web semántica que es básicamente la facilidad de hacer búsquedas por palabras claves y la web 4.0 que empezó en 2016 ofreciendo

un comportamiento e interacción más intuitivo y predictivo con búsquedas más acertadas con solo realizar una afirmación o llamada (Latorre, 2018).

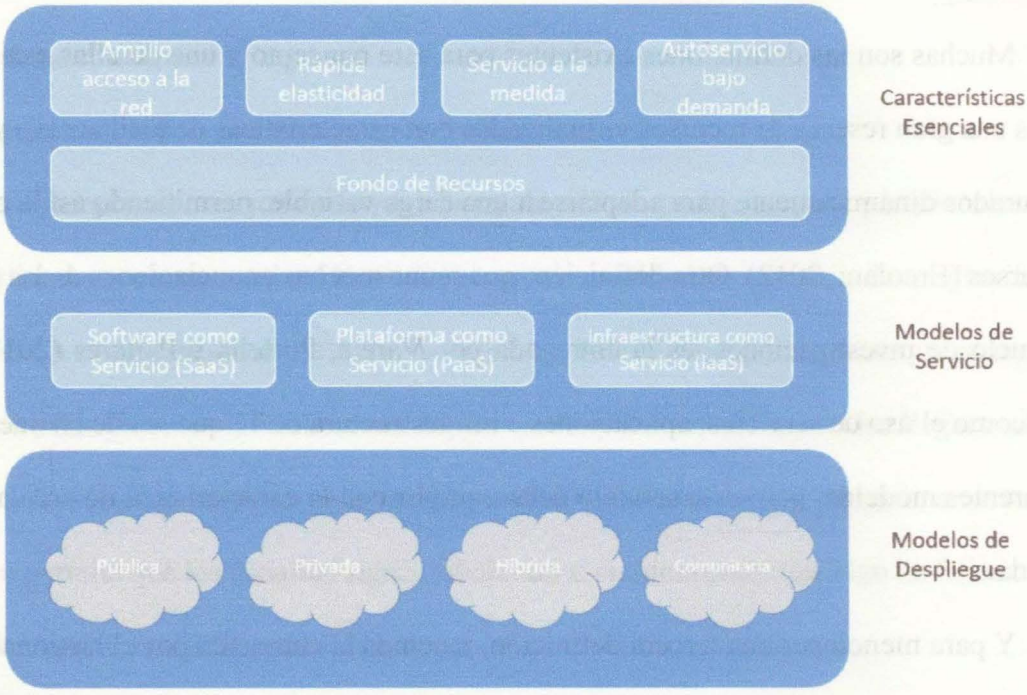
Computación en la Nube.

Muchas son las definiciones existentes para este concepto y una de ellas establece que la nube es una gran reserva de recursos virtualizados con características de fácil acceso y usabilidad; configurados dinámicamente para adaptarse a una carga variable, permitiendo así la optimización de recursos (Ercolani, 2012). Otra definición, que reúne muchas enunciaciones dadas por expertos y producto de investigaciones, es la entregada por Varela, Portella y Pallares (2017), donde la define como el uso de servicios, aplicaciones e infraestructura de TI que reside en internet a través de diferentes modelos; pero este servicio debe cumplir con la característica de escalabilidad bajo demanda.

Y para mencionar una tercera definición, tenemos la entregada por el National Institute of Standars and Technology NIST (Mell & Grance, 2011), donde la nube es un modelo para permitir ubicuidad, conveniencia, acceso a la red bajo demanda, a un conjunto compartido de recursos informáticos, los cuales pueden ser aprovisionados de forma muy rápida con un mínimo esfuerzo del administrador y la interacción con el proveedor. Además, se definen unos componentes de esta tecnología, unos modelos para la prestación del servicio y unos modelos para realizar su implementación, los cuales se pueden ver sintetizados en la siguiente imagen.

Figura 1

Modelo de Computación en la Nube



Nota: Modelo de la definición de Clouding Computing. Adaptado de NIST (Mell & Grance, 2011)

Dentro de las características que diferencian esta tecnología de los sistemas tradicionales, según las NIST, se encuentran el autoservicio bajo demanda, las múltiples formas de acceso, los recursos compartidos, la elasticidad y el servicio medido.

Modelos de Servicio

Infraestructura como servicio (IaaS). Según Jansen (2012) en este modelo el equipamiento es proveído en forma de máquinas virtuales y el cliente mantiene las aplicaciones, los tiempos de ejecución, la integración SOA (Servicio Orientado a Arquitectura) y las bases de datos, mientras que el proveedor del servicio mantiene la virtualización de los recursos, que se traducen en los servidores, el almacenamiento y las redes.

Plataforma como servicio (PaaS). En este modelo, basándonos en el concepto dado por Sefraoui et al. (2014) el cliente desarrolla sus propias aplicaciones usando el servicio proveído y debe mantener únicamente esas aplicaciones con sus datos, mientras que el proveedor del servicio de nube debe mantener los tiempos de ejecución, la integración SOA, las bases de datos, servidores de software, la virtualización, el hardware, almacenamiento y las redes.

Software como servicio (SaaS). Como lo mencionan Guo y Ma (2018), este modelo representa una nueva forma de entregar servicios a los clientes en el cual el vendedor aloja los servicios, los mantiene y los administra de forma centralizada, proporcionando a los clientes el acceso a través de la red y sobra de acuerdo a su uso sobre el mismo. Igualmente Sobhan (2019), lo definen como la última capa de un sistema en nube, en la cual el cliente tiene acceso a un sistema previamente instalado en la infraestructura del vendedor, bajo la figura de pago por uso, proporcionando características de personalización. En este modelo el cliente únicamente tiene la responsabilidad sobre sus datos, todos los demás componentes del servicio son responsabilidad del proveedor.

Para visualizar con más claridad las responsabilidades tanto del proveedor de los servicios de nube como del cliente, tomamos la siguiente imagen que facilita su comprensión.

Figura 2

Modelo de Responsabilidades Compartidas

Nota: Modelo para ilustrar las responsabilidades del cliente y el proveedor sobre la nube. Adaptado de Thales Data Threat Report/451 Research, 2017 (Thales, 2017)

Modelos de Despliegue

Estos servicios pueden ser ofrecidos bajo diferentes modalidades, lo que depende específicamente del usuario, sus necesidades y también su presupuesto. Así entonces, se tienen los siguientes modelos para el despliegue de la tecnología de computación en la nube:

Nube pública. Bajo el concepto de Ramírez et al. (sf.) éste modelo ofrece al público en general el servicio de consumo de recursos de TI a través de Internet y poder ser de forma gratuita o bajo un costo. Complementando Lehto Rajamäki y Rathod (2012), lo describen como una infraestructura entregada a cualquier cliente y que siempre será propiedad del proveedor del servicio; dicha infraestructura es administrada por el proveedor y puede prestar servicio a múltiples clientes.

Nuble privada. Ramírez et al. (s.f.) lo definen como recursos de TI similares a los ofrecidos en la nube pública, pero son accedidos únicamente por funcionarios de organizaciones privadas, permaneciendo fuera del alcance físico y lógico de usuarios no autorizados. Ercolani (2012), lo define como una infraestructura gestionada únicamente para una organización; puede ser gestionada por la misma organización, por un tercero o por una combinación de éstos y la infraestructura físicamente puede estar ubicada dentro o fuera de las instalaciones de la organización que hace uso de los servicios.

Nube híbrida. Esta es una infraestructura compuesta de dos nubes o más, las cuales pueden ser privadas, comunitarias o públicas y mantienen una única entidad, pero están unidas por la tecnología estandarizada lo que permite la portabilidad de los datos y aplicaciones (Ercolani, 2012).

Nube comunitaria. Sefraoui et al. (2014) lo definen como una infraestructura aprovisionada para un uso exclusivo y compartida por una comunidad específica, por ejemplo, los entes gubernamentales. Puede ser propietaria, administrada y operada por una o más organizaciones dentro de la comunidad. En adición, Ercolani (2012), dice que este tipo de nube soporta una comunidad con intereses comunes como misión, requisitos de seguridad, políticas y consideraciones sobre cumplimiento normativo y que adicionalmente puede estar ubicada dentro o fuera de la comunidad.

Para hablar de *Cloud Computing* y pensar en una migración de la plataforma tecnológica de una Institución Militar, es necesario conocer los estándares que se han dispuesto por organizaciones internacionales con el fin de garantizar el correcto funcionamiento; de tal forma que a continuación se van a mencionar estos estándares y se va a hacer énfasis en los pertinentes a la ciberseguridad.

Estándares Aplicables a la Computación en la Nube

El análisis de los estándares aplicables a la tecnología de computación en la nube se hará basados en el documento "El estudio del clouding computing. Retos y oportunidades" (Ureña, 2012).

Estándares Relacionados con la Interoperabilidad

Estos estándares garantizan el funcionamiento de las tecnologías en nube en compatibilidad con otras nubes y con las aplicaciones dispuestas para el uso de la misma. Así entonces, podemos encontrar estándares como los definidos por el Instituto Nacional de Estándares y Tecnología (NIST) por sus siglas en inglés Hogan, Liu, Sokol y Tong (2011) que se relacionan continuación:

- Open Cloud Computing Interface (OCCI), desarrollado por la Open Grid Forum.
- Cloud Data Management Interface (CDMI), desarrollado por la Storage Networking Industry Association, SNIA.
- IEEE P2301, Guide for Cloud Portability and Interoperability Profiles (CPIP), desarrollado por el Institute of Electrical and Electronics Engineers.
- IEEE P2302, Standard for Intercloud Interoperability and Federation (SIIF), desarrollado por el Institute of Electrical and Electronics Engineers.

Estándares Relacionados con la Portabilidad

El desarrollo de estos estándares va enfocado a garantizar que la virtualización utilizada en la computación en la nube, la cual hace uso del empaquetado de sistemas con todas sus características listas para el uso del cliente final, permitan la portabilidad a cualquier plataforma de tecnología de nube (Ureña, 2012). El Instituto Nacional de Estándares y Tecnología (NIST) relaciona los siguientes, Hogan et al. (2011):

- Cloud Data Management Interface (CDMI), desarrollado por la Storage Networking Industry Association, SNIA.
- Open Virtualization Format (OVF), desarrollado por el Grupo de Trabajo de Administración Distribuida por sus siglas en ingles DMTF.
- IEEE P2301, Guide for Cloud Portability and Interoperability Profiles (CPIP), desarrollado por el Institute of Electrical and Electronics Engineers.

Estándares Relacionados con la Seguridad y el Nivel de Servicio

La seguridad en la nube es una de las mayores fuentes de desconfianza de los usuarios, pues el hecho de almacenar su información en una infraestructura de un tercero o compartida, según sea el modelo de despliegue elegido, es motivo de incertidumbre. Es por esto que los proveedores de los servicios de computación en la nube tienen como premisa garantizar los tres pilares de la seguridad de la información (confidencialidad, disponibilidad e integridad). En procura de mantener estos pilares, la seguridad en la nube se enfoca en reforzar el control perimetral, ofrecer métodos fuertes de criptografía e implementar mecanismos de gestión de logs o archivos de registro de eventos para tranquilidad de los clientes (Ureña, 2012).

Para brindar soluciones seguras a los clientes, los proveedores de nube se centran especialmente en los siguientes vectores:

- Protección de los datos de los clientes contra el acceso no autorizado.
- Protección contra las amenazas a la cadena de suministro.
- Protección contra el acceso no autorizado a la infraestructura de nube.
- Protección a nivel de usuario de los navegadores utilizados para acceder a los recursos de la nube.

- Implementación de controles de acceso y tecnologías de detección de intrusos en la nube.
- Definición de límites de confianza y responsabilidades entre el proveedor de los servicios de nube y el cliente.
- Aseguramiento de la portabilidad, garantizando que el cliente pueda migrar entre diferentes plataformas de nube, sin interrupciones significativas del servicio.

Entre los estándares desarrollados para garantizar la seguridad podemos encontrar los siguientes, distribuidos por la categoría:

Autenticación y Autorización

De acuerdo con información relacionada por Ureña (2012) quienes se apoyan en información publicada por diferentes organizaciones, se tienen los siguientes estándares:

- RFC 5246: Secure Sockets Layer (SSL) / Transport Layer Security (TLS), desarrollado por el Grupo de Trabajo de Ingeniería de Internet por sus siglas en ingles IETF.
- RFC 3820: X.509 Public Key Infraestructure (PKI) Proxy Certificate Profile, desarrollado por el Grupo de Trabajo de Ingeniería de Internet por sus siglas en ingles IETF.
- RFC 5280: Internet X.509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile, desarrollado por el Grupo de Trabajo de Ingeniería de Internet por sus siglas en ingles IETF.
- RFC 5849: Oauth (Open Authorization Protocol), desarrollado por el Grupo de Trabajo de Ingeniería de Internet por sus siglas en ingles IETF.
- OpenID Authentication, desarrollado por la Fundación OpenID.
- eXtensible Access Control Markup Language (XACML), desarrollado por OASIS estándar.

- Security Assertion Markup Language (SAML), desarrollado por OASIS estándar.
- FIPS 181: Automated Password Generator, desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) (Hogan et al. , 2011)
- FIPS 190: Guideline for the use of Advanced Authentication Technology Alternatives, desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).
- FIPS 196: Entity Authentication using public key cryptography, desarrollado por el Instituto Nacional de Estándares y Tecnología (NZIST).

Confidencialidad

- RFC 5246: Secure Sockets Layer (SSL) / Transport Layer Security (TLS), desarrollado por el Grupo de Trabajo de Ingeniería de Internet por sus siglas en ingles IETF.
- Key Management Interoperability Protocol (KMIP), desarrollado por OASIS estandar.
- XML Encryption Syntax and Processing, desarrollado por el Consorcio World Wide Web.
- FIPS 140-2: Security Requirements for Cryptographic Modules, desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).
- FIPS 185: Escrowed Encryption Estandard /EES), desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).
- FIPS 197: Advanced Encryption Standard (AES), desarrollado por desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).
- FIPS 188: Standard Security Label for Information Transfer, desarrollado por desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).

Integridad

- XML Signature (XMLDSig), desarrollado por el Consorcio World Wide Web.

- FIPS 180-3: Secure Hash Standard (SHS), desarrollado por desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).
- FIPS 186-3: Digital Signature Standard (DSS), desarrollado por desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).

Gestión de Identidad

- Service Provisioning Markup Language (SPML), desarrollado por la WSFederation and WS-Trust.
- X.idmcc – Requirement od IdM in Cloud Computing, desarrollado por la Unión Internacional de Comunicaciones por sus siglas en inglés ITU.
- Security Assertion Markup Language (SAML), desarrollado por OASIS estandar.
- OpenID Authentication, desarrollado por la Fundación OpenID.
- FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors, desarrollado por desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).

Monitoreo y Respuesta a Incidentes

- NIST SP 800-126: Security Content Automation Protocol (SCAP), desarrollado por desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).
- NIST SP 800.61: Computer Security Incident Handling Guide, desarrollado por desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).
- X.1500 Cibersecurity Information Exchange techniques, desarrollado por la Unión Internacional de Comunicaciones por sus siglas en inglés ITU.
- X.1520: Common vulnerabilities and Exposures, desarrollado por la Unión Internacional de Comunicaciones por sus siglas en inglés ITU.

- X.1521: Common Vulnerability Scoring Systems, desarrollado por la Unión Internacional de Comunicaciones por sus siglas en inglés ITU.
- PCI Data Security Standard, desarrollado por PCI SCC.
- FIPS 191: Guideline for the Analisys of Local Area Network Security, desarrollado por desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST).

Disponibilidad

ISO/PAS 22399:2007 Guidelines for Incident preparedness and operational continuity management; desarrollada por la Organización Internacional de Normalización por sus siglas en inglés ISO.

De esta forma es posible evidenciar que hay una gran cantidad de estándares aplicados a la tecnología en la nube y para cada una de las categorías o características que se desarrollan, con el fin de garantizar al usuario que los servicios, la seguridad de los datos, la migración y la integración sean los adecuados.

Tabla 1

Resumen de Estándares

Pilar	Estándar	Descripción
Autenticación y autorización	RFC 5246: Secure Sockets Layer (SSL) / Transport Layer Security (TLS).	Utilizado para proporcionar comunicaciones seguras a través de la red.
	RFC 3820: X.509 Public Key Infraestructure (PKI) Proxy Certificate Profile.	Utilizado para estandarización de certificados de claves públicas y algoritmos de validación.

Pilar	Estándar	Descripción
	RFC 5280: Internet X.509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile.	Define métodos para revocación de los certificados.
	RFC 5849: Oauth (Open Authorization Protocol).	Utilizado para permitir la autorización de las API´s para las aplicaciones.
	OpenID Authentication.	Utilizado para proporcionar identificación a los usuarios dentro de una página web.
	eXtensible Access Control Markup Language (XACML).	Utilizado para definir el lenguaje de las políticas de control de acceso en XML y como realizar la evaluación de las peticiones de acceso.
	Security Assertion Markup Language (SAML).	Se usa para definir el esquema XML para intercambiar los datos requeridos en los procesos de autenticación y autorización entre un proveedor de identidad y un proveedor de servicio.
	FIPS 181: Automated Password Generator.	Estándar que provee la generación automatizada de contraseñas.
	FIPS 190: Guideline for the use of Advanced Authentication Technology Alternatives.	Usado para verificar las identidades de los usuarios de los sistemas de información, haciendo recomendaciones para la adquisición de tecnología que sirva de respaldo de dichos métodos de identificación.
	FIPS 196: Entity Authentication using public key cryptography.	Estándar que provee dos protocolos de desafío sobre una respuesta para suministrar autenticación de una entidad a

Pilar	Estándar	Descripción
		un sistema informático. Utilizado generalmente en los inicios de sesión.
Confidencialidad	RFC 5246: Secure Sockets Layer (SSL) / Transport Layer Security (TLS).	Utilizado para proporcionar comunicaciones seguras a través de la red, aplicable también a la protección de la confidencialidad.
	Key Management Interoperability Protocol (KMIP).	Este protocolo se usa para definir el formato de manipulación de las llaves criptográficas en un servidor de administración de llaves.
	XML Encryption Syntax and Processing.	Este protocolo especifica un proceso para cifrar los datos y representarlos en XML.
	FIPS 140-2: Security Requirements for Cryptographic Modules.	Esta publicación del estándar obedece a conceptos de seguridad en equipos de cómputo de Estados Unidos para la acreditación de módulos criptográficos.
	FIPS 185: Escrowed Encryption Estandard /EES).	Estándar para Comunicaciones cifradas, basado en la custodia de claves que permite su conocimiento de forma clandestina por parte de agencias gubernamentales autorizadas.
	FIPS 197: Advanced Encryption Standard (AES).	Es un esquema de cifrado por bloques que utiliza un tamaño fijo de dichos bloques y de llaves.
	FIPS 188: Standard Security Label for Information Transfer.	Protocolo utilizado para determinar cómo manejar los datos entre sistemas abiertos.

Pilar	Estándar	Descripción
Integridad	XML Signature (XMLDSig).	Es un estándar que define la sintaxis XML para una firma digital.
	FIPS 180-3: Secure Hash Standard (SHS).	Estándar que utiliza un algoritmo para la generación de un hash que transforma un conjunto de datos en un valor único de una longitud fija.
	FIPS 186-3: Digital Signature Standard (DSS).	Estándar que especifica un conjunto de algoritmos utilizados para generar firmas digitales.
Gestión de identidad	Service Provisioning Markup Language (SPML).	Es un estándar basado en XML con el fin de intercambiar información del aprovisionamiento de servicios, usuarios y recursos entre organizaciones.
	X.idmcc – Requirement od IdM in Cloud Computing.	Este estándar se utiliza para entregar los requerimientos para la administración de las identidades en las infraestructuras de nube.
	Security Assertion Markup Language (SAML).	Se usa para definir el esquema XML para intercambiar los datos requeridos en los procesos de autenticación y autorización entre un proveedor de identidad y un proveedor de servicio. Estándar también aplicado a mantener la gestión de identidades.
	OpenID Authentication.	Utilizado para proporcionar identificación a los usuarios dentro de una página web. Estándar también aplicado

Pilar	Estándar	Descripción
		para mantener la gestión de identidades.
	FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors.	Este estándar identifica la estructura y requerimientos técnicos para la identificación de los empleados y contratistas federales del gobierno de los Estados Unidos.
	NIST SP 800-126: Security Content Automation Protocol (SCAP).	Este estándar define el formato y nomenclatura por las cuales se comunica a máquinas y personas, la información acerca de fallas de software y configuraciones de seguridad.
	NIST SP 800.61: Computer Security Incident Handling Guide.	Esta guía se crea para asistir a las organizaciones en la mitigación del riesgo de la seguridad de computadores e incidentes, suministrando una guía de buenas prácticas.
Monitoreo y respuesta a incidentes	X.1500 Cibersecurity Information Exchange techniques.	Su objetivo es estandarizar la forma en que se comparte la información acerca de técnicas de ciberseguridad entre diferentes organizaciones.
	X.1520: Common vulnerabilities and Exposures.	Su finalidad es estandarizar la nomenclatura utilizada para reportar las vulnerabilidades de seguridad conocidas en hardware y software, siendo definido y mantenido por la corporación MITRE.
	X.1521: Common Vulnerability Scoring Systems.	Es un estándar utilizado para evaluar la gravedad de las vulnerabilidades de seguridad de los sistemas de

Pilar	Estándar	Descripción
		información, permitiendo a los desarrolladores priorizar la atención a las brechas de seguridad.
	PCI Data Security Standard.	Es un estándar aplicado a la seguridad de los datos para la industria de la tarjeta de pago, que pretende ayudar a asegurar los datos procesados, almacenados y transmitidos con el fin de evitar fraudes con el uso de las tarjetas de pago.
	FIPS 191: Guideline for the Analisys of Local Area Network Security.	Este documento tiene como finalidad, ofrecer una guía de buenas prácticas a los administradores, oficiales de seguridad y usuarios de la red LAN, con el fin de proteger los datos almacenados, procesados y transmitidos a través de dicha red. Ayudando a determinar los controles más efectivos para procurar la seguridad de la LAN.
Disponibilidad	ISO/PAS 22399:2007 Guidelines for Incident preparedness and operational continuity management.	Este documento suministra una guía de buenas prácticas para organizaciones de tipo privado, gubernamental o no gubernamental, para desarrollar criterios y preparación para la continuidad operacional.

Marco Regulatorio de Colombia

Colombia es uno de los países que cuenta a la fecha con un conjunto de leyes que facilitarán el desarrollo del Cloud Computing. A continuación, se describen estas leyes y se enuncian los temas más importantes que éstas mencionan:

Ley 1273 de 2009. Por medio de la Ley 1273 de 2009 expedida por el Congreso de Colombia (2009a) se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Esta ley protege a los sistemas de Información de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. La Ley penaliza, entre estos atentados, el acceso abusivo a los sistemas informáticos, la interceptación de datos, la ejecución de daños informáticos, el uso de software malicioso, la violación de los datos personales, la suplantación de sitios web para capturar datos personales, el hurto por medios informáticos y semejantes y la Transferencia no consentida de activos

Ley 1221 de 2008 – Ley de teletrabajo. Por medio de esta ley, se establecen normas para promover y regular el Teletrabajo y se provee un marco de seguridad jurídica.

Esta ley expedida por el Congreso de Colombia (2008a) define el teletrabajo en sus distintas formas, establece una política pública de fomento al teletrabajo y una red nacional de fomento al teletrabajo. De igual manera, menciona que el Gobierno Nacional pondrá en funcionamiento un sistema de inspección, vigilancia y control para garantizar el cumplimiento de la legislación laboral en el marco del teletrabajo y se proveen las garantías laborales, sindicales y de seguridad social para los teletrabajadores

Ley 1266 de 2008. La ley 1266 de 2008 Declarada Exequible mediante Sentencia C- 1011 del 16 de octubre de 2008., dictan las disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países, entre otros (Congreso de Colombia, 2008b).

Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países (Congreso de Colombia, 2008b).

Ley 1341 de 2009. Por medio de esta ley expedida por el Congreso de Colombia (2009b) se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Esta ley tiene por objeto determinar el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y

facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información (Congreso de la República, 2009b)

CONPES 3854 de 2016. En el CONPES 3854/16 del Departamento Nacional de Planeación- DNP (2016) se adopta la gestión del riesgo como núcleo principal para la implementación de manera proactiva. El objetivo de esta política Nacional es fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital, en un marco de cooperación, colaboración y asistencia. Lo anterior con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

Casos de Migración a la Nube

Estos casos fueron extractados del texto "Cloud Computing una perspectiva para Colombia" (Mesa Sectorial Cloud, 2010).

Universidad de los Andes. Se encuentra desarrollando el proyecto "Opportunistic Cloud Computing Infraestructure as a service Model", Este proyecto enmarcado en una tesis de Maestría en Ingeniería – Sistemas y Computación, tiene como objetivo el desarrollo de un modelo Cloud Computing de Infraestructura como Servicio (Cloud IaaS) para desplegar y entregar recursos y servicios computacionales fundamentales, a través de una infraestructura oportunista de crecimiento horizontal (Rosales, Castro & Villamizar, 2011).

Para ello se desarrollará una arquitectura Cloud Computing de propósito general que enmarque el modelo de servicio Cloud IaaS en una nube privada cuya infraestructura estará compuesta prevalentemente por hardware económico, heterogéneo, distribuido, de dominio administrativo independiente y actualmente disponible en los laboratorios de cómputo del campus de la Universidad de los Andes (Rosales et al., 2011).

SENA – Google. El Servicio Nacional de Aprendizaje (SENA) y Google están trabajando desde hace un año en la plataforma misena.edu.co. En este momento, más de 360 mil usuarios en la comunidad misena.edu.co están trabajando en la plataforma Google Apps. Las cuentas activas involucran la participación desde aprendices e instructores hasta funcionarios administrativos, usuarios del Servicio Público de Empleo e integrantes de las Mesas Sectoriales. Se espera contar con más de 3 millones de usuarios beneficiados al año 2010 (Mesa Sectorial Cloud, 2010).

Aspectos para Tener en Cuenta en la Migración hacia la Nube

Migración y portabilidad. Hoy en día existen muchos tipos de despliegues de nubes, donde las organizaciones podrían moverse entre ellas sin afectación de los usuarios finales, por tanto, es una característica que ha cobrado importancia al momento de la selección por parte de los clientes; este concepto es asimilado también como la interoperabilidad entre los proveedores de servicios en nube, que obedece a la capacidad de transferir las cargas de trabajo, importar y exportar recursos y gestión de usuarios entre diferentes vendedores (Cortés García, 2017).

Teniendo en cuenta que la Fuerza Aérea Colombiana es una entidad pública que se rige por la ley 80 de 1993 (Estatuto General de Contratación de la Administración Pública Colombiana), está sujeta además de la calidad del servicio, a los costos, pues en la eventualidad de existir dos proveedores que cumplan con las especificaciones técnicas mínimas requeridas por la entidad para una eventual migración a la nube, se deberá seleccionar aquel que tenga un costo más bajo (Congreso de Colombia, 1993)

Escalabilidad, La mayoría de las definiciones indican que la elasticidad está basada en cómo rápidamente un ambiente en la nube es capaz de adaptarse a las necesidades del usuario (Lehrig, Eikerling & Becker, 2015). Este concepto es fundamental para una Entidad de seguridad como lo es la FAC, pues consiste en migrar de forma gradual hacia la nube algunos servicios y

tecnologías, con lo que permite evaluar el comportamiento, usabilidad, costos y beneficios de dicho proceso y además analizar la posibilidad de mantener en sitio aquellos servicios que son nicho del negocio que por su susceptibilidad deban mantenerse en sitio. Es necesario aclarar que, en el momento de la realización de la presente monografía, la FAC ya migro hacia la nube el servicio de correo electrónico Institucional utilizando el servicio ofrecido de Office 365 mediante los Acuerdo Marco de Colombia compra eficiente.

Seguridad y privacidad. Mientras que uno de los principales obstáculos de cara a la migración hacia la nube es la seguridad, la computación en la nube rompe paradigmas dando oportunidades para innovación y aprovisionamiento de servicios de seguridad que mantienen la proyección de mejorar el promedio de seguridad de algunas organizaciones; los mayores beneficiado con estos enfoques, son las pequeñas organizaciones que cuentan con números limitados de administradores de tecnología y personal de seguridad, pudiendo obtener la economía de escala que se le otorgaría a una gran empresa (Jansen & Grance, 2011).

Sin embargo, autores como Sinjilawi, Al-Nabhan y Abu-Shanab (2014) ven aun retos por cumplir en materia de seguridad, reflejados en aspectos como los Niveles de Acuerdo de Servicios por sus siglas en ingles SLA, donde el usuario no tiene el control total de los recursos en la nube, pero debe tratar de compensar esta desventaja, estableciendo uno SLA que garanticen la confianza, rendimiento, disponibilidad y calidad de los recursos ofrecidos.

Algunos autores como Sharma, Bansal y Sharma (2012) clasifican los retos de seguridad dependiendo el tipo de nube, de acuerdo a la siguiente tabla:

Tabla 2.

Clasificación de los Retos de Seguridad

Nube Personal	Nube General
-Administración de identidad y acceso. -Protección de Datos. -Inteligencia de seguridad. -Seguridad de software, plataforma e infraestructura.	-Ataques de DoS. -Ataques sobre máquina virtual. -Colocación de Código malicioso. -Ataques sobre la máquina física.
Nube de Dominio Específico	**Nube Mixta**
-Cumplimiento y auditoria. -Características del Cortafuegos -Detección de intrusos. -Controles de Acceso. -Protección Antimalware y antivirus.	-Múltiples tenats de nubes. -Preocupación de cumplimiento contínuo. -Administración de acceso y control de acceso. -Estiramiento de datos.

Nota: Adaptado de Cloud Computing: Different Approach & Security challenge. (Sharma, Bansal & Sharma, 2012)

Dados los beneficios y retos en materia de seguridad digital, el enfoque que se le ha dado a este proyecto de investigación (Ciberseguridad hacia la nube), toma gran relevancia a la hora de comparar los modelos de administración de la información, pues muchas veces no se tiene en cuenta que la nube cuenta con una gran capa de seguridad conformada por muchas de las herramientas que quizá hoy en día no se encuentran en los modelos on premise o que migrar puede representar en cierta forma la pérdida del control sobre la información y los recursos, todo dependiendo del modelo de despliegue y el tipo de nube que se seleccione.

Reglamentación legal y jurídica

Otra dificultad acerca de la computación en la nube es el movimiento de los datos, los cuales podrían ser movidos entre diferentes países y por tanto enfrentar diferentes regulaciones locales. La anonimización de la información puede ser la solución para asegurar la privacidad de la información de los clientes. Uno de los principales retos legales es la ambigüedad de los roles

de los proveedores de servicios en nube que se puede encontrar al momento de una migración (Sinjilawi et al., 2014).

Basado en lo expuesto por estos autores, se debe evaluar cuidadosamente el control y el derecho de propiedad que la Institución tenga en todo momento sobre la información migrada hacia la nube, sin importar el país en el cual se encuentren físicamente los datos, pues es importante recordar que hay diferentes enfoques a este respecto, principalmente en el modelo norteamericano y el europeo. Además, se debe tener en cuenta la legislación colombiana, con la reglamentación Nacional mencionada anteriormente en el presente documento.

Priorización de Objetivos y Verificación de la Tolerancia al Riesgo

La protección de los datos en el entorno laboral ha sido un reto para los profesionales de seguridad por décadas; puesto que no hay una seguridad 100% bajo ninguna perspectiva y decisiones complejas deben ser tomadas en las distintas capas del negocio (Donald, Oli & Arockiam, 2013).

Bajo esta perspectiva es importante que, una vez conocidos los objetivos de la migración hacia la nube, se haga una verificación de las arquitecturas de los sistemas objeto de migración, detallando su nivel de seguridad, resiliencia ante ataques y dimensionar la afectación que pudiera tener para la continuidad del negocio.

Protección de Datos con un Plan de Seguridad Proactivo

Los planes de seguridad no son una tarea fácil para una organización, pues esto incluye entender el panorama de las amenazas y trabajar en proteger la organización contra esas amenazas requiere principalmente de dos cosas, las políticas y la tecnología (Donald et al., 2013).

Siguiendo este enfoque, los planes de seguridad deben contemplar la nube como esa nueva extensión de la infraestructura tecnológica de la organización y destinar recursos (tecnología,

personal, políticas) para su protección, analizando el entorno global de las amenazas que cambiarían por ser un entorno más abierto.

Prepare la Respuesta para un Inevitable Ataque Sofisticado

Con la evolución continua de las amenazas avanzadas, los delincuentes informáticos logran encontrar vulnerabilidades y es inevitable que en cierto momento la organización tenga brechas de seguridad que no puede anticipar (Donald et al., 2013).

Teniendo en cuenta los autores, un plan unificado y probado para responder a estos ataques bajo situación críticas es un recurso importante para hacerle frente a las amenazas y debe ser considerado por una institución, tanto si desea migrar a la nube como si desea mantener su infraestructura sobre premisas, este plan debe contar con recurso humano entrenado y capacitado para atender la novedad, así como procedimientos claros y establecidos previamente.

Administración de Identidad y Acceso

Una eficiente administración del acceso de los empleados a aplicaciones sensibles y datos es uno de los más grandes retos de seguridad para las organizaciones de hoy. A menudo, las organizaciones cuentan con una gran cantidad de usuarios privilegiados que, debido a una ineficiente administración, se presentan sobre privilegiados, es decir, que les son asignados más permisos de los que requieren para realizar su trabajo (Hummer, Kunz, Netter, Fuchs & Pernul, 2016).

Como medida para mitigar esto, las organizaciones han implementado sistemas centralizados para la administración de las identidades, permitiendo estandarizar el proceso de ciclo de vida de los usuarios, reducir las vulnerabilidades y cumplir con las regulaciones a nivel nacional e internacional.

Como lo mencionan Hummer et al. (2016) un típico sistema de IAM por sus siglas en inglés Identity Access Management (Administración de acceso de identidad) está compuesto por tres pilares: Procesos, tecnologías y políticas. El núcleo del proceso y ciclo de vida de la identidad se basa en el aprovisionamiento o desaprovisionamiento del usuario mediante la gestión de privilegios implementado con la tecnología disponible; controlados por un conjunto de políticas tanto a nivel tecnológico como la sincronización y almacenamiento de datos.

Se podría pensar que asegurar la identidad para el acceso a las tecnologías de nube es un asunto menor, pero en su investigación Al-Bayati, Clarke y Dowland (2016) encuentran que el CIF por sus siglas en ingles Cloud Industry Forum reportó para el año 2014 que el 79% de los negocios del Reino Unido usaron al menos uno de los servicios de nube y se calculó que para 2018 el gasto en los servicios de nube superaría los 180 billones de dólares. Esto nos da una idea de las grandes cantidades de recursos que se mueven a través del cloud y que no garantizar la identidad, puede causar grandes inconvenientes a una organización.

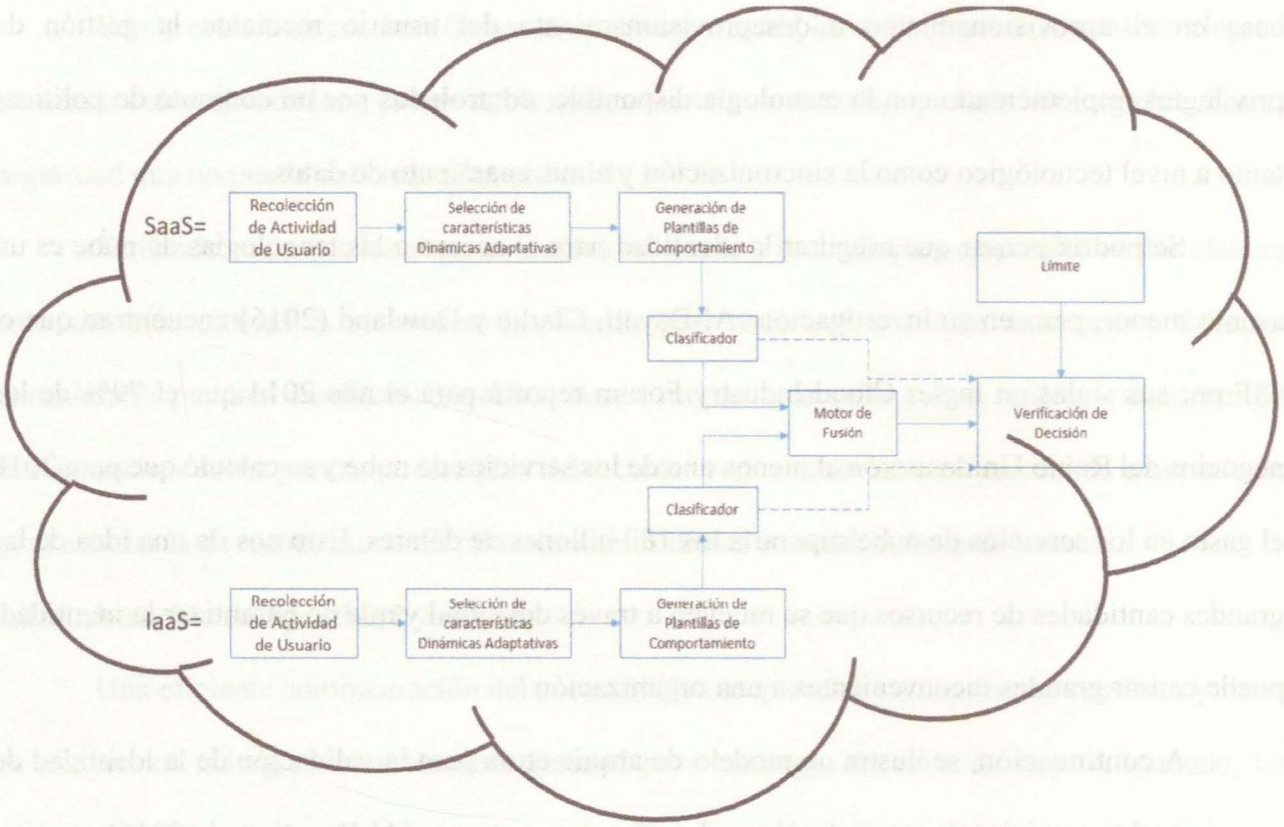
A continuación, se ilustra un modelo de arquitectura para la validación de la identidad de usuario en los servicios de computación en la nube, expuesto por (Al-Bayati et al., 2016).

Modelo de Arquitectura para Verificación de Usuario en un Proveedor de Nube

- Recolección de actividad de usuario. En esta etapa se recolectan y se realiza el preprocesamiento los datos de interacción del usuario y se almacenarán en una base de datos (Al-Bayati et al., 2016).
- Selección de características dinámicas adaptativas. Este componente se centra en identificar un conjunto de características del usuario, lo cual permitirá una clasificación más robusta. Estas características pueden ser hora, fecha de acceso, tipo de evento, nombre de la aplicación, uso de CPU, memoria e interacción con los servicios (Al-Bayati et al., 2016)

Figura 3

Modelo de arquitectura de verificación de usuario en un proveedor de servicio de computación en la nube



Nota. Adaptado de Adaptative behavioral profiling for identity verification in cloud computing: A model and preliminary analysis (Al-Bayati et al., 2016).

- **Generación de plantillas de perfil.** Las plantillas de comportamiento se obtienen a partir de los datos obtenidos en las etapas previas (Al-Bayati et al., 2016).
- **Clasificador:** Se implementará un clasificador adaptativo según la naturaleza de las características (Al-Bayati et al., 2016).
- **Motor de fusión:** Este motor decide si el sistema se basa en un solo perfil o en varios para tomar la decisión. Esto dependerá de cuántos servicios IaaS o PaaS el usuario haga uso, si es

uno solo el sistema podría trabajar con un solo perfil, pero si tiene más de uno podrían ser varios (Al-Bayati et al., 2016).

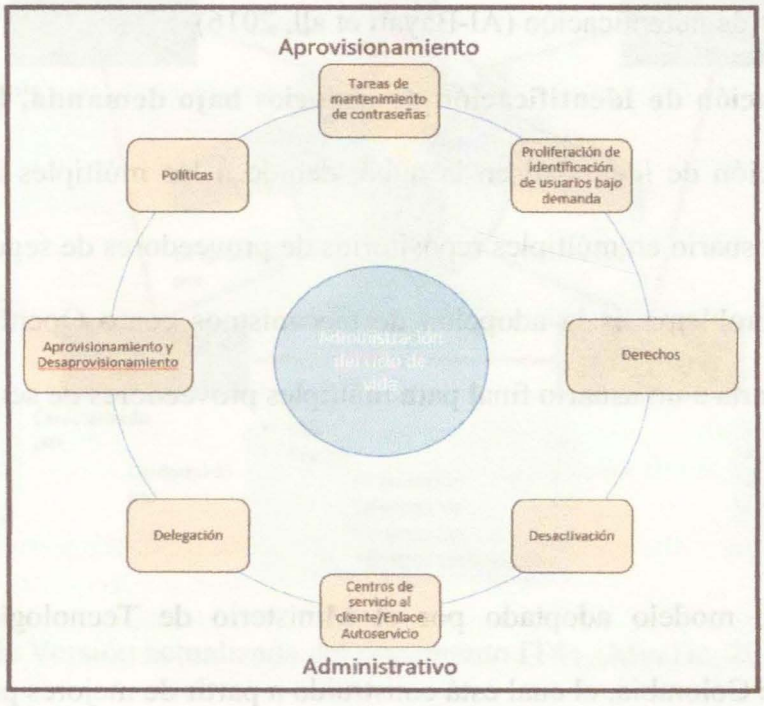
- **Decisión de verificación:** En este componente se toma la decisión. Se administran los puntajes obtenidos del clasificador; si el puntaje es cercano al umbral establecido se consideraría un usuario legítimo, de lo contrario se continuarían con otros indicadores antes de tomar la decisión final (Al-Bayati et al., 2016).

Ciclo de Vida de la Administración de Identidad

Este ciclo de vida tiene como función administrar de la identidad de los usuarios asociados a sus credenciales y derechos.

Figura 4

Administración del Ciclo de Vida de la Identidad



Nota: Modelo que ilustra el ciclo de vida de la identidad de un usuario en un sistema de información. Adaptado de Adaptive behavioral profiling for identity verification in cloud computing: A model and preliminary analysis (Al-Bayati et al., 2016)

Según Amaya (2016) el ciclo de vida gestiona los repositorios de identidades, define las fuentes de autoridad, os roles y las políticas, la automatización del aprovisionamiento automatizado y los mecanismos de control de acceso. El componente administrativo define reglas y provee componentes de autoservicio, El aprovisionamiento en *clouding computing* significa proveer en el tiempo exacto o bajo demanda las identidades requeridas para acceso a recursos (Al-Bayati et al., 2016).

El aprovisionamiento y desaprovisionamiento en tiempo real de una cuenta de usuario implica sincronizar instantáneamente con todos los proveedores de servicio participantes en el proceso; cualquier retraso en este proceso podría causar brechas de seguridad (Al-Bayati et all, 2016).

Algunas características importantes de este ciclo de vida son:

- **Autorización,** la cual se refiere a establecer atributos que especifican los derechos de acceso y privilegios de autenticación (Al-Bayati et all, 2016).
- **Proliferación de Identificación de usuarios bajo demanda,** la cual es un gran reto para la administración de identidad en la nube, debido a las múltiples identidades que puede adoptar un mismo usuario en múltiples repositorios de proveedores de seguridad; pero una forma para superar este problema es la adopción de mecanismos como OpenID, el cual asigna una identificación primaria a un usuario final para múltiples proveedores de servicio (Al-Bayati et all, 2016).

IT4+

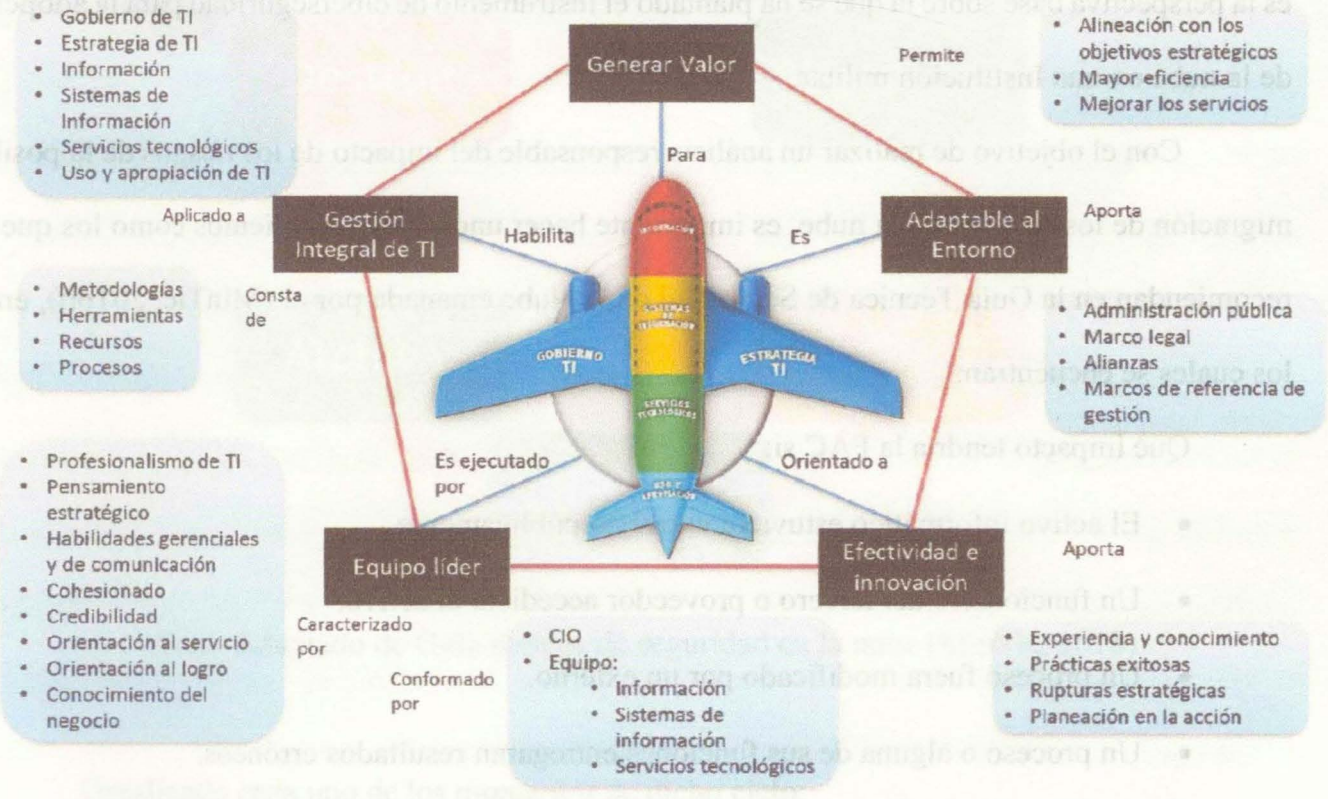
IT4+ es un modelo adoptado por el Ministerio de Tecnologías de Información y Comunicaciones de Colombia, el cual está construido a partir de mejores prácticas y experiencias aprendidas durante la implementación de estrategias de gestión de TIC durante los últimos 10 años.

Se basa en la gestión estratégica con tecnología, alineando la gestión tecnológica con la estrategia sectorial o Institucional, generando valor para el sector, la entidad, clientes y usuarios. Sus componentes son la Estrategia de TI, Gobierno de TI, Análisis de Información, Sistemas de información, Gestión de servicios tecnológicos y apropiación y uso (MinTic, 2016a).

En la siguiente figura se hace un resumen de las como esta aplicado este modelo, de qué consta, quién debe ejecutarlo, hacia qué está orientado, características y el producto que genera.

Figura 5

Que es el Modelo IT4+



Nota: Tomado de Versión actualizada del documento IT4+ (MinTic, 2016a)

La propuesta de valor que tiene el modelo IT4+ es la de generar un impacto profundo en el futuro de las organizaciones, donde la tecnología es un agente potencial de transformación y generación de valor, atenuando distintos problemas que enfrenta la tecnología, enmarcados en las siguiente categorías: La mayoría de los proyecto de TI no son exitosos, los proyectos de TI son costosos y no siempre es claro su retorno, los sistemas de información no se integran y no facilitan las acciones coordinadas, hay una amplia brecha entre los directivos y la gente de TI y la gestión de TI está rezagada frente a las nuevas tendencias del entorno (MinTic, 2016a).

Seguridad en la Nube

En esta sección, se abordará un tema de suma importancia en la presente monografía, pues es la perspectiva base sobre la que se ha plantado el instrumento de ciberseguridad para la adopción de la nube en una Institución militar.

Con el objetivo de realizar un análisis responsable del impacto de los riesgos de la posible migración de los servicios a la nube, es importante hacer unos cuestionamientos como los que se recomiendan en la Guía Técnica de Seguridad de la Nube emanada por el (MinTic, 2016b), entre los cuales se encuentran:

Qué impacto tendría la FAC si:

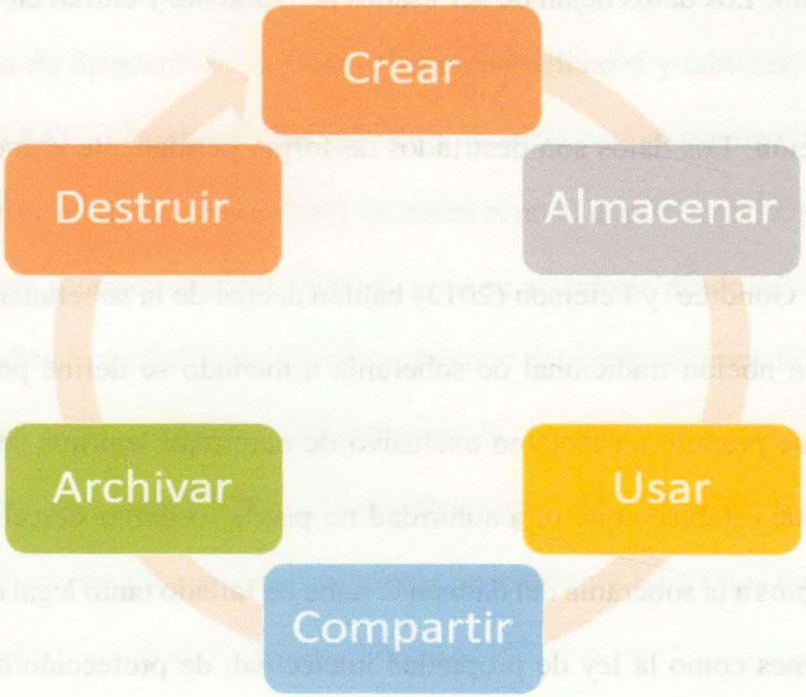
- El activo informático estuviera expuesto públicamente.
- Un funcionario del tercero o proveedor accediera al activo.
- Un proceso fuera modificado por un externo.
- Un proceso o alguna de sus funciones entregaran resultados erróneos.
- Si la información o datos fueran modificados de manera inesperada.
- Si se presentaran fallas de disponibilidad.
- La información se encontrará almacenada en otro país.

- Si se presentaran conflictos con el país donde se encuentren almacenados los datos.

Ahora bien, para un correcto tratamiento de los datos que se migrarían hacia la nube, es importante conocer el ciclo de vida de seguridad de los datos, lo cual se ilustra con la siguiente figura:

Figura 6

Ciclo de Vida de Seguridad de los Datos



Nota: Adaptado de Guía técnica de seguridad en la nube (MinTic, 2018)

Detallando cada uno de los momentos de dicho ciclo:

- **Creación**: Creación es la generación de nuevo contenido digital, o la alteración, actualización o modificación de contenido existente.

- **Almacenamiento**: Almacenamiento es el 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.

Ahora bien, Gondree y Peterson (2013) hablan acerca de la soberanía del dato, lo cual es un contexto legal la noción tradicional de soberanía a menudo se define por dos derechos: un derecho positivo que permite un reclamo exclusivo de autoridad legítima sobre un objeto y un derecho negativo que establece que otra autoridad no puede reclamar derecho sobre ese objeto; aplicar estos conceptos a la soberanía del dato en la nube ha fallado tanto legal como técnicamente, mientras que nociones como la ley de propiedad intelectual, de protección de datos y la ley de confidencialidad, otorgan derechos a los propietarios similar a la física pero no es posible disfrutar de las nociones tradicionales de soberanía debido a las ambigüedades en jurisdicción del dato en la nube que hacen que el "propietario" no pueda excluir el interés de otra parte.

Tomando estas consideraciones, surgen dos preguntas obligadas a la hora de planear una migración hacia la nube:

- ¿Quién accede a los datos Institucionales? Es importante conocer en cada uno de los sistemas de información que se desean migrar hacia la nube, qué usuarios acceden a estos datos, puesto que la FAC cuenta con distintos sistemas, de los cuales algunos son de uso general, otros de uso operacional, administrativo y logístico principalmente y en cada uno de ellos se debe discernir el tipo de usuario que estará accediendo.
- ¿Cómo pueden acceder a dichos datos? Con el esquema tradicional que existe actualmente en la Institución, la forma de acceder a los datos es en cierta forma limitada a los equipos de cómputo de escritorio, portátiles conectados a la red FAC y en algunos casos particulares a través de dispositivos móviles tales como celulares y tabletas; todos ellos siempre conectados a la red FAC. El gran cambio que se produciría con la arquitectura migrada hacia la nube no es principalmente el cómo acceder a los datos si no el dónde hacerlo, pues los dispositivos seguirían siendo muy seguramente los mismos, pero se accedería desde casi cualquier parte del mundo, esto dependiendo de los controles de acceso que determine el área de seguridad digital de la Institución. Otro punto clave a considerar es la posible utilización de dispositivos no Institucionales, conocido como BYOND por sus siglas en inglés (Bring Your Own Device) que se podrían usar para el acceso a los datos si no existen restricciones para ellos puestas en sistemas de seguridad de la nube.

Gobierno de la Información

Este concepto es fundamental a la hora de pensar en una migración hacia la nube, pues aquí la Institución debe considerar las políticas y procedimientos para gestionar el uso de la información en la nube y para esto se deben tener en cuenta las siguientes consideraciones:

Clasificación de la información. La clasificación le otorga un nivel o categoría a la información. Para esto es necesario recordar que existen dos leyes que rigen la clasificación de la

información en Colombia, la primera es la ley de inteligencia y contrainteligencia N° 1621 de 2013 (Congreso de Colombia, 2013), que clasifica la información de inteligencia en Ultrasecreto, Secreto, Confidencial y Restringido y la segunda es la ley de transparencia N° 1712 de 2014, la cual establece los niveles de clasificación Publico-Reservado y Público-Clasificado (Congreso de Colombia, 2014).

Políticas jurisdiccionales y de localización. Proporcionar gestión de configuración y mecanismos de aplicación de políticas para plataformas confiables que incluyen la aplicación de restricciones basadas en geolocalización es una forma de realizar una migración segura y basada en confianza (Bartock, Scarfone & Feldman, 2016). Basados en este enfoque, e importante definir dónde se pueden ubicar geográficamente los datos. Para este ítem, es importante tener en cuenta la jurisdicción legal colombiana que regula este aspecto al igual que la del país o región donde se vaya a almacenar nuestra información.

Autorizaciones. Diferentes autores plantean diversos métodos para controlar el acceso a los recursos en la nube, Punithasurya y Priya (2012) plantean 3 métodos de control: Control de acceso discrecional en el cual se otorgan los accesos a los usuarios basados en su identidad y las políticas establecidas. Control de acceso obligatorio, que se basa en el nivel de seguridad y los principios de lectura y escritura que pueden ser otorgados a un usuario y finalmente el control de acceso basado en roles, en el cual lo accesos son basados en los roles y responsabilidades de los individuos que deben ser identificados claramente en el ambiente en nube.

Así entonces, es importante tener claridad de qué tipo de método podría ser asumido por la Institución que desee migrar hacia la nube, con el fin de dar a los usuarios los permisos necesarios para cumplir todas sus funciones y mantener la seguridad de la información y la infraestructura.

Propiedad. La propiedad de la información es mucho más compleja de los que se podría pensar dependiendo del modelo de nube del que se hable. Hay dudas aún sin resolver en aspectos como la propiedad intelectual, la imagen de la marca, la visibilidad y el control sobre los datos que se subirán a la nube (Peña-López & Guillén, 2012).

En este enfoque, ¿Quién es el responsable final de la información? La Organización, el proveedor del servicio en la nube, ¿el país donde residen físicamente los datos? ¿Compartida? Establecer esos acuerdos de servicio y responsabilidades sobre los datos, debe ser un paso importante que va a permitir conocer los riesgos y adoptar medidas para controlarlos. Sin embargo, todo se define dependiendo del modelo de despliegue en nube que se desea incorporar, puesto que, en un modelo de nube privada o comunitaria, no se presentaría la dualidad o confusiones referente a quien es el dueño y responsable de los datos, porque indiscutiblemente serían de la entidad.

Ventajas y Desventajas de la Computación en la Nube

Dada la información recolectada y analizada en el presente capítulo, es posible establecer las ventajas y desventajas que trae consigo la adopción de la computación en la nube, lo que depende en muchas ocasiones del modelo de despliegue y tipo de nube que se desea adquirir, pero para los casos más generalizados se podrían enunciar las siguientes:

Dentro de las principales ventajas, como lo definen Cruz-Chávez, Peralta, Martínez y Cruz-Rosales (2014), está el acceso a la información desde cualquier lugar, contando con una disponibilidad de las 24 horas, los 365 días del año. Igualmente, está la facilidad de acceso al sistema, que puede ser desde dispositivos móviles, computadores portátiles o de escritorio, entre muchos más; hay servicios gratuitos o pagados según sea la necesidad y no es necesario combatir contra la saturación de un ordenador o una aplicación en nuestro sistema, pues basta con un

navegador web para acceder al recurso que es suministrado por el proveedor. Otra ventaja sin duda es la posibilidad de escalabilidad que ofrece la nube a las organizaciones, donde según sus requerimientos y necesidades, el crecimiento puede darse con tan solo unos clics y finalmente esta la capacidad de almacenamiento y procesamiento de datos, que se obtiene con tecnología de punta y sin necesidad de contar con las robustas infraestructuras en sitio que se requieren cuando se tienen los procesos de forma local.

Ureña (2012) hace una división de las ventajas según el sector donde se aplique, por ejemplo para la empresa privada unas ventajas importantes serían, el mejoramiento del índice económico y financiero, el hecho de poder enfocarse en el nicho de negocio apoyado con la computación en la nube, la rapidez de acceso; a la economía, organizaciones públicas y ciudadanos, ofrecería una mayor y mejor oferta de los servicios, la oportunidad de un gobierno abierto y con mayor alcance y cubrimiento y facilidad de acceso a la educación.

Pero también existen unas desventajas o retos que la nube debe superar para lograr tener una mayor aceptación y confianza en los usuarios. Para Cruz-Chávez et al. (2014), las principales desventajas son el acceso de la información de la organización estaría en manos de una tercera empresa; se generaría una dependencia de los servicios en línea; percepción de la pérdida del control y manejo de la información en la nube; dependencia fuerte de los proveedores de internet y de la velocidad ofrecida, lo que podría desencadenar aumento de costos y por último y no menos importante, la posibilidad de que delincuentes informáticos ataquen la infraestructura en la nube con la finalidad de hurtar la información o afectar en cualquier forma la prestación de los servicios.

También para Ureña (2012) existe la duda sobre la disponibilidad del servicio, representada en la garantía del cumplimiento de los niveles de acuerdos de servicio que puedan ser acordados con el proveedor para aquellos procesos que sean críticos en la organización; estas dudas son

importantes concertarlas en el momento de la adquisición de los servicios, dejando establecidos unos acuerdos favorables y exigentes de acuerdo con la necesidad del servicio. También estaría la falta de integración total entre las tecnologías y plataformas de los proveedores, que limitarían la migración de los datos y servicios entre plataformas a requerimiento del usuario.

Con la finalidad de ilustrar mejor al lector, las ventajas y desventajas se ilustran en la siguiente tabla:

Tabla 3.

Ventajas y Desventajas de la Adopción de la Tecnología Clouding Computing

Ventajas	Desventajas
Facilidad de acceso desde cualquier lugar con conexión a internet.	Información de las organizaciones en manos de un tercero (Dependiendo el modelo utilizado).
Aumento en el índice de disponibilidad de los servicios.	Dependencia de los servicios en línea y conexión a internet.
Facilidad de acceso a la información a través de distintos medios (Computadores, tables, móviles, etc)	Percepción de pérdida de control y manejo de la información (Depende del modelo seleccionado).
Facilidad en escalabilidad.	Aumento de la exposición de la información a todos los usuarios sen internet (Depende del modelo seleccionado).
Facilidad en la elasticidad de acuerdo a los requerimientos cambiantes de la organización.	Posibilidad de integración entre las tecnologías en sitio y en la nube.
Facilidad para el aumento en la capacidad de almacenamiento.	Dependencia de los acuerdos de niveles de servicio SLA ofrecidos por el proveedor en nube.
Facilidad en el procesamiento de datos.	

Ventajas	Desventajas
Ayuda en el mejoramiento de los índices económicos (Actualización tecnológica, administración, soporte, energía, mantenimiento, entre otros).	
Reducción de personal en administración de infraestructura.	
Facilidad de migración de los datos entre nubes.	
Capacidad de contar con plataformas de seguridad a la medida para protección de los datos e infraestructura.	
Mayor alcance y cubrimiento de los servicios hacia los ciudadanos (Aplicable para el sector Gobierno)	

Nota: Fuente elaboración propia basada en la literatura analizada

Es posible apreciar que hay muchas ventajas, pero también hay algunas desventajas; sin embargo, la mayoría de las desventajas enunciadas, se aplican a algunos modelos como nube pública o híbrida, disminuyendo considerablemente para los modelos de nube privada y comunitaria donde sería más notorio el apalancamiento que dan los servicios en nube para lograr un desarrollo tecnológico importante en una organización.

Capítulo 2

Entrevista a Expertos en Ciberseguridad y Tecnologías de Información

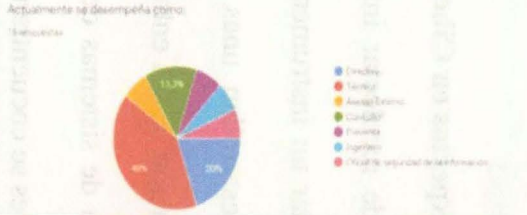
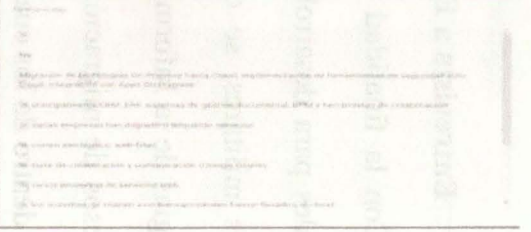
Con la finalidad de recolectar información que permita establecer los requerimientos funcionales para desarrollar un instrumento de ciberseguridad para la migración a la nube de entidades militares, se desarrollan unas entrevistas a personal experto en ciberseguridad y Tecnologías de la Información. Estas entrevistas se realizan a personal que haya estado inmerso en procesos de migración de sistemas de información a cualquier tipo de nube, de diferentes sectores dentro de los cuales se encuentran el público, privado, la academia y sector de defensa.

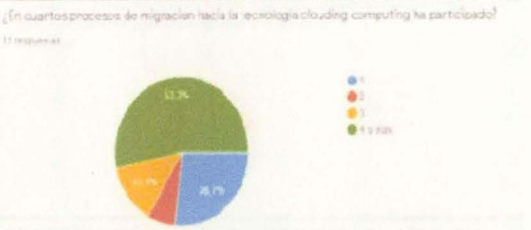
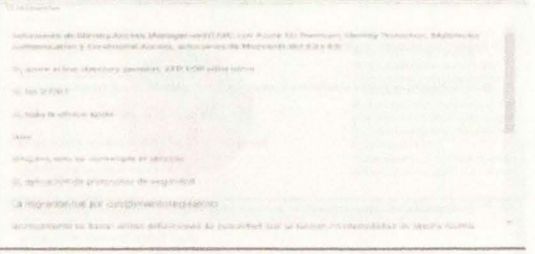
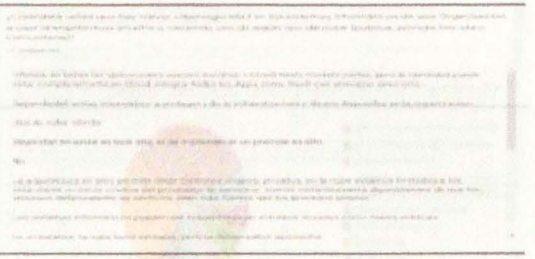
La totalidad de expertos a los que se les realizó la entrevista fue de quince (15), entre los cuales se encuentran cuatro (04) del sector público, siete (07) del sector privado, y cuatro (04) del sector mixto. Dentro del sector público encontramos personal perteneciente a entidades del sector militar y defensa, investigación y sector social; en el sector privado encontramos personal perteneciente a empresas de seguros, empresas de TI e implementadoras de productos de seguridad de la información, asesores externos y del ámbito financiero y en el sector mixto encontramos personal de empresas de Telecomunicaciones y energéticas. Es de aclarar que, aunque el enfoque del presente trabajo de investigación está dirigido hacia entidades militares, en la actualidad la única Fuerza Militar Colombiana que ha realizado algún proceso de migración hacia la nube es la Fuerza Aérea Colombiana, por lo cual no se realizan entrevistas a personas de las demás Fuerzas, pero si a personal de la Policía Nacional de Colombia quienes cuentan con plataformas en nube.

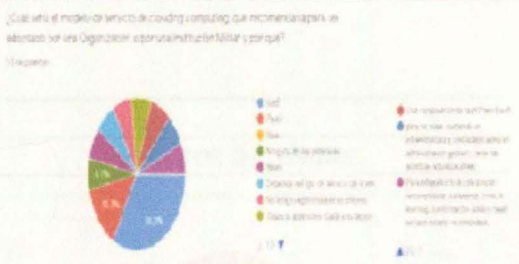
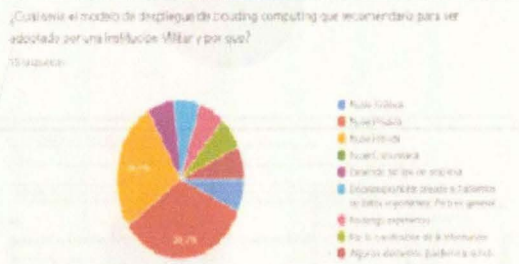
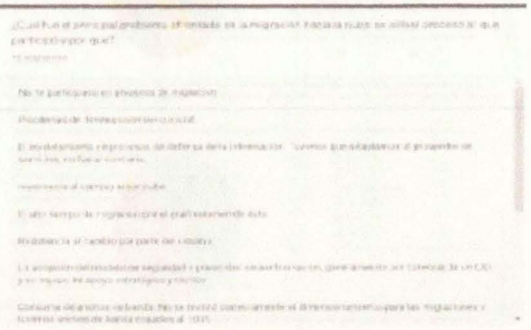
La cantidad de entrevistas realizadas se ajusta a los sectores más representativos en el ámbito Nacional y dan una perspectiva generalizada que es muy importante para el logro del objetivo del presente trabajo de investigación. Este personal cuenta con estudios de pregrado y postgrados relacionados con Tecnologías de la Información y seguridad informática o ciberseguridad y se desempeñan en sus entidades en dichas ramas, lo cual hace que sean las personas adecuadas para brindar apoyo con sus conocimientos.

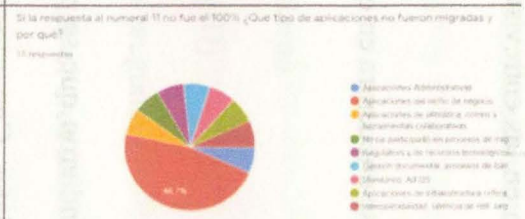
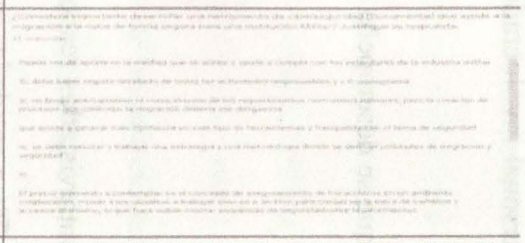
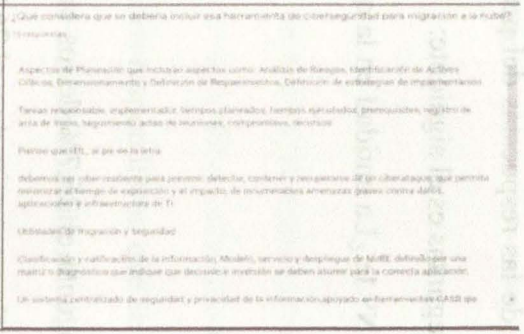
Tabla 4

Consolidado Entrevistas

DATOS CONSOLIDADOS ENTREVISTA A EXPERTOS		
PREGUNTA	**RESPUESTA**	**DATOS OBTENIDOS**
¿La entidad en la que se desempeña se encuentra en el sector? Público Privado Mixto Otra	A esta pregunta el 26,7% de los entrevistados respondieron que se pertenecian al sector público, el 46,7% al sector privado y el 26,7% a entidades mixtas.	
La entidad en la que se desempeña es de tipo: Organización Militar Academia Sector Financiero Sector Defensa Otra	A esta pregunta el 33,3% de los entrevistados respondieron que se desempeñan en entidades de servicios de tecnología, el 20% en el sector de servicios y consultoria, el 13,3% en Organizaciones Militares, el 13,3% en entidades de tipo financiero, el 13,3% en el sector gubernamental, y el 6,7% en entidades del sector energético.	
Actualmente se desempeña como: Directivo Técnico Asesor Externo Otra	Frente a esta pregunta el 40%(de los entrevistados respondieron que se desempeñan en el área técnica, el 20% en el área Directiva, el 13,3% en el área de consultoria, el 6,7% como asesor externo, el 6,7% en el área de preventa, el 6,7 en el área de ingeniería y el 6,7 en seguridad informática.	
¿Ha participado en la adopción de la tecnología de clouding computing para un sistema institucional o empresarial? Si la respuesta es SI explicar brevemente en cual. Texto de respuesta larga	Como respuesta a esta pregunta, el 93,3% de los entrevistados respondío que ha participado en procesos de migración hacia la tecnología clouding computing y el 6,7% no ha participado en algún proceso de este tipo.	

PREGUNTA	RESPUESTA	DATOS OBTENIDOS
¿En cuantos procesos de migración hacia la tecnologia clouding computing ha participaco? 1 2 3 4 o más	A esta pregunta, el 53,3% de los entrevistados respondió haber participado en mas de 4 procesos de migración hacia la nube, el 26,7% ha participado en 1 proceso de migración, el 13,3% ha participado en 3 procesos de migración y el 6,7% ha participado en 2 procesos de migración.	
Si la respuesta al numeral 4 fue afirmativa; ¿sabe si el proceso de migración hacia la nube se hizo basado en algún modelo que contemplara la ciberseguridad? Si la respuesta es Si explicar cual. Texto de respuesta larga	Frente a esta pregunta, 3 entrevistados respondieron que no se tuvieron en cuenta modelos de seguricad, 1 respondió que no sabe al respecto y 11 respondieron que se tuvieron en cuenta algunos aspectos de ciberseguridad.	
¿Considera usted que hay mayor ciberseguridad en los sistemas informáticos de una Organización al usar la arquitectura en sitio o haciendo uso de algun tipo de nube (publica, privada, hibrida o comunitaria)? Texto de respuesta larga	Como respuesta a esta pregunta, 8 entrevistados respondieron que es mas seguro la arquitectura en la nube, 2 respondieron que es mas seguro la arquitectura en sitio y 5 respondieron que depede mucho de factores externos, las formas de implementación y que realmente todo es susceptible de ser vulnerado.	

PREGUNTA	RESPUESTA	DATOS OBTENIDOS
¿Cuál sería el modelo de servicio de cloud ng computing, que recomendaría para ser adoptado por una Organización o por una Institución Militar y por qué? IaaS PaaS SaaS Ninguna de las anteriores Otra	A esta pregunta el 40% de los entrevistados respondieron que recomiendan la adopción de la nube bajo el modelo IaaS, el 13,3% el modelo PaaS, el 13,3% el modelo SaaS, el 13,3% respondieron que recomiendan una combinación de los modelos de nube, el 6,7% manifiesta no tener experiencia sobre el entorno, el 6,7% responde que depende del tipo de servicio que se quiera migrar y el 6,7% menciona que ninguna.	
¿Cuál sería el modelo de despliegue de cloud ng computing que recomendaría para ser adoptado por una Institución Militar y por qué? Nube Pública Nube Privada Nube Híbrida Nube Comunitaria Otra	Frente a esta pregunta el 33,3% de los entrevistados respondió que recomienda el modelo de nube privada, el 26,7% recomienda la nube hibrida, el 6,7% recomienda la nube pública, el 26,6% menciona que depende de los servicios y requerimientos a migrar y el 6,7% responde no tener experiencia en el sector militar.	
¿Cuál fue el principal problema afrontado en la migración hacia la nube en el(los) proceso(s) que participó y por qué? Texto de respuesta larga	En torno a esta pregunta, los entrevistados respondieron principalmente: -Problemas con el dimensionamiento de la solución en nube. -Falta de modelamiento de los servicios de seguridad en la nube. -Resistencia al cambio por parte de los usuarios. -Problemas de integración de aplicaciones legacy. -Problemas con la identidad de los usuarios en nube.	

PREGUNTA	RESPUESTA	DATOS OBTENIDOS
¿En el(los) proceso(s) de migración hacia la nube en los que participó, que porcentaje de las aplicaciones de la entidad fueron migradas hacia la nube? 0% - 24% 25% - 49% 50% - 74% 75% - 100%	Como respuesta a esta pregunta, el 40% de los entrevistados respondió que se migraron hasta un 24% de las aplicaciones de la entidad, el 33,3% respondió que se migraron entre un 25% y un 49% y el 26,7% respondieron que se migraron entre un 50% y un 74% de las aplicaciones.	
Si la respuesta al numeral 11 no fue el 100% ¿Que tipo de aplicaciones no fueron migradas y por que? Aplicaciones Administrativas Aplicaciones del nicho de negocio Aplicaciones de ofimática, correo y herramientas colaborativas Otra	A esta pregunta el 46,7% de los entrevistados respondió que no se migraron aplicaciones del nicho de negocio, las demas respuestas abarcan aplicaciones administrativas, de seguridad, de infraestructura crítica, de monitoreo, financieras y de datos confidenciales y correo electrónico.	
¿Considera importante desarrollar una herramienta de ciberseguridad (Documental) que ayude a la migración a la nube de forma segura para una Institución Militar? Justifique su respuesta. Texto de respuesta larga	En respuesta a esta pregunta, el 80% de los entrevistados respondió que si sería necesario desarrollar una herramienta de ciberseguridad, el 13,3% respondieron que no y el 6,7% respondió no tener experiencia en el sector militar frente a esta pregunta.	
¿Qué considera que se deberia incluir esa herramienta de ciberseguridad para migración a la nube? Texto de respuesta larga	Frente a esta pregunta hay varias opiniones, dentro de las cuales se encuentran: -Análisis de riesgos, identificación de activos críticos, dimensionamiento y estrategias de implementación. -Seguimiento de buenas prácticas como ITIL. -Contar con una adecuada ciberseguridad. -Clasificación de información, definir el modelo de despliegue. -Contar con unos adecuados acuerdos de niveles de servicio.	

Nota: Fuente Elaboración Propia

El análisis de las respuestas del personal involucrado en las entrevistas, discriminado en cada una de las preguntas es el siguiente:

Pregunta N° 1: ¿La entidad en la que se desempeña se encuentra en el sector?

- Público.
- Privado.
- Mixto.

A esta pregunta el 26,7% de los entrevistados respondieron que se pertenecían al sector público, el 46,7% al sector privado y el 26,7% a entidades mixtas. Con estos porcentajes se puede apreciar que se tiene una muestra importante de cada uno de los sectores en los cuales se puede encontrar una entidad, lo cual es de gran valor para tener en cuenta todas las perspectivas en los procesos de migración hacia la nube.

Pregunta N° 2: ¿La entidad en la que se desempeña es de tipo?

- Organización Militar.
- Academia
- Sector Defensa.
- Sector Financiero.
- Otro (¿Cuál?)

A esta pregunta el 33,3% de los entrevistados respondieron que se desempeñan en entidades de servicios de tecnología, el 20% en el sector de servicios y consultoría, el 13,3% en Organizaciones Militares, el 13,3% en entidades de tipo financiero, el 13,3% en el sector gubernamental, y el 6,7% en entidades del sector energético. La variedad de expertos a los que se les realizó la entrevista da un espectro amplio que permitirá conocer las opiniones y experiencias en distintos sectores sobre procesos de migración hacia la nube.

Pregunta N° 3: Actualmente se desempeña como:

- Directivo.
- Técnico.
- Asesor externo.
- Otro (¿Cuál?)

Frente a esta pregunta el 40% de los entrevistados respondieron que se desempeñan en el área técnica, el 20% en el área Directiva, el 13,3% en el área de consultoría, el 6,7% como asesor externo, el 6,7% en el área de preventa, el 6,7 en el área de ingeniería y el 6,7 en seguridad informática. Es importante para el presente trabajo de investigación, tener el punto de vista de los diferentes niveles dentro de una organización, pues las perspectivas pueden variar y cada uno tiene un aporte significativo para realizar los procesos de migración a la nube de la forma más acertada.

Pregunta N° 4: ¿Ha participado en la adopción de la tecnología de *clouding computing* para un sistema Institucional o empresarial? Si la respuesta es SI explicar brevemente en cual.

Como respuesta a esta pregunta, el 93,3% de los entrevistados respondió que ha participado en procesos de migración hacia la tecnología *clouding computing* y el 6,7% no ha participado en algún proceso de este tipo. Con esta afirmación, las posibilidades de que sus aportes en la entrevista contribuyan a la construcción de un adecuado instrumento de ciberseguridad para migración hacia la nube se incrementan debido a sus experiencias y conocimientos.

Pregunta N° 5: ¿En cuántos procesos de migración hacia la tecnología *clouding computing* ha participado?

- 1
- 2
- 3

- 4 o más.

A esta pregunta, el 53,3% de los entrevistados respondió haber participado en más de 4 procesos de migración hacia la nube, el 26,7% ha participado en 1 proceso de migración, el 13,3% ha participado en 3 procesos de migración y el 6,7% ha participado en 2 procesos de migración. Con estos datos se puede evidenciar que los entrevistados son personas idóneas que han participado en diversos procesos de migración y que tienen una experiencia importante para aportar al presente trabajo de investigación.

Pregunta N° 6: Si la respuesta al numeral 4 fue afirmativa; ¿sabe si el proceso de migración hacia la nube se hizo basado en algún modelo que contemplara la ciberseguridad? Si la respuesta es SI explicar cuál.

Frente a esta pregunta, 3 entrevistados respondieron que no se tuvieron en cuenta modelos de seguridad, 1 respondió que no sabe al respecto y 11 respondieron que se tuvieron en cuenta algunos aspectos de ciberseguridad como el MSPI (Modelo de Seguridad y Privacidad de la Información), estándares de casas fabricantes como Microsoft, lineamientos de la norma ISO-27001, ISO-27018, reglamentaciones de la ENISA (Agencia Europea de seguridad de las redes y de la información) y modelos de la NIST (National Institute of Standards and Techonology).

Pregunta N° 7: ¿Considera usted que hay mayor ciberseguridad en los sistemas informáticos de una Organización al usar la arquitectura en sitio o haciendo uso de algún tipo de nube (pública, privada, híbrida o comunitaria)? Justifique su respuesta.

Como respuesta a esta pregunta, 8 entrevistados respondieron que es más segura la arquitectura en la nube, 2 respondieron que es más segura la arquitectura en sitio y 5 respondieron que la seguridad depende mucho de factores externos, las formas de implementación y despliegue de las tecnologías y servicios. De igual forma, mencionan que en cierto modo todo es susceptible

de ser vulnerado y para evitarlo, la infraestructura debe ser robustecida con los protocolos debidos y siguiendo las buenas prácticas que se puedan adoptar al respecto.

Pregunta N° 8: ¿Cuál sería el modelo de servicio de clouding computing, que recomendaría para ser adoptado por una Organización o por una Institución Militar y por qué?

- IaaS
- PaaS
- SaaS
- Ninguna de las anteriores

A esta pregunta el 40% de los entrevistados respondieron que recomiendan la adopción de la nube bajo el modelo IaaS (Infraestructura as a Service), el 13,3% el modelo PaaS (Platform as a Service), el 13,3% el modelo SaaS (Software as a Service), el 13,3% respondieron que recomiendan una combinación de los modelos de nube, el 6,7% manifiesta no tener experiencia sobre el entorno, el 6,7% responde que depende del tipo de servicio que se quiera migrar se podría pensar en cualquiera de los tipos de nube y el 6,7% menciona que no recomendaría adoptar ninguna. Dadas las respuestas, se puede evidenciar que mayoritariamente se prefiere el modelo de IaaS en el cual el proveedor ofrece los recursos de procesamiento, almacenamiento y comunicaciones que el usuario requiere para ejecutar desde sistemas operativos, aplicaciones o cualquier tipo de software y en el cual el usuario es responsable por el soporte, mantenimiento y funcionamiento de lo que despliegue sobre la infraestructura del proveedor (Joyanes, 2012).

En la variedad de las respuestas se puede evidenciar que dependiendo del tipo de servicio que se proyecte migrar hacia la nube se podría seleccionar el mejor modelo, en definitiva, algunos entrevistados no se inclinan por algún modelo de servicio específico pues según manifiestan cado

uno de estos modelos tiene unas ventajas y desventajas que deben ser analizadas en cada caso particular.

Pregunta N° 9: ¿Cuál sería el modelo de despliegue de clouding computing que recomendaría para ser adoptado por una Institución Militar y por qué?

- Nube pública
- Nube Privada
- Nube híbrida
- Nube comunitaria

Frente a esta pregunta el 33,3% de los entrevistados respondió que recomienda el modelo de nube privada, el 26,7% recomienda la nube híbrida, el 6,7% recomienda la nube pública, el 26,6% menciona que depende de los servicios y requerimientos a migrar y el 6,7% responde no tener experiencia en el sector militar. Con esto se puede evidenciar que la mayoría de los entrevistados tienen tendencia a utilizar los recursos propios de las organizaciones militares para la formación de una nube privada donde se tenga el control total de la información e infraestructura tecnológica y la opción de nube pública donde no se tiene el control sobre los recursos ni el software es la menos recomendada. También un porcentaje importante concuerda en que la selección del modelo de despliegue se debe hacer dependiendo del tipo de servicio que se desee migrar.

Pregunta N° 10: ¿Cuál fue el principal problema afrontado en la migración hacia la nube en el(los) proceso(s) que participó y por qué?

Frente a esta pregunta, los entrevistados respondieron una variedad de problemas presentados, lo que es muy interesante para el presente trabajo de investigación, donde se observan problemas de dimensionamiento inicial de la migración, problemas con el modelamiento de los

procesos de seguridad de la información a migrar, problemas de seguridad y privacidad de la información acompañados de falta de apoyo de nivel estratégico y táctico, problemas de arquitectura y diseño, dificultades en la integración de aplicaciones *legacy* y problemas con la sincronización de las identidades que acceden a los servicios en la nube. Todas estas dificultades dan al presente trabajo de investigación, referentes muy importantes para fortalecer esos puntos débiles en los procesos y entregar una herramienta útil que aporte a los procesos de migración de una entidad militar hacia la tecnología *clouding computing.*

Pregunta N° 11: ¿En el(los) proceso(s) de migración hacia la nube en los que participó, que porcentaje de las aplicaciones de la entidad fueron migradas hacia la nube?

- 0 - 24%
- 25% - 49%
- 50% - 74%
- 75% - 100%

Como respuesta a esta pregunta, el 40% de los entrevistados respondió que se migraron hasta un 24% de las aplicaciones de la entidad, el 33,3% respondió que se migraron entre un 25% y un 49% y el 26,7% respondieron que se migraron entre un 50% y un 74% de las aplicaciones. Esto nos da un panorama que nos dice que aún la mayoría de las organizaciones han migrado ya un porcentaje considerable de sus aplicaciones y la tendencia hacia este comportamiento es creciente en todos los sectores del país.

Pregunta N° 12: Si la respuesta al numeral 11 no fue el 100% ¿Qué tipo de aplicaciones no fueron migradas y por qué?

- Aplicaciones Administrativas
- Aplicaciones del nicho de negocio

- Aplicaciones de ofimática, correo y herramientas colaborativas
- Otras (¿Cuáles?)

A esta pregunta el 46,7% de los entrevistados respondió que no se migraron aplicaciones del nicho de negocio, las demás respuestas abarcan aplicaciones administrativas, de seguridad, de infraestructura crítica, de monitoreo, financieras y de datos confidenciales y correo electrónico. Esta respuesta nos indica que las organizaciones aún prefieren mantener aquellos servicios cruciales para su funcionamiento y producción en las infraestructuras en sitio, con su seguridad y bajo su control total, optando por migrar hacia la nube aquellos servicios complementarios y no cruciales, que no contienen información de secretos industriales o información sensible.

Estas respuestas son muy importantes para tenerlas en cuenta a la hora de emitir un documento de ciberseguridad para la migración hacia la nube de una entidad militar, donde según la tendencia demostrada en esta pregunta, lo más viable sería mantener las aplicaciones de nicho de negocio militares en sitio.

Pregunta N° 13: ¿Considera importante desarrollar una herramienta de ciberseguridad (Documental) que ayude a la migración a la nube de forma segura para una Institución Militar? Justifique su respuesta.

Como respuesta a esta pregunta, el 80% de los entrevistados manifiesta que sí consideran importante desarrollar una herramienta de ciberseguridad para la migración a la nube para una Institución Militar, añadiendo opiniones que deben ser estándares obligatorios, con actividades claras y específicas, con responsables y cronogramas detallados, siguiendo las mejores prácticas y con políticas definidas. Un 13,3% de los entrevistados respondió que no lo ven necesario teniendo en cuenta que ya existen algunas guías y el 6,7% respondió que no tiene la suficiente experiencia en el sector militar para responder a este cuestionamiento. Con estas respuestas se puede evidenciar

que si es importante la construcción de la herramienta de migración hacia la nube y aunque el 13,3% de los entrevistados dice que ya existen algunos documentos guías, éstos son enfocados a organizaciones del sector privado, empresas u otros y no a entidades militares.

Pregunta N° 14: ¿Qué considera que se debería incluir esa herramienta de ciberseguridad para migración a la nube?

Frente a esta pregunta, los entrevistados tienen varias observaciones importantes, entre las cuales se destacan, tener claros y definidos responsables, tiempos de migración, seguimiento a actividades y recursos disponibles; de igual forma buenas prácticas como ITIL, sistemas de seguridad, privacidad y cifrado de la información; tener en cuenta políticas para dispositivos móviles y SLA (Acuerdos de nivel de servicio) y validación de entidades para acceso a la nube, entre otros. Estas respuestas son de suma importancia para el presente trabajo de investigación, puesto que, en la elaboración de la herramienta de ciberseguridad para la migración hacia la nube, se tendrán en cuenta estas opiniones de personal que ha participado en diferentes procesos de migración, para poder detallar el cómo sería una forma basada en buenas prácticas de realizar todas estas actividades y procesos.

Análisis de las Respuestas

Una vez recolectada la información de los expertos en ciberseguridad y Tecnologías de la Información, se identifican unos puntos importantes para consultar, lo cuales son sugeridos para implementar procesos de migración hacia la nube con buenas prácticas, estándares y protocolos de seguridad; entre estos tenemos algunos como:

Tener definida una solución de administración de identidad: Como lo mencionan (Hummer et al., 2016), un típico sistema de IAM por sus siglas en inglés Identity Access Management (Administración de acceso de identidad) está compuesto por tres pilares: Procesos, tecnologías y

políticas. El núcleo del proceso y ciclo de vida de la identidad se basa en el aprovisionamiento o desaprovisionamiento del usuario mediante la gestión de privilegios implementado con la tecnología disponible; controlados por un conjunto de políticas tanto a nivel tecnológico como la sincronización y almacenamiento de datos.

Contar con un múltiple factor de autenticación: la MFA por sus siglas en inglés Multi Factor Autentication es un sistema de seguridad que como su nombre lo sugiere, necesita más de una forma para la verificación de la legitimidad de la identidad en una transacción, combinando dos o más credenciales independientes basados en 3 pilares: lo que se (ej: una contraseña), lo que soy (ej: verificación biométrica) y lo que tengo (ej: una Smart Card); esto con el fin de crear capas de seguridad al momento de la autenticación y hacer más complejo un ataque de suplantación de identidad (Montañés, 2019).

Implementación de la ISO/IEC 27001: Este estándar internacional certificable perteneciente a la familia de los estándares ISO 27000 que tiene como objetivo ayudar a las organizaciones a proteger su información, entregando los diferentes requerimientos necesarios para establecer un Sistema de Gestión de Seguridad de la Información (Ñique- Morazzani, 2016).

Modelo de Seguridad y Privacidad de la Información MSPI: Es un modelo que contempla un ciclo de 5 fases que permite a las entidades gestionar adecuadamente la seguridad y privacidad de sus activos de información; estas fases son, diagnóstico, planificación, implementación, evaluación de desempeño y mejora continua (MinTic, 2016b).

Contar con herramientas tipo Cloud Acces Security Broker CASB: Esta tecnología actúa como un guardián, que permite a las organizaciones extender el alcance de sus políticas de seguridad informática más allá de su infraestructura física. Esta tecnología puede proporcionar puntos de control para el acceso, evitar descarga de información en dispositivos inseguros, aplicar

cifrado de información, implementar políticas de Data Lost Prevention DLP, políticas de Network Access Control NAC y garantizar el cumplimiento de políticas de intercambio de datos; todo esto basado en tres pilares que son, visibilidad, identidad y control de acceso (Kaur & Gupta, 2019).

Implementación de la norma ISO/IEC 27018: Esta norma permite a los proveedores de nube pública, evaluar riesgos e implementar controles para la protección de los datos personales almacenados. Esta norma se basa en leyes y regulaciones emitidas en la Unión Europea, por tanto, puede considerarse como un estándar o como un código de buenas prácticas para el proveedor de nube pública (Cassasola, Maqueo, Molina, Moreno & Recio, 2014).

Tener en cuenta buenas prácticas como Information Techonology Infrastructure Library ITIL: Este marco de buenas prácticas compilados por organizaciones públicas y privadas alrededor del mundo, cuyo objetivo es entregar servicios de TI de alta calidad, implementado principalmente para mejorar el enfoque de servicio al cliente y para incrementar el interés, efectividad y transparencia en el gobierno de TI (Alimam, Bertin & Crespi, 2017).

Conclusiones de la Entrevista a Expertos

Para establecer los requerimientos funcionales necesarios para la elaboración del instrumento de ciberseguridad en la migración a la nube, se desarrollaron 15 entrevistas a personal experto en ciberseguridad y aunque el porcentaje de aplicaciones que las organizaciones en los diferentes sectores de nivel nacional han migrado hacia la nube es aún cercano al 25%, la tendencia hacia la migración es un comportamiento creciente. Esto representa un reto importante para las empresas, pues como mencionan Márquez, Rosado, Mellado y Fernández-Medina (2014) la tendencia de la industria de TI hace que los clientes de estos nuevos modelos de prestación de servicios se enfrenten a desafíos nuevos en cuanto a la gestión de la seguridad de sus aplicaciones en este nuevo entorno.

Como comportamiento generalizado, se puede observar que las organizaciones aún mantienen cierto recelo de migrar sus aplicaciones de nicho de negocio hacia la nube pero si tienden a migrar servicios secundarios como aplicaciones administrativas, ofimática, servicios de correo electrónico, servicios de páginas y portales web, servicios de mercadeo, sistemas de planificación de recursos por sus siglas en inglés *Enterprise Resources Planning* ERP, sistemas de relación con clientes por su siglas en inglés *Customer Relationship Management* CRM y suites de trabajo colaborativo; cómo se puede apreciar, estos tipos de aplicaciones representan un sector muy importante de los tipos de sistemas que son utilizados por la mayoría de las organizaciones, de tal forma que la tendencia hacia la migración en un periodo de tiempo no muy largo podría ser inversa a los resultados obtenidos en la presente entrevista, donde es posible que se tengan migrados hacia al nube cerca del 75% de las aplicaciones y el 25% que representan las aplicaciones de nicho de negocio, sean las únicas que permanezcan en sitio.

También se puede observar que los entrevistados ven la necesidad de crear un instrumento de ciberseguridad para migración hacia la nube, puesto que, aunque existen diferentes metodologías y guías para migrar hacia la nube, en torno a organizaciones militares no existe una que tome en consideración aspectos como las regulaciones que las rigen, el tipo de información que se maneja y su funcionamiento en torno a la disponibilidad, entre otros.

Se pudo observar que la Fuerza Aérea Colombiana es la única entidad militar Colombiana que actualmente está haciendo uso de algún tipo de nube, pues al contactar personal del Ejército Nacional y la Armada Nacional, mencionaron que no han incursionado en la tecnología de nube en ninguno de sus modelos de servicio; así entonces, la Fuerza Aérea Colombiana se convierte en un caso importante para análisis de su proceso de migración a la nube y referente para la construcción del instrumento de ciberseguridad para migración hacia la nube, que es el objeto del presente trabajo de investigación.

Por último, se evidenció que las diferentes organizaciones que han realizado procesos de migración hacia la nube, se han enfrentado a diversos problemas, entre los cuales sobresalen algunos como modelamiento de los procesos de seguridad de la información a migrar, problemas de seguridad y privacidad de la información, problemas de dimensionamiento de la infraestructura, falta de organización y desconocimiento frente a las capacidades ofrecidas en la nube para la protección de la información; dificultades que se tienen como objetivo subsanar con el cumplimiento del objetico de la presente monografía.

Capítulo 3

Instrumento de Ciberseguridad para Migración a la Nube de Entidades Militares. Caso de Estudio Fuerza Aérea Colombiana

En el presente capítulo se desarrolla la creación del instrumento de ciberseguridad para migración hacia la nube aplicable a organizaciones militares, tomando como caso de estudio la Fuerza Aérea Colombiana; el cual se realiza basado en los aportes hechos por el personal entrevistado en el capítulo 2 del presente documento al igual que estándares de buenas prácticas y modelos existentes. Entonces, lo enunciado por Rashmi y Sahoo (2012) cobra mucho sentido en el presente trabajo de investigación:

> La nube es una promesa para todos los tipos de organizaciones y promete grandes beneficios por lo que la migración hacia la nube debe ser un proceso meticulosamente planeado, ya que se tienen que estudiar factores relevantes para que la migración no sea un proceso de resultados catastróficos, por lo tanto se requiere un modelo que oriente, aconseje y sirva como guía a las empresas, para que éstas se puedan basar en él y aprovechar la nube de manera eficaz (Rashmi & Sahoo, 2012, p. 17).

Ahora bien, las organizaciones militares son atípicas en su composición y dentro de su ecosistema se encuentran muchos roles, desde ámbitos comunes a las demás organizaciones como los campos administrativos, manejo de recursos, actividades de mantenimiento, áreas de comunicaciones, logística hasta otras más específicas como manejo de información de inteligencia militar y operacional y secretos de Estado. De igual forma, encontramos aspectos únicamente aplicables a Organizaciones militares como actividades de seguridad y defensa de la Nación, mantenimiento de la soberanía, lo cual hace que las características y formas de manejo,

almacenamiento, difusión y acceso a la información sean particulares y no sea posible seguir un modelo de migración a la nube de igual forma como se haría para una empresa de cualquier otro sector económico del país.

Un aspecto relevante a la hora de proyectar un proceso de migración hacia la nube de una Organización militar es la ubicación geográfica de los usuarios que accederían a los sistemas, puesto que dada la misión de las Fuerzas Militares de Colombia, existen unidades militares ubicadas en ciudades principales y secundarías donde se cuenta con un nivel de acceso a la red óptimo, pero también se cuenta con unidades en territorios alejados, fronteras, selvas y ríos, donde las comunicaciones se dan por enlaces satelitales de poco ancho de banda que cambian la perspectiva de una empresa del común.

Es importante también resaltar que las Fuerza Militares Colombianas cuentas con una red integrada de comunicaciones que ofrece conectividad a nivel WAN por sus siglas en inglés Wide Area Network o red de área ampliada, presente en algunos lugares donde no se cuentan con más operadores de comunicaciones comerciales; esto ofrece una ventaja para los servicios de TI que son canalizadas a través de esta infraestructura para dar salida hacia internet.

Dado este escenario y entendiendo que hacer el símil con alguna organización de otro sector del país es complejo y no sería acertado, se hace necesario elaborar un instrumento que ayude a realizar la migración hacia la tecnología clouding computing de forma segura y que le ayude a la organización a determinar cuáles son los sistemas y datos que debería migrar, hacia donde debería migrarlos y cuál debería ser la forma más acertada de hacerlo.

En la actualidad, no existe una metodología definida o un estándar ampliamente aceptado para que las organizaciones adopten un modelo específico de computación en la nube para sus infraestructuras de TI (Mohammad & Mcheick, 2011).

Cada organización define los requerimientos de integración y estandarización de sus plataformas y servicios de TI considerando el perfil de los procesos de los planes estratégicos de la organización, definiendo la arquitectura, organización y relaciones de la tecnología, acompañados de la visión general de la Institución (Chávez, 2017). Teniendo en cuenta estos conceptos, las organizaciones emplean las llamadas estrategias de migración, que son métodos específicos para cada caso de migración, en razón a que en muchas ocasiones una entidad utiliza una metodología propia basada en requerimientos específicos que difícilmente será aplicable a otro proceso de migración (Gutiérrez, Almeida & Romero, 2018).

Es así, como basados en diferentes metodologías estudiadas, modelos de migración hacia la nube, documentos de buenas prácticas y las recomendaciones dadas por los expertos en ciberseguridad y Tecnologías de la Información entrevistados, se elabora el siguiente instrumento de migración hacia la nube para entidades militares, desde la perspectiva de ciberseguridad.

El siguiente instrumento es de carácter orientar y no constituye obligatoriedad para las entidades:

Instrumento de Ciberseguridad para Migración a la Nube de Entidades Militares. Caso de Estudio Fuerza Aérea Colombiana

El presente documento se estructura en una seria de fases dependientes de su predecesora, las cuales deberían ser seguidas cuidadosamente con el fin de analizar la conveniencia de una migración de servicios y posteriormente conseguir un resultado satisfactorio en términos de productividad y seguridad.

Dados los resultados de la entrevista a expertos obtenidos en el capítulo 2 del presente documento y las recomendaciones para la selección del modelo de nube para una organización militar halladas en la literatura analizada en al capítulo 1, el instrumento de ciberseguridad para la

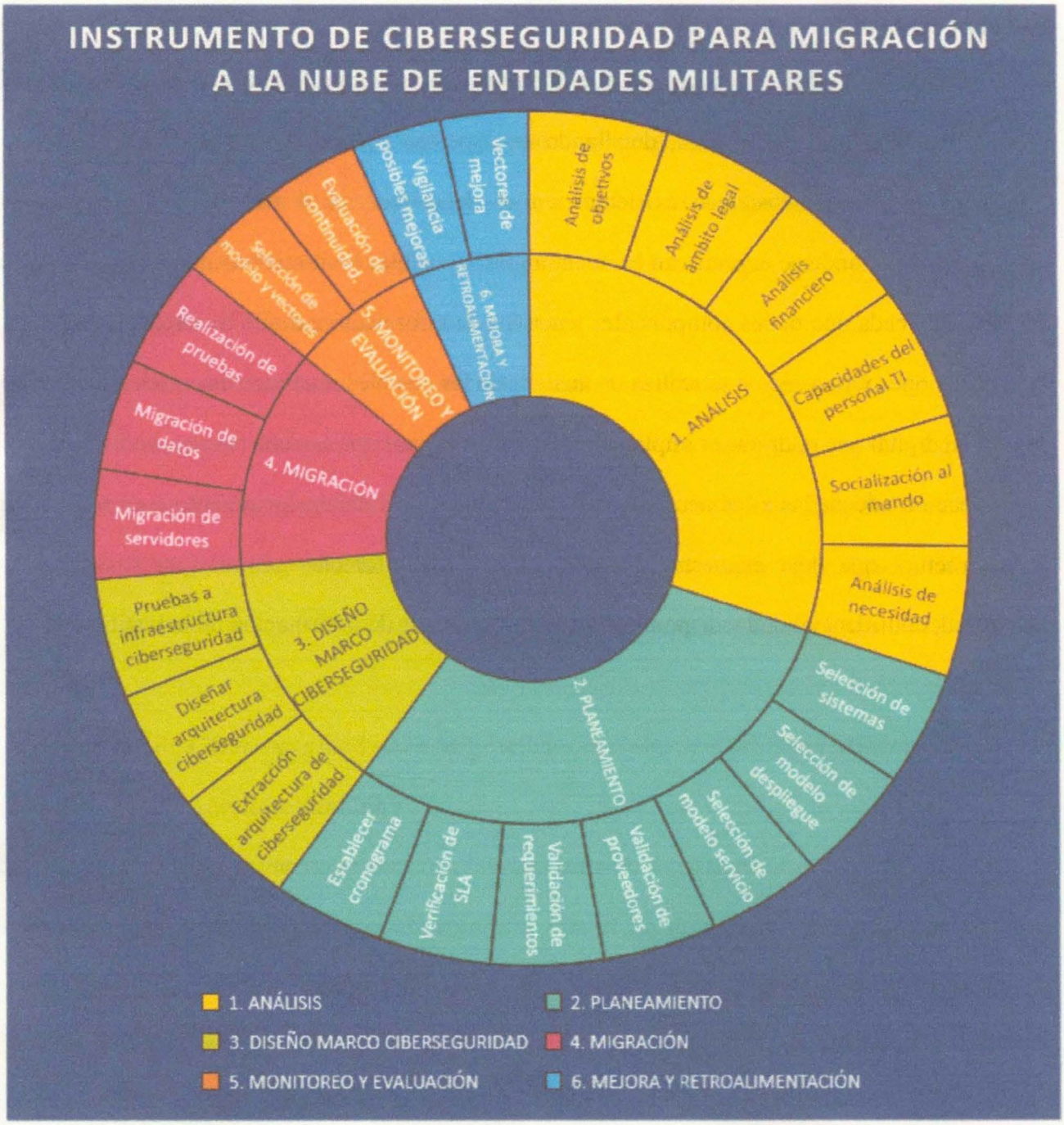
migración a la nube de entidades militares se centrará en los modelos de despliegue de nube privada y comunitaria.

Enfoque del Instrumento en Ciberseguridad

Este instrumento se realiza con el enfoque de ciberseguridad, para lo cual se detalla una fase exclusiva para esta temática, detallando en aspectos como la extracción del modelo de ciberseguridad de los sistemas existentes en el datacenter, el diseño de dicho marco de ciberseguridad, donde se especifican las tecnologías y posibles herramientas que podrían tenerse en cuenta en cada uno de los componentes y activos de información, desde las capas físicas hasta las aplicaciones y finalmente se realiza un análisis de las posibles pruebas a esa infraestructura de seguridad digital que podrían ser implementadas para asegurar que la nube cuenta con las medidas de protección adecuadas a las necesidades, sin caer en sobre dimensionamiento o en una pobre infraestructura que deje expuesta la información a los diferentes actores que amenazan la integridad, confidencialidad y disponibilidad de los sistemas de información de la Institución.

Figura 7

Instrumento de ciberseguridad para la migración a la nube en entidades militares



Nota: Ilustración del instrumento de ciberseguridad para migración a la nube, basado en fases donde la jerarquía mas alta se encuentra en el centro del gráfico. Fuente Elaboración Propia

Fase N° 1: Análisis

Análisis de alineación de objetivos estratégicos de la Institución. Determinar cómo va a ayudar la tecnología de la nube a cumplir los objetivos de la organización es fundamental, por esto antes de cualquier implementación es necesario revisar si los objetivos estratégicos de la Institución están alineados con los objetivos que se pudieran alcanzar con el uso de la tecnología de clouding computing (Gutiérrez et al., 2018). Por tanto, un análisis de alineación de objetivos debe conllevar a las siguientes actividades:

- Verificación de la alineación de la migración hacia la nube con el plan estratégico Nacional.
- Verificación de la alineación de la migración hacia la nube con el plan estratégico sectorial (Sector Defensa).
- Verificación de la alineación de la migración hacia la nube con el plan estratégico Institucional (Fuerza Aérea Colombiana, 2011).
- Verificación de la alineación de la migración hacia la nube con los objetivos estratégicos Institucionales.

Análisis del ámbito legal. En el análisis del ámbito legal se deben tener en cuenta como mínimo los siguientes aspectos:

- Verificar las leyes de carácter Nacional aplicables a la organización militar.
- Verificar acuerdo suscritos por el país aplicable a la temática.
- Verificar las leyes y normas de carácter sectorial (Sector Defensa).
- Verificar la normatividad interna de la Institución.

El documento de Consejo Regional de Política Económica y Social CONPES 3995 publicado el 01 de julio de 2020 por el Departamento Nacional de Planeación (2020), menciona o siguiente:

> El Ministerio de Tecnologías de la Información y las Comunicaciones en conjunto con el Ministerio de Defensa Nacional y la Dirección Nacional de Inteligencia, crearán una serie de guías metodológicas para la identificación y gestión de riesgos de seguridad digital en la adopción que las entidades del sector público hagan de tecnologías de la 4RI, tales como, IoT, blockchain, big data, computación en la nube e inteligencia artificial (p. 37).

En el análisis de documentos legales que enmarquen el uso de la nube para las organizaciones militares en Colombia, no se halló ninguno que impidiera tácitamente el uso de alguno de los modelos de nube, pero si se encuentran tal como en el documento citado anteriormente, directrices para fortalecer el uso de estas tecnologías emergentes y buscar el desarrollo nacional a través de su uso.

Por tanto, legalmente sería posible hacer uso de la tecnología de clouding computing en una organización militar siempre y cuando se tengan en cuenta particularidades como la reserva legal de información operacional, inteligencia, protección de datos personal, consagrados en la ley estatutaria 1621 de 2013 Ley de Inteligencia y ley 1712 de 2015 ley de transparencia (Congeso de Colombia, 2013 y 2015).

Análisis Financiero y retorno de la inversión. Es necesario realizar un comparativo de los costos actuales en mantenimiento, actualización y crecimiento de la infraestructura tecnológica sobre los costos en la nube, para lo cual se recomienda tener en cuenta como mínimo los siguientes aspectos:

- Costos en adquisición, configuración, puesta a punto y despliegue de la infraestructura.
- Costos del ancho de banda de conexión hacia internet.
- Costos de ancho de banda a nivel de conexión WAN (Conexión entre sedes de la Organización).
- Costos de soporte técnico de los equipos de la infraestructura en nube.
- Costos de licenciamiento del software para la virtualización de los servicios.
- Costos en la capacitación del personal para la administración de la infraestructura en nube.
- Costos del licenciamiento de sistemas operativos de los servidores en nube.
- Costos de licenciamiento del software para la prestación de los diferentes servicios migrados a la nube.
- Costos en horas hombre para efectuar la transición de los sistemas en sitio hacia el entorno de la nube.
- Costos de consumo de energía.

Finalmente en este proceso de análisis financiero, como mencionan Hoyos y Toro /2013) es importante que la organización se haga la siguiente pregunta ¿Cuál será el retorno de la inversión? y ¿En cuánto tiempo se verá reflejado el retorno?. Esta pregunta se podrá resolver teniendo en cuenta el análisis de cada uno de los ítems antes mencionados en el presente numeral y haciendo una comparativa de los costos que se asumirán una vez migrados hacia la nube.

Al finalizar, el ROI por sus siglas en inglés Return of Investment tal como relacionan Cavalcanti y Sobejano (2011) será calculado por la fórmula:

ROI = [(Ganancias-inversión) / inversión] * 100

Para los proyectos de tecnología las ganancias serán el resultado de la diferencia en los costos de adquisición y mantenimiento tecnológico de la infraestructura en nube sobre la infraestructura en sitio, sumando aspectos importantes como costos de personal, agilidad de acceso, movilidad y disponibilidad, que son factores un poco complejos de evaluar pero que significan grandes ventajas a la hora de hacer una comparativa.

Análisis de capacidades del personal de TI. Para pensar en una migración exitosa hacia la nube, la organización debe considerar las capacidades de su personal de Tecnologías de la Información; puesto que el sostenimiento de una plataforma en nube requiere habilidades que difieren del sostenimiento de un centro de datos en sitio. El personal que va a administrar estas tecnologías, va a necesitar capacitación sobre estas nuevas arquitecturas sobre las cuales se migrará la organización (Rashmi & Sahoo, 2012).

Estas capacitaciones no se deben tomar como un costo adicional para sostenimiento de la tecnología en la nube, puesto que son equivalentes a las capacitaciones y actualización de conocimientos que deben tener los administradores de los centros de cómputo en sitio para mantenerlo en funcionamiento, pro si se deben cambiar de paradigma, apuntando a la capacitación en nuevas tecnologías como virtualización y administración de los recursos en nube.

Socialización del proyecto al alto mando. El alto mando de la organización debe conocer y entender las consideraciones que llevan al área de TI a pensar en una migración de servicios a la nube. Pues como dicen Hausman, Cook & Sampaio (2013) los empleados técnicos y de negocio pueden trabajar juntos para determinar el impacto que tiene en la organización la migración de un proceso determinado a la nube, pero en últimas los proyectos siempre se traducen en costos y beneficios y esto es lo que se examina a nivel gerencial lo cual es la función de los altos mandos en las organizaciones militares.

Una vez que el alto mando haya entendido las razones del proyecto de migración, que tengan claras las ventajas, riesgos y desventajas del proyecto, será posible seguir avanzando técnicamente. Y es que no solo son costos, la implementación de un proceso de migración va a impactar directamente a muchas de las áreas de la organización, entregando nuevas formas de acceder a los recursos tecnológicos, suministrando nuevas capacidades y limitando algunas otras y estas son consideraciones importantes que los mandos deben tener claras para dimensionar las consecuencias que puede traer la adopción de la tecnología *clouding computing.*

Análisis de necesidad de la migración. En este punto, es importante que la organización tenga claro el resultado que espera obtener de la migración a la nube; en término de ingeniería, es responder a las preguntas ¿Va a mejorar mi competitividad? o ¿Voy a mejorar procesos de costos y productivos que aporten al cumplimiento de los objetivos estratégicos? (Gutiérrez & Almeida, 2019).

Si la respuesta a estas preguntas tiene un fundamento ampliamente reconocido por el comité de TI de la Institución, entonces valdrá la pena continuar el proceso para una migración hacia la nube.

Para el caso de una entidad militar colombiana, estas preguntas se podrían responder de la siguiente forma:

¿Qué problema se desea resolver? Se consigue principalmente solucionar problemas de disponibilidad de los servicios tecnológicos de la Institución, problemas de escalabilidad teniendo en cuenta las necesidades crecientes de los diferentes procesos misionales. Esto teniendo en cuenta que en el centro de datos en sitio se presentan indisponibilidades por mantenimientos y la accesibilidad a los sistemas de información solo se podía ofrecer desde dentro de la infraestructura tecnológica. Las necesidades de escalabilidad están siendo analizadas constantemente por las áreas

de TI de las diferentes Fuerza Militares, buscando presentar propuestas que puedan cubrir las necesidades, puesto que dentro de estas hay procesos sensibles para las instituciones.

¿Cómo se quiere mejorar un proceso apoyando con la tecnología en la nube? Hay numerosos procesos susceptibles de mejora con la ayuda de la tecnología en nube, por enumerar algunos, se encuentra los Planes de Recuperación ante Desastres por sus siglas en inglés DRP, para lo cual es muy factible un proceso en nube; procesos de analítica de big data y plataformas de seguridad informática como servicios en nube, son entre otros, algunos de los proyectos que a menudo se estudian para determinar su viabilidad de robustecerlos a través de plataformas en nube, con el modelo más apropiado.

Fase N° 2: Planeamiento

Selección de los sistemas de información susceptibles de migración. Una recomendación acerca cómo empezar a usar la tecnología de clouding computing, es no migrar a la nube los datos o procesos más sensibles, empezando por procesos poco críticos par la misión de la organización, que no manejen información confidencial y poco a poco cuando se vaya ganando confianza y experiencia en el ámbito, ir avanzando hacia algunos más complejos (Guerra, 2018)

Siendo esta, una recomendación generalizada entre la literatura analizada en la presente monografía y también expresada por los expertos en ciberseguridad y TI entrevistados en el capítulo 2, se considera importante que la entidad militar que desea incursionar en el proceso de migración hacia la nube seleccione desde esta perspectiva sus aplicaciones, para lo cual podría iniciar por algunas como:

- Servicios de correo electrónico no operacional, utilizados para temas administrativos, contractuales y demás que no contengan información clasificada, operacional, de inteligencia, secretos de estado o que afecten la soberanía Nacional.

- Sistemas de big data de información no clasificada.
- Servicios de seguridad informática para protección de las infraestructuras en nube y las que aún se mantienen en sitio.
- Sistemas de almacenamiento de información no clasificada.
- Servicios colaborativos para trabajos con información no clasificada.
- Sistemas de contratación pública.
- Sistemas de gestión documental de información no clasificada.
- Sistemas de inventarios y control administrativo de bienes y servicios.
- Sistemas de control educativo.

Una vez la entidad haya abordado los procesos de migración de los tipos de sistemas mencionados anteriormente y hayan ganado experiencia, creado confianza en a la infraestructura de nube (privada o comunitaria) y ésta se haya fortalecido con procesos, tecnología y recurso humano, se podrá pensar en iniciar procesos de migración de otros sistemas más críticos o sensibles.

Como una forma de ayudar a la entidad a seleccionar esos servicios susceptibles de ser migrados a la nube, a continuación se muestra una metodología basada en la clasificación de amenazas, examinando probabilidad de ocurrencia, impacto, tolerancia al riesgo y la cantidad de usuarios que podrían ser afectados Gutiérrez et al., 2018).

Tabla 5

Evaluación y Clasificación de Amenazas y Criterios de Probabilidad de Ocurrencia

Amenaza	
Actos intencionales	Ataques a la red, software malicioso, acceso no autorizado.
Actos no intencionales	Entradas inadvertidas o inválidas de datos, comandos mal ejecutados.
Amenazas naturales	Inundaciones, terremotos, tornados, avalanchas, deslizamientos de tierra.
Amenazas ambientales	Fallas de energía, polución, contaminación.
Probabilidad de Ocurrencia	
1	Muy baja. Es muy poco probable, generalmente ocurren menos de 1 vez cada 10 años.
2	Baja. Ocurren menos de 1 vez al año, pero más que una vez cada 10 años.
3	Moderada. Es algo probable, con rango de ocurrencia entre 1 y 10 veces al año.
4	Alta. De muy probable ocurrencia que se presentan entre 10 y 100 veces por año.
5	Muy alta. De probabilidad inminente, que se presentan más de 100 veces por año.

Nota: Adaptado de Modelo de auditoria para una red corporativa de datos para prevenir ciberdelitos (Camacho & Camacho, 2020)

Para la medición de la tolerancia al riesgo, se ilustra en la siguiente tabla, donde (Páez (2012) establece unos tiempos de respuesta mínimos que debido a la criticidad de la operación de las entidades militares, son ajustados par una respuesta más ágil.

Tabla 6

Clasificación de la Tolerancia al Riesgo

Tolerancia al Riesgo	Descripción
1	Sistemas de información misionales y servicios de TI de apoyo a toda la organización
6	Sistemas de información de apoyo a las labores administrativas y logísticas y servicios de administración y gestión de TI
12	Sistemas de información y servicios de TI de apoyo sólo a procesos específicos.

Nota: Tomado de La computación en la nube, como solución a los problemas de disponibilidad y continuidad en los servicios informáticos de la aeronáutica civil (Murcia, 2012)

La siguiente tabla ilustra el impacto a la organización, causado por una posible falla del sistema de información:

Tabla 7

Clasificación del Impacto de la Amenaza

Calificación del impacto	Descripción
10	Bajo: No afecta la misión de la organización, la reputación o los intereses.
50	Medio: Afecta notablemente la misión de la organización, la reputación o los intereses.
100	Alto: Impide el cumplimiento de la misión, la reputación o los intereses.

Nota: Tomado de La computación en la nube, como solución a los problemas de disponibilidad y continuidad en los servicios informáticos de la aeronáutica civil (Murcia, 2012)

Una vez analizados estos factores mediante la clasificación asignada, es posible determinar la criticidad de los servicios de TI susceptibles de ser migrados a la nube, mediante la siguiente tabla:

Tabla 8

Criticidad de los Servicios de TI

N°	Servicio de TI	Amenaza	Probabilidad de ocurrencia	Impacto	Tolerancia al riesgo	Usuarios afectados
1	Nombre del servicio	Actos intencionales				
		Actos no intencionales				
		Desastres naturales				
		Riesgos ambientales				

Nota: Tomado de Diseño de un modelo de migración a cloud computing para entidades públicas de salud (C. A. Gutiérrez et al., 2018).

Selección de modelo de despliegue en nube a usar. En el presente trabajo de investigación, dado el análisis de la literatura y la conclusión de los expertos entrevistados, se recomienda el uso del modelo de nube privada aunque teniendo en cuenta la gran cantidad de recursos que implica la adquisición de una nube privada para una entidad militar, se podría pensar en una nube comunitaria, donde pudieran fusionarse entidades afines, tales como el sector defensa, con lo cual la infraestructura sería propia y se compartirían por entidades afines en su misionalidad y con un mismo modelo de trabajo.

Selección del modelo de servicio en nube a usar. De acuerdo con el modelo de despliegue recomendado para una entidad militar que sería privada o comunitaria, no estaría disponible el modelo de servicio de Software como Servicio ni el modelo de Plataforma como Servicio, dado que la infraestructura sería propia o de la comunidad de entidades afines; por esta razón el modelo de servicio que se debería utilizar sería el de Infraestructura como servicio, donde la infraestructura es común y para el uso de las entidades del sector defensa y cada entidad estaría en la capacidad de desplegar allí sus diferentes sistemas, de mantenerlos y soportarlos, para dar los servicios requeridos a sus usuarios.

Validación de los proveedores de servicios en nube. Teniendo en cuenta los dos numerales anteriores, en este punto se tienen dos opciones, la primera es aplicable en caso de que la nube privada o comunitaria vaya a ser administrada por personal integrante de la o las entidades militares, en cuyo caso no se debería seleccionar ningún proveedor de servicio en nube, solamente se seleccionaría el proveedor o fabricante del hardware y software que se utilizaría para la creación de esta infraestructura.

El segundo caso es aplicable en la medida en que se decida tomar el modelo de nube privada gestionada, en la cual los proveedores ofrecen a los clientes una nube privada que es implementada, configurada y gestionada por un tercero, lo cual permite que las organizaciones con poca experiencia o escaso personal de TI presten un servicio de calidad haciendo uso de la infraestructura en nube (RedHat, 2020).

Conociendo esto, es importante conocer algunos criterios señalados por le empresa (RedHat, 2020) que se pueden tener en cuenta a la hora de seleccionar el proveedor podría realizar esa gestión de la nube privada o comunitaria que podría sería adoptada por la organización militar:

- Una ubicación cercana al centro de datos de la nube facilita el mantenimiento y soporte de la infraestructura.
- Asegúrese que el proveedor cumpla con las normas aplicables a la organización militar y entienda los riesgos de seguridad y complejidad de la entidad.
- Verifique el nivel de confiabilidad de ofrecen los proveedores, lo cual depende de la criticidad de los servicios migrados; generalmente son ofrecidos niveles del 99,9 o superiores.
- Asegúrese que el personal cuenta con la suficiente capacitación y experticia técnica para llevar a cabo las tareas encomendadas.
- Dimensione el alcance del soporte que quiere contratar; puede ser solo para la gestión de la nube o abarcar en mayor medida los requerimientos de TI que tenga la organización.
- Realice un análisis del costo y beneficio ofertado por el proveedor.
- Verifique la experiencia en tiempo en el negocio del proveedor y su calidad de desempeño (Gutiérrez et al., 2018).

Validación de los requerimientos técnicos de los sistemas a migrar. Para esta actividad, el área de infraestructura de la entidad militar deberá hacer un inventario detallado de los requerimientos que se están utilizando en el datacenter en sitio por cada uno de los sistemas propuestos a migrar hacia la nube, con el fin de dimensionar acertadamente las necesidades en la nube. Entre las principales consideraciones se deben establecer como mínimo las siguientes:

- Documentar la función del sistema de información.
- Documentar las áreas que hacen uso del sistema de información.
- Clasificar el tipo de información que maneja el sistema.
- Hacer el inventario de la arquitectura del sistema de información (Servidores front y back, bases de datos y su forma de conexión).

- Verificar las interacciones del sistema de información con otros sistemas y documentarlos para establecer dichas conexiones de nuevo luego de migrado a la nube.
- Verificar y documentar la forma en que acceden los usuarios y administradores al sistema de información.
- Documentar el consumo de red del sistema de información.
- Verificar la ubicación de los componentes del sistema de información (Granja de servidores, DMZ, servidores en diferentes sitios, entre otros).
- Consolidar la información acerca de versiones del sistema operativo sobre el cual corre el sistema de información (Incluye los servidores de aplicaciones y de bases de datos).
- Establecer la cantidad de "cores" utilizados por el sistema (Incluye los servidores de aplicaciones y de bases de datos).
- Establecer la cantidad de memoria RAM utilizada por el sistema de información (Incluye los servidores de aplicaciones y de bases de datos).
- Documentar el espacio de almacenamiento utilizado por el sistema de información (Incluye los servidores de aplicaciones y de bases de datos).
- Verificar si los diferentes licenciamientos utilizados en el sistema en sitio aplican para infraestructuras en nube, con sistemas virtualizados.
- Verificar la seguridad del sistema en sitio (controles fisicos y lógicos, seguridad perimetral, cifrado de datos en tránsito y en reposo, control de autenticación y gestión de identidades).
- Documentar el o los administradores funcionales y técnicos del sistema de información.
- Verificar si el sistema tiene sistema de respaldo.
- Verificar si soporta direccionamiento sobre IPv4 e IPv6,

Verificación de los acuerdos de niveles de servicio en infraestructura. Dado que el modelo de despliegue de la nube sugerido para la entidad militar es el privado o comunitario, estos acuerdos de servicio se podrían establecer siempre y cuando se elija el modelo de nube privada gestionada por un tercero, en cuyo caso la entidad podría requerirlos basados en el siguiente modelo:

Tabla 9

Niveles de Criticidad de las Afectaciones del Servicio

Prioridad		Descripción
1	Crítica	Las operaciones de la entidad están detenidas o severamente impactadas de manera que no se puede continuar su desarrollo. La operación es de misión crítica para la entidad y/o está en situación de emergencia.
2	Alta	La entidad experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida.
3	Media	La entidad presenta una pérdida de servicio menor, el impacto es un inconveniente.
4	Baja	No impacta el desarrollo de las operaciones militares, no se experimenta perdida del servicio y no se impide la operación de los sistemas.

Nota: Fuente Elaboración propia

Basados en la tabla de criticidad, se establecer los tiempos de respuesta que serían adecuados para resolución de las fallas presentadas en la infraestructura en nube para ua entidad militar.

Tabla 10

Tiempos de Respuesta para la Solución de Fallas

Prioridad		Descripción
1	Crítica	De manera presencial o remota en un tiempo máximo de 30 minutos.
2	Alta	De manera presencial o remota en un tiempo máximo de 90 minutos.
3	Media	De manera presencial o remota en un tiempo máximo de 4 horas.
4	Baja	De manera presencial o remota en un tiempo máximo de 24 horas.

Nota: Fuente Elaboración propia basado en análisis de literatura

Establecer un cronograma de migración. El cronograma para el proceso de migración es el siguiente paso, el cual se debe establecer lo más detalladamente posible, señalando actividades macro y las subactividades, los tiempos proyectados para la realización de estas actividades, los productos y los responsables. El siguiente es un ejemplo de cómo se podría establecer dicho cronograma.

Tabla 11

Propuesta de Modelo de Cronograma

Actividad macro	Sub-actividades	Plazo	Producto	Responsable
Actividad 1	Sub-Actividad 1	2 días	Producto 1	Responsable 1
	Sub-Actividad 2	1 día	Producto 2	Responsable 2
	Sub-Actividad 3	3 días	Producto 3	Responsable 3

Nota: Fuente Elaboración propia basado en análisis de literatura

Fase N° 3: Diseño de Marco de Ciberseguridad

En esta fase se va a proponer un diseño de ciberseguridad para desplegarlo en la infraestructura de la nube, bajo los modelos de despliegue privada o comunitaria.

Extracción de la arquitectura de ciberseguridad para el sistema en sitio. En la extracción de la arquitectura de ciberseguridad del sistema es la actividad en la que el modelo de seguridad es obtenido a partir del propio código y documentación, con la ayuda de procesos de ingeniería inversa; esto tiene como objetivo facilitar las tareas y pasos para que el analista pueda identificar los requisitos y controles de seguridad (Márquez et al., 2014).

Alineándonos con lo anterior, se deberían realizar mínimo las siguientes actividades:

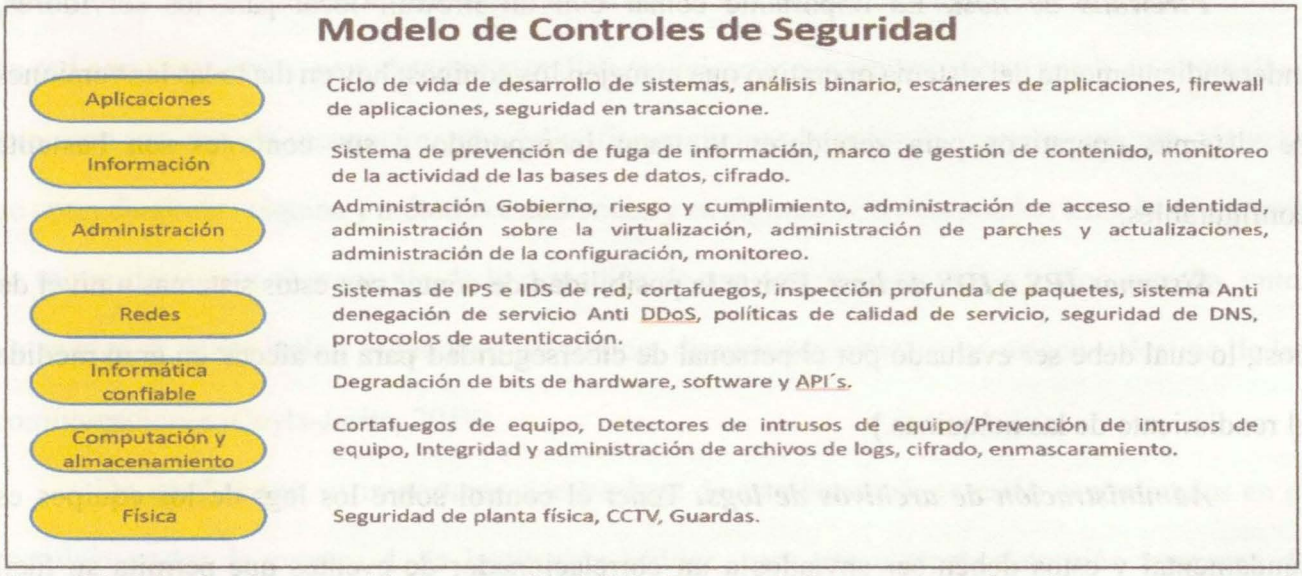
- Verificar los controles de seguridad físicos que se tengan en los servidores de aplicaciones y bases de datos del sistema de información.
- Verificar el sistema de protección de dispositivos con que cuentan los servidores del sistema.
- Verificar los privilegios de navegación hacia internet con que cuentan los servidores del sistema.
- Establecer los permisos de acceso de entrada y salida de los servidores del sistema.
- Establecer el modelo de parches y actualizaciones con que cuentan los servidores del sistema.
- Verificar los controles contra fuga de información con que cuenta el sistema de información a nivel físico y lógico.
- Verificar el sistema de cifrado de los datos en reposo y en tránsito desde y hacia el sistema.

- Verificar los controles lógicos de acceso al sistema, desde y hacia la red interna de la institución.
- Verificar los controles de seguridad perimetrales del sistema.
- Verificar la existencia y configuración de copias de respaldo ante fallos del sistema.
- Verificar la existencia y arquitectura de la alta disponibilidad del sistema.
- Verificar el sistema de gestión de acceso e identidad para ingreso al sistema.
- Verificar la existencia o no del módulo de auditorías de seguridad del sistema.
- Verificar los protocolos de comunicación internos y externos del sistema.

Diseñar la arquitectura de ciberseguridad para llevar a la nube. En este actividad se deben diseñar y definir los componentes que formarán el núcleo de la arquitectura de ciberseguridad para el sistema migrado a la nube (Márquez et al., 2014).

Figura 8

Mapeo del Sistema Cloud/Controles IG



Nota: Modelo de ciberseguridad para aplicabilidad en una infraestructura de nube capas. Adaptado de Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 (Brunette & Mogull, 2009)

Este modelo de ciberseguridad para una infraestructura en nube es bastante acertado y se ajusta a las necesidades de una entidad militar. Es por esto que nos vamos a centrar en la sección del Modelo de Controles de Seguridad y a explicar su inclusión en la infraestructura en la nube.

Control físico

Seguridad de la planta física. En este aspecto es importante tener un control estricto sobre el ingreso a la planta física de los equipos que conformarán la infraestructura de la nube privada o comunitaria que utilizará la entidad militar. Algunos controles mínimos que se deben tener son: Sistema de extinción de incendios, sistema de control de temperatura de precisión, adecuada iluminación y espacio, pintura y material adecuado, sistema neutralizador de estática, entre otros.

Circuito cerrado de televisión. Cámaras ubicadas dentro y fuera del datacenter.

Controles de acceso. Estos deben contar con autenticación de mínimo dos factores, donde se pueden encontrar acceso por reconocimiento de iris o huella, tarjeta de acceso o contraseña, entre los más comunes y eficientes.

Seguridad en los equipos y almacenamiento

Firewalls de host. Es importante contar con un firewall local para los servidores, independientemente del sistema operativo que manejen los equipos; hoy en día todas las versiones de sistemas operativos para servidores lo traen incorporado y sus controles son bastante configurables.

Sistemas IPS e IDS de host. Existe la posibilidad de contar con estos sistemas a nivel de host, lo cual debe ser evaluado por el personal de ciberseguridad para no afectar en gran medida el rendimiento de las máquinas.}

Administración de archivos de logs. Tener el control sobre los logs de los equipos es fundamental y estos deben ser enviados a un correlacionador de eventos que permita su fácil análisis.

Cifrado. Es necesario considerar el cifrado de los datos del sistema en la nube sin que esto afecte el rendimiento del sistema.***Enmascaramiento.*** Esta técnica consiste en sustituir los datos reales por otros realistas que cumplen con el formato estándar de cada tipo de dato y podemos encontrar el enmascaramiento persistente que es generalmente utilizado para trabajo en ambientes de pruebas y el no persistente, utilizado para trabajo en ambientes productivos (Prado, 2018).

Informática de confianza

Degradación de bits de hardware, software y API´S. Es importante realizar los procedimientos necesarios para tener un hardware y software de confianza, contando con la degradación de bits que con el tiempo van afectando la información (software) debido a la degradación paulatina de los bits como parte del desgaste de los dispositivos físicos (Amidon, 2016).

Red de datos.

Sistemas de IPS e IDS de red. Es imprescindible contar un con sistema de prevención y detección de intrusos a nivel de la red de la infraestructura en nube. Los sistemas más conocidos de IPS/IDS trabajan de dos formas, basados en uso indebido, que básicamente comparan el tráfico de red con unas firmas, para detectar el tráfico malicioso y existen los que se basan en anomalías, que usan patrones de reconocimiento del tráfico maliciosa basados en comportamiento, técnicas de aprendizaje de máquina y métodos estadísticos y en algunos sistemas pueden tener la autonomía de tomar decisiones al momento de la detección de una acción maliciosa o tráfico extraño, entre los cuales se puede incluir el bloqueo del tráfico, direcciones y máquinas origen y destino de las comunicaciones (Coyla-Jarita, 2019).

De igual forma, es importante que los logs de esta herramienta están centralizados en el correlacionador de eventos de la Institución Militar, para una correcta detección temprana de posibles eventos que atentes contra la seguridad de la infraestructura.

Firewall o cortafuegos. El concepto de firewall no es algo nuevo en el lenguaje de ciberseguridad, pero si es algo que aún está muy vigente en cualquier arquitectura de seguridad; El sistema de firewall se puede encontrar en hardware o software y ofrece seguridad a los activos a través de diferentes métodos como reglas de entrada y salida que permiten o deniegan el tráfico hacia ciertos recursos, el filtrado de tráfico basado en tipos de protocolos y aplicaciones; además proveen segmentación y delimitación de zonas de la red como la DMZ, que se encuentra entre la zona confiable y la no confiable y muchos de éstos sistemas incorporan características de filtro de navegación, IDS/IPS y NAC; la forma en la que los firewalls controlar el tráfico entrante y saliente de la red es a través de la imposición de una seria de reglas que permiten acceder o restringir el acceso a los recursos; dichas reglas son leídas y ejecutadas por el firewall de forma ascendente, teniendo la mayor prioridad siempre la que se encuentre más arriba (Mullo- Pilamunga, 2019).

Inspección profunda de paquetes. Muchos dispositivos en medio de la red hoy en día realizar inspección a los paquetes de tráfico, lo cual resulta benéfico tanto para el administrador de red como para los usuarios finales, siendo posible detectar paquetes maliciosos enviados desde un origen comprometido; de igual forma pueden prevenir fuga exfiltración datos sensibles de las organizaciones. Pero existe un reto importante para este procedimiento y se ha venido acrecentando con el auge de protocolos cifrados para la transmisión de datos, tales como HTTPS (Sherry,Lan, Popa & Ratnasamy, 2015).

Para poder inspeccionar HTTPS, los sistemas de inspección profunda de paquetes han creado unos protocolos de inspección de SSL de una forma que viola el enfoque de seguridad punto a punto y las garantías que ofrece SSL y algunas entidades como las del sector financiero tienen prohibición de tráfico que haya sido inspeccionado por razones de una posible alteración a los paquetes, que genere la corrupción de los mismos; esto acarrea un gran reto para la realización de la inspección de paquetes (Sherry et al., 2015).

Sin embargo, analizar los protocolos seguros como HTTPS se ha convertido hoy en una necesidad importante al interior de las instituciones militares, puesto que muchos ataques, tráficos malicioso, software de VPN para anonimizar la navegación y contenido con malware, viaja a través de este protocolo; por lo cual sería interesante examinar alternativas como las propuestas por (Sherry et al., 2015) con nuevas técnicas de inspección profunda de tráfico cifrado sin hacer intrusión en los paquetes pero garantizando un examen que proteja tanto la red como el usuario.

Sistema Anti Denegación de Servicio Anti DDoS. Los sistemas de protección contra ataques de denegación de servicio deben estar presente en la arquitectura de ciberseguridad para la nube privada o híbrida que adoptará la Institución Militar, puesto que se convierte en un blanco de interés para cibercriminales y hacktivistas que pudieran afectarla a través de las numerosas técnicas entre las cuales se encuentran ataques como la renegociación TLS, ataque de HTTP lento, inundación de paquetes HTTP, inundación de DNS, DNS amplificado, NTP amplificado, inundación de método SYN y protocolo UDP, inundación de peticiones PING, ente otros (Centro criptológico Nacional, 2020).

A continuación de listas unos procedimientos que pueden ser tenido en cuenta para implementarse en los dispositivos de seguridad perimetral de la infraestructura en nube, para mitigar los ataques de denegación de servicio simple y distribuida (Centro criptológico Nacional, 2020).

- Limitar el número de conexiones por dirección IP.
- Bloquear los rangos de direcciones IP de países con los cuales no se tenga ningún servicio.
- Activar las protecciones frente a ataques SYN flood o inundación de método SYN.
- Limitar el número de peticiones por segundo desde una misma dirección IP.

- Cerrar las conexiones HTTP lenta.
- Bloquear todas las direcciones IP sospechosas de realizar ataques de denegación de servicio utilizando Dynamic IP Restrictions.
- Implementar sistemas de cache que permitan gestionar peticiones sin que sean procesadas por el backend.
- Limitar el número de conexiones a los servidores de backend.
- Implementar sistemas captcha en los formularios públicos sin autenticación para evitar ataques por medio de robots.
- Establecer umbrales de conexiones por segundo.
- Instalar o configurar el firewall de aplicaciones destinado a los servidores de aplicaciones.
- Regular el número de conexiones máximas simultáneas.
- Controlar el número de descargas desde una única dirección IP.
- Mantener monitoreo y control sobre las peticiones más pesadas a las bases de datos Institucionales.
- ***Políticas de calidad de servicio.*** La calidad de servicio en la nube es la capacidad de proveer prioridad sobre aplicaciones, servicios de clientes específicos, flujos de datos o también garantizar ciertos niveles de rendimiento de la infraestructura, dependiendo siempre del modelo de despliegue seleccionado, lo que generalmente está asociado a un costo por estos privilegios (Bown & Jayapriya, 2014). Con estos estándares se evitan cuellos de botella en la transferencia de información, priorizando el ancho de banda para las necesidades de cada usuario (Abad & Cazar, 2014). Hoy en día muchos dispositivos traen inmersa la capacidad de hacer calidad de servicio, tales como enrutadores, conmutadores o firewalls.

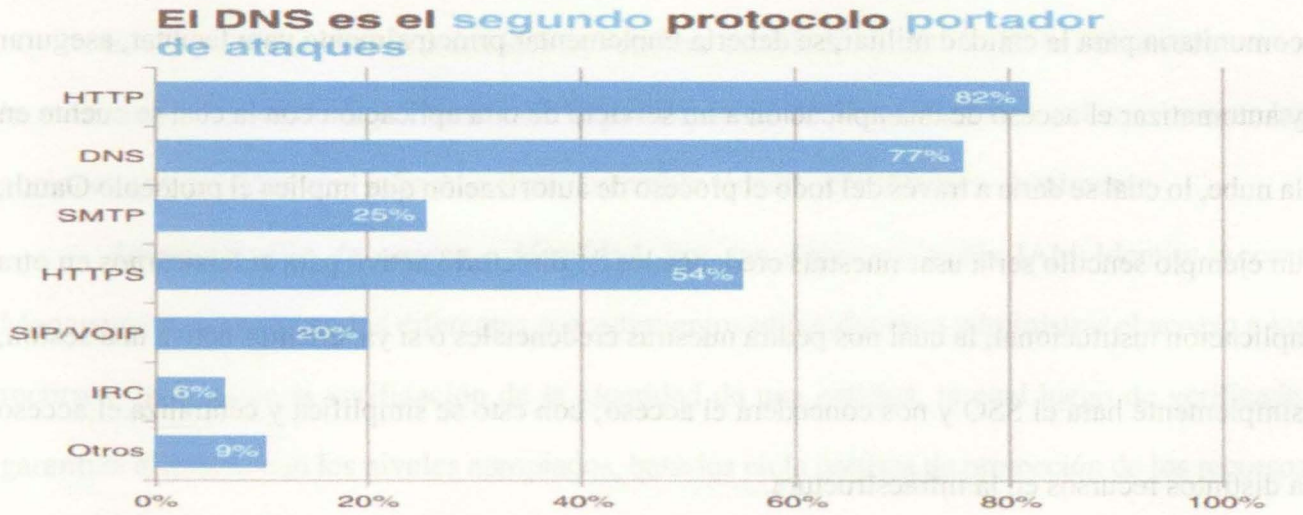
Es importante saber a qué aplicaciones o servicios se les va a dar prioridad, por ello, aunque las necesidades pueden variar dependiendo de la organización, entre las recomendaciones más generalizadas se encuentran los servicios de voz y video en tiempo real (Abad & Cazar, 2014)

Seguridad de DNS. La seguridad del protocolo DNS (Domain Name System) en las arquitecturas de ciberseguridad de las instituciones militares hoy en día no es una prioridad que ocupe muchos recursos y esfuerzos, puesto que es un vector de ataque reciente que ha cobrado fuerza y ha materializado ataques de exfiltración de datos y lentitud en la navegación sin que en muchas ocasiones nos hayamos enterado de que ha sucedido.

Como menciona López (2013), entre los principales tipos de ataques contra el DNS, se encuentran el envenenamiento de caché en el cual todas las solicitudes de resolver que le lleguen al servidor serán direccionadas al sitio malicioso; también existen ataques de DNS spoofing, amplificación de DNS donde se pretende desbordar la capacidad de respuesta del DNS y secuestro de DNS o DNS Hijacking entre los más comunes.

Figura 9

Vectores de Ciberataques



Nota: Tomado de Protección de la infraestructura DNS por dentro y por fuera (Infoblox, 2014)

Como se puede apreciar, el DNS es el segundo protocolo portador de ataques a nivel mundial, pero esto puede pasar inadvertido en las organizaciones debido a la dificultad del monitoreo de dichos ataques.

Para combatir este tipo de ataques, la infraestructura en nube podría contar con un firewall de DNS, que proteja las consultas DNS dirigidas por malware a dominios maliciosos impidiendo que los clientes se infecten y que se establezca comunicaciones con los sitios de comando y control de botnets. De igual forma estos sistemas pueden realizar el monitoreo de las solicitudes de los usuarios al interior de la Institución, generando estadísticas útiles para los análisis, al tiempo que pueden actuar como cache de DNS que ayude a mejorar los tiempos de navegación y el rendimiento de la máquina (Infoblox, 2014).

Protocolos de autenticación. Oauth es uno de los protocolos de autorización de inicio de sesión único SSO más ampliamente implementados y permite a una tercera aplicación tener acceso limitado a recursos protegidos sin compartir credenciales, a través de access tokens creadas por los proveedores Oauth. La metodología de roles que trabaja este protocolo se basa en el rol propietario del recursos, servidor de recursos, cliente y servidor de autorización (Alonso, 2015).

Aterrizando este concepto a la usabilidad que se le puede dar en la nube privada o comunitaria para la entidad militar, se debería implementar principalmente para facilitar, asegurar y automatizar el acceso de una aplicación a un servicio de otra aplicación con la cual se cuente en la nube, lo cual se daría a través del todo el proceso de autorización que implica el protocolo Oauth; un ejemplo sencillo sería usar nuestras credenciales de directorio activo para autenticarnos en otra aplicación institucional, la cual nos pedirá nuestras credenciales o si ya tenemos activa una sesión, simplemente hará el SSO y nos concederá el acceso; con esto se simplifica y centraliza el acceso a distintos recursos en la infraestructura.

Administración

Administración Gobierno, riesgo y cumplimiento. La implementación exitosa de un sistema integrado para la administración de Gobierno, riesgo y cumplimiento proporciona a la organización la capacidad de administrar sus riesgos, reducir los costos asociados a múltiples instalaciones y minimizar la complejidad para los administradores. Un sistema GRC es un concepto integrado que puede comprender desde organizar una auditoria anual hasta el establecimiento de controles continuos y monitoreo sobre los procedimientos, establecer roles y responsabilidades en los procesos misionales y usuarios del sistema y el procedimientos de análisis de los datos (Papazafeiropoulou & Spanaki, 2016).

Por supuesto, un sistema GRC es la herramienta fundamental para el control integral y gobierno de una organización y llevado al ámbito de las tecnologías de información, el uso de esta herramienta podría proporcionar a las oficinas de gobierno corporativo de TIC y oficinas de planeación, el establecimiento de metas a corto, mediano y largo plazo, la medición de los avances, el apego a los lineamiento de entidades como el Ministerio de Tecnologías de Información y Comunicaciones, las políticas sectoriales e Institucionales aplicables a la temática y tener una total organización de quién hace qué, cual es el objetivo y cuando lo habrá alcanzado.

Esto permitirá a los administradores, verificar cuando los objetivos de la infraestructura en la nube estén desviándose y a través de la participación de todos los interesados, encausar las acciones que permitan una infraestructura sostenible técnica, económica y legalmente.

Administración de acceso e identidad. Por sus siglas en inglés IAM Identity Access Management, consiste en los diferentes procedimientos utilizados para administrar el acceso a los recursos. Se basa en la verificación de la identidad de una entidad, la cual luego de verificada, garantiza el acceso con los niveles apropiados, basados en la política de protección de los recursos (Sharma, Dhote & Potey, 2016).

Las ventajas que podría tener una infraestructura en nube que cuenta con un sistema de gestión de acceso e identidad, son muchas, tales como la protección tanto de los datos asociados al usuario como los recursos de la organización, se hace un control de acceso eficiente basado en roles, se puede dar un cumplimiento más eficiente a la normatividad y regulaciones al respecto, reducción de costos administrativos en la gestión de las cuentas de usuario, incremento en la productividad por reducción en los tiempos de espera de la gestión de las cuentas y privilegios, funcionalidades de autoservicio, integración de servicios y repositorio de datos bajo una misma arquitectura de usuario y unificación de los datos del usuario a través de todos los sistemas de la organización (Montoya & Restrepo, 2012).

Un sistema de gestión de identidad con todas estas características puede solventar uno de los principales miedos de la adopción de sistemas en nube, que es el garantizar que una entidad es quien dice ser cuando intenta acceder a un recursos informático, lo cual para una organización militar es de suma importancia; este sistema de gestión deberá ir robustecido con un doble factor de autenticación, con un sistema de auditoria consolidado en el correlacionador de eventos y monitoreado por el personal de seguridad informática e integrado a todos los sistemas en la infraestructura en la nube privada o comunitaria adoptada por la entidad militar.

Administración sobre la virtualización. La virtualización se define como una tecnología que incluye abstracción entre el hardware y el software, el sistema operativo y las aplicaciones que se ejecutan sobre esta. Esta abstracción o multiplexación de un recurso físico oculta detalles técnicos detrás de la encapsulación, creando una interfaz externa que esconde una implementación subyacente para lo cual se vale de recursos como las máquinas físicas, sistemas operativos anfitriones, sistemas operativos invitados que corren sobre el anfitrión, software hipervisor, aplicaciones y redes principalmente (Nazareno, 2018).

Apoyado en este concepto, es posible decir que la administración de esta tecnología de virtualización que será el "core" de la infraestructura en la nube privada o comunitaria que adoptará la organización militar, es fundamental para poder explotar esas ventajas de la nube que entre otras son la flexibilidad, disponibilidad, escalabilidad, seguridad, costo, balanceo de cargas, entre otras.

Para esto es importante que la organización cuente con personal capacitado en la administración de esta tecnología, elegir cuidadosamente el hardware que soportará la infraestructura y el software hipervisor que se va a utilizar, contar con un soporte especializado y garantías para solución de inconvenientes.

Administración de parches y actualizaciones. La administración de parches es el proceso para identificar, adquirir, instalar y verificar los parches y actualizaciones de productos y sistemas; está enfocado a corregir problemas de seguridad y funcionalidad en software y firmware. Los parches son usualmente la forma más efectiva de mitigar las vulnerabilidades de software y con frecuencia son una solución efectiva. De igual forma, los parches pueden adicionar nuevas características al software y firmware, incluyendo capacidades de seguridad (Souppaya & Scarfone, 2013).

Sin duda mantener actualizado el hardware, firmware, los sistemas operativos, aplicaciones y complementos, es un punto muy importante para que la infraestructura en nube tenga una seguridad menos vulnerable antes ataques o fallas y para esto es importante contar un sistema de gestión de actualizaciones y vulnerabilidades, que no solo se resume en un software que ejecuta dicha tarea, es necesario contar con un programa que cuenta con personal capacitado, un proceso documentado y difundido en la organización, una infraestructura para pruebas de los parches antes del lanzamiento en producción, entre muchas otras cosas que corresponden al ciclo de gestión de parches.

Con esto se busca superar los retos importantes que a menudo se enfrenta el proceso de gestión de parches, que debe superar paradigmas como los tiempos de lanzamiento, la priorización de actividades y la prueba para evitar errores de parches que puedan afectar gravemente la infraestructura en cualquiera de sus componentes (Souppaya & Scarfone, 2013).

Administración de la configuración. La administración de la configuración es la disciplina de controlar la evolución de los sistemas y software. Esta administración compromete factores como la identificación de la configuración, control de la configuración, informes de estado, revisión, creación de procesos de administración y equipos de trabajo para la mejora de los productos. Con esto se pueden generar beneficios como un continuo seguimiento a los cambios, organización de tareas, asegurar la correcta configuración, cambios correctos sobre una línea base, reducción de costos, información ágil para reportes, entre otros (Paredes, Hinojosa & Ruiz, 2016).

Este concepto nos lleva a pensar que la organización necesita un sistema de administración de la configuración de la infraestructura en nube. Según Carrizo y Alfaro (2018), un sistema que provee un registro de los cambios o mejoras realizadas, controlando la documentación y entregables, tanto sus versiones como su modificación, es considerado como un sistema de administración de configuración.

Ahora bien, para un correcto funcionamiento de la infraestructura en nube, evitando errores humanos, que permita conocer quien ha hecho qué y cuándo, tener una trazabilidad de la configuración del hardware y software, es importante contar con un sistema de este tipo. En el mercado hay diferentes tipos de estos sistemas, pero es importante analizar el nivel de la tecnología de la nube de la organización, para asegurar la compatibilidad y aprovechamiento de todas las capacidades que un sistema de administración de configuración puede entregar.

Monitoreo. En el monitoreo de la infraestructura, se habla de dos tipos: activo y pasivo, cada uno con diferentes técnicas, estrategias, métricas y herramientas. En el monitoreo activo se introducen paquetes de prueba a la red o aplicaciones para medir su comportamiento y sirve para detectar problemas de red, diagnosticas retardos o pérdidas de paquetes, medir disponibilidad de recursos, entre los más importantes; el monitoreo pasivo se enfoca en recolectar datos y analizar el tráfico de la red usando herramientas como snifers, herramientas de monitoreo de ancho de banda y dispositivos con protocolos como SNMP (Simple Network Management Protocol) en sus diferentes versiones con el objetivo de caracterizar la red y contabilizar su uso (Junco & Rabelo, 2018).

Bajo este enfoque, las organizaciones se pueden preguntar ¿Qué monitorear? Respecto a esto Junco y Rabelo (2018) mencionan aspectos importantes como los anchos de banda, el consumo de CPU de los equipos, el consumo de memoria, el estado físico de las conexiones, los tipos de tráfico en la red, las alarmas y los servicios web. Ahora bien, al monitoreo de la red se le debe sumar el monitoreo de las herramientas de seguridad informática en todos los niveles, para lo cual todo debe estar centralizado hacia un correlacionador de eventos y usa serie de tecnologías que permitan un análisis automatizado de los comportamientos que se observan en la infraestructura. Esto se puede orientar a un modelo de SOC (Security Operations Center) capacitado para centralizar y dar respuesta a las necesidades de monitoreo y seguridad de la organización.

Información

Sistema de prevención de fuga de información. Por sus siglas en ingles conocido como DLP Data Lost Prevention, es un sistema que comprende un conjunto de herramientas destinadas a evitar el envío de información sensible, confidencial o crítica fuera de la organización y además

comprende las tecnologías que detectan, monitorean y evitan la fuga de información a través de la inspección de contenidos, propietarios, destinatarios, propósitos, medios y tiempos de transmisión de la información (Torres, 2015).

Los sistemas DLP están presentes desde hace algún tiempo en las infraestructuras de seguridad informática de las Fuerzas Militares Colombianas y adoptados en sus dos principales vectores que comprenden DLP de host y DLP de red, analizando la información en sus tres estados dependiendo de la ubicación que corresponden a almacenada, en uso y movimiento; por tanto, es un factor importante a considerar para la infraestructura en la nube privada o comunitaria que podría adoptar la organización militar contar con un sistema de DLP y un proceso que permita explotar estas capacidades y brindar seguridad a la información de la entidad.

}***Marco de gestión de contenido.*** Esta tecnología conocida del inglés como Content Management Framework CMF, que es una personalización de las soluciones CMS con la función de crear, actualizar, publicar, trasladar, archivar y remover la información de una organización. Esta es una tecnología que puede ser analizada por la entidad para ayuda en el manejo de su información, para gestionar de forma correcta y con más rendimiento la información que contendrán sus aplicaciones y sistemas de información (Horton, 2016).

Monitoreo de la actividad de las bases de datos. Monitorear las bases de datos de los diferentes sistemas anidados en la nube, es una tarea compleja que a menudo requiere de tecnologías especializadas en dicha labor. Diferentes herramientas en el mercado proveen capacidades de cifrado de las bases de datos y una completa auditoria, suministrando elementos para análisis de auditorías e investigaciones de tipo forense, detectando accesos no autorizados y actividades fraudulentas, permitiendo hacer filtros, monitoreos y bloqueos sobre el tráfico en la capa de aplicación de un servidor de aplicaciones web; se puede encontrar como hardware y

software y realiza sus bloqueos basado en las reglas y políticas previamente creadas que son generalizadas en dos grandes grupos llamados listas negras y listas blancas. Para alimentar estos dos grandes grupos, los Web Application Firewall WAF han adoptado varias técnicas que significan un porcentaje mayor en la detección de unos productos sobre otros, donde podemos encontrar inclusive técnicas modernas de análisis de comportamiento e inteligencia artificial (Tekerek & Bay, 2019).

Entonces, la organización militar debería pensar en contar con una herramienta de monitoreo de las bases de datos que tenga la capacidad de proteger los diferentes tipos de bases de datos que se puedan encontrar en sus sistemas de información que migrarían a la nube; bases de datos estructuradas y no estructuradas, de diferentes fabricantes y en diferentes estados (físicas o virtuales), para así centralizar en una sola herramienta el control de este activo fundamental en el funcionamiento de la infraestructura.

Cifrado. El cifrado de los datos, viene de la definición de la palabra inglesa encrypt, lo cual se puede sintetizar básicamente en la ciencia que apunta hacia la seguridad de los datos y documentos, utilizando códigos y claves que permiten almacenar información sensible que puede circular en medios ya sean públicos o privados y que solo podrá ser conocida por el emisor y receptor siempre y cuando tenga la forma de cifrarla y descifrarla (Medina, 2017).

El uso del cifrado de la información almacenada en la nuble privada o comunitaria para la organización militar debe ser un aspecto de total relevancia a la hora de planear la arquitectura de seguridad, es importante verificar las características de cifrado en la información en uso, e tránsito y en reposo, con las implicaciones que ello trae, puesto que es bien sabido que al someter la información a procesos de cifrado, se deben considerar variables el aumento en su tamaño lo que conlleva a que se contemple mayor espacio en almacenamiento y transporte.

El cifrado puede apoyar no solo la seguridad de la información como datos ilegibles, si no también, usarse para procesos de autenticación, no repudio y firma de documentos, características que apoyan en gran medida los procesos de la entidad (Corrales, Cilleruelo & Cuevas, 2014).

Aplicaciones

Ciclo de vida de desarrollo de sistemas. Conocido como SDLC por sus siglas en inglés Systems Development Life Cycle, según autores se puede componer de 8 fases entre las cuales encontramos la iniciación y fase de conceptualización, fase de planeación, definición de requerimientos, diseño y desarrollo, fase de pruebas, entrenamiento e implementación, operación y mantenimiento y finalmente la fase de disposición (Singletary & Baker, 2019).

Tener un ciclo de vida de desarrollo de sistemas o software bien estructurado y que se lleve a cabo plenamente por la organización, es muy importante puesto que genera software de calidad y además se debe incluir el componente de seguridad desde sus inicios, para así evitar retrocesos o demoras en la puesta en marcha de proyectos por brechas de seguridad.

Análisis binario. El análisis binario en la creación de aplicaciones y software, ayuda a crear software de mejor calidad y seguridad. Debido al crecimiento de los requerimientos y necesidades de los clientes, los desarrolladores tienen un panorama más complejo y es necesario apoyarse en herramientas que realicen en análisis binario de los desarrollos. El análisis del código es una técnica que ayuda a generar software con calidad, identificando a tiempo, errores en la escritura del código. En el análisis estático de código, se obtiene información sobre la estructura del programa permitiendo el estudio de los elementos estructurales, mientras que, en el análisis dinámico, se analizan las propiedades del sistema en tiempo de ejecución. Por medio de estos análisis se busca obtener características, métricas u otra información que permita realizar los

cálculos para la mejora del software, manteniendo la semántica original (Guamán, Pérez & Correa, 2020).

Contar con unas herramientas apropiadas para realizar este análisis del software, complementará las actividades del paso anterior (Ciclo de vida de desarrollo de sistemas) y permitirá que las aplicaciones que se van a soportar en la nube de la organización militar cuenten con calidad, alto rendimiento y se optimice el tiempo de los desarrolladores, incrementando la productividad y reduciendo costos asociados.

Escáneres de aplicaciones. Las herramientas de escaneo de aplicaciones son muy usadas hoy en día, especialmente con el fin de hallar vulnerabilidades de seguridad en las aplicaciones de las organizaciones. De ahí la importancia de tener una herramienta confiable, pues a menudo se encuentran tecnologías que generan un gran número de falsos positivos o verdaderos negativos. Los escáneres de vulnerabilidades suministran una forma automática investigar las vulnerabilidades evitando realizar tareas repetitivas y tediosas una y otra vez para cientos y miles de tipos de vulnerabilidades existentes (Joshi & Singh, 2016).

Siguiendo el camino para fortalecer las aplicaciones sobre la nube de la entidad y de acuerdo con lo anterior, es importante que la entidad cuenta con un escáner de aplicaciones, que permita identificar y corregir a tiempo las vulnerabilidades. Hoy en día en el mercado hay diversos tipos de herramientas que cumplen estas funciones, de ahí, la importancia de hacer un análisis minucioso de cuales se adaptan mejor a las necesidades de la entidad y bajo un proceso bien estructurado, realizar los escaneos con regularidad a las aplicaciones, lo cual debe ir seguido del respectivo plan de mitigación de vulnerabilidades.

Firewall de aplicaciones web. Muchos sitios web, aplicaciones y servidores reciben y procesan requerimientos de fuera de la red confiable de la organización, ocasionando que sean

vulnerables a diferentes tipos de ataques como inyección de SQL, cross-site scripting y denegación de servicio entre otros. Los firewall de aplicaciones web proporcionan una capa de seguridad entre esas amenazas y la infraestructura web externa de la organización. Los WAF (Web Application Firewall) proveen monitoreo, detección y prevención contra ataques en la capa de aplicación, inspeccionando el tráfico http y https, basándose en sus políticas (Verizon Media Platform, 2020).

El WAF puede proteger la aplicación web contra ataques DoS o DDoS, validación de protocolos, identificación maliciosa de clientes, ataques de firmas genéricas, ataques de firmas conocidas, troyanos y puertas traseras (Verizon Media Platform, 2020).

Una opción bastante viable para un WAF, es tomarlo como servicio, donde grandes compañías ofrecen unos niveles de seguridad bastante óptimos, con controles parametrizables de acuerdo a las necesidades de la entidad y debido a sus robustos recursos, pueden soportar ataques de gran volumen y entregar un tráfico limpio a las aplicaciones expuesta de la entidad militar.

Seguridad en transacciones.La seguridad en las transacciones hace referencia a las técnicas y prácticas que garantizarán la protección contra el espionaje y la modificación intencional de la información (Rane & Meshram, 2012)

Para proveer seguridad en las transacciones, Rane y Meshram (2012) recomiendan que la organización adopte los siguientes enfoques:

- Cifrado de los datos en reposo y en transmisión.
- Implementación del protocolo SSL (Security Socket Layer) que proveerá cifrado, autenticación e integridad de los datos en la transmisión.
- Implementación del protocolo HTTPS.
- Implementación de sellos de confianza de sitios y programas, que generan seguridad y confianza por parte del cliente.

- Contar con una firma digital, que será invalidada si los datos son alterados.
- Contar con certificados digitales en los servicios expuesto. Para los servicios expuestos hacia internet se recomienda un certificado emitido por una entidad externa y a nivel interno es posible contar con certificados auto firmados.

Verificar los acuerdos de niveles de servicio para la infraestructura de ciberseguridad en la nube. Teniendo en mente que el modelo de nube recomendada para la entidad militar será el privado o comunitario, los SLA requeridos para la infraestructura de seguridad se deberán exigir a la entidad que gestione la nube (En caso de que se adopte el modelo de nube privada gestionada), de lo contrario se deberá proyectar la implementación una infraestructura de ciberseguridad que se adapte a las necesidades de la entidad; en cualquiera de los dos casos, se podrá tomar como referencia la siguiente tabla, que ilustra los tiempos de disponibilidad que se podrían contemplar.

Tabla 12

Medición de Disponibilidad

Periodo de Análisis	Porcentaje de Disponibilidad	Porcentaje de Fuera de Servicio	Total de tiempo de falla
1 Año	98%	2%	7,3 días
	99%	1%	3,65 días
	99,9%	0,1%	525,6 min
	99,99%	0,01%	52,56 min
	99,999%	0,001%	5,26 min
	99,9999%	0,0001%	31,5 seg

Nota: Adaptado de Los 5 nueves: Mito o realidad (Barja, s. f.)

La entidad militar deberá determinar el nivel de disponibilidad que exigirá al encargado de gestionar su infraestructura en nube o de implementar las herramientas de ciberseguridad de tal

forma que proporcionen los niveles de disponibilidad deseados, teniendo en cuenta las implicaciones en infraestructura que conlleva el aumentar dicho porcentaje.

Realización de pruebas a la infraestructura de ciberseguridad en la nube antes de migrar el sistema. La gran cantidad de aplicaciones y protocolos en el ecosistema de la nube, pueden generar debilidades que los ciber delincuentes querrán explotar con diferentes fines, que van desde causar estragos, obtener beneficios económicos, ganar acceso a información restringida y fines políticos entre otros. Pero, con una constante verificación del estado de la infraestructura y los controles de ciberseguridad, la penetración a los sistemas de la nube podría hacerse mucho más robusta y dificultar que los ataques tengan éxito (Nikolov & Slavyanov, 2018).

Existen diferente posiciones sobre las pruebas de vulnerabilidad a los sistemas de ciberseguridad de una entidad, algunos autores mencionan que es más eficiente contratar una empresa externa especializada que realice una prueba de penetración completa cada cierta cantidad de tiempo y otros autores como Romero (2019) menciona que la propia organización puede realizar sus pruebas de penetración de forma constante incluso con el uso de herramientas libres que comúnmente se encuentran en distribuciones de Linux para seguridad y diferentes estándares de pruebas para sitios web, aplicaciones y servidores.

Verificando estos enfoques, es posible recomendar que la entidad militar cuente con estas dos formas combinadas de probar su infraestructura de ciberseguridad, puesto que una entidad externa podrá tener un enfoque particular que posiblemente detecte vulnerabilidades importantes y también es importante contar con herramientas propias que realicen un test constante a la plataforma y retroalimenten en tiempo real a los analistas de seguridad, quienes podrán evaluar para recomendar tomas las acciones pertinentes que permitan cerrar las brechas de seguridad que puedan poner el riesgo la información de la entidad.

Fase N° 4: Migración

Los pasos en esta etapa varían dependiendo del modelo de servicio y de despliegue seleccionado. Teniendo en cuenta los datos obtenidos en la entrevista a expertos en ciberseguridad y TI, la opción más recomendada para ser adoptada por una organización militar es el modelo de nube privada y siendo consecuentes con el costo de implementar una nube para una sola entidad militar, se hace más viable la adopción de una nube comunitaria, utilizada por entidades afines como las Fuerzas Militares Colombiana o el Ministerio de Defensa Nacional.

Migración de servidores. Aunque en el presente documento no se entrará en el detalle técnico de cómo realizar el proceso de la migración de la entidad militar hacia la nube, por no ser el objetivo de la monografía, en aspectos generales la entidad deberá replicar su infraestructura en sitio sobre la nube, luego probar que las máquinas y servidores son funcionales; posteriormente realizar una réplica de los registros DNS.

Migración de datos. Para migrar los datos, la organización se puede apoyar de un gestor de archivos, realizar un respaldo de las bases de datos, verificar la existencia de certificados de seguridad en la nube, analizar y replicar enlaces internos de los sistemas migrados para evitar redirecciones a los servidores antiguos y finalmente revisar el funcionamiento de los servicios migrados antes de iniciar las pruebas con usuarios (Guerra, 2018).

Para esta migración, se pueden tener en cuenta estándares de buenas prácticas como Information Technology Infraestructure Library ITIL y controles aplicables como los mencionados en la norma técnica ISO/IEC 27001 para el aseguramiento de los datos que se van a migrar.

Realización de pruebas. En algunas ocasiones y siempre bajo el criterio de la entidad, es posible mantener la infraestructura funcionando en paralelo, es decir, tener unas actividades en la

nueva infraestructura de nube y otras en el datacenter en sitio, hasta asegurar que el servicio en la nube sea completamente estable (Hoyos, & Toro, 2013).

De igual forma Hoyos y Toro (2013) plantean unas preguntas que es necesarios responder con el fin de asegurar que la nube está cumpliendo los requerimientos técnicos:

- ¿La herramienta ha estado disponible siempre que se ha requerido?
- ¿La herramienta puede soportar la carga de información que se requiere?
- ¿Se ha detectado alguna falla o problema que pueda comprometer la información almacenada en la herramienta?
- ¿El acceso y privilegios de los usuarios son los requeridos por la entidad?
- ¿Todas las funcionalidades de la herramienta están operando correctamente?

Fase N° 5: Monitoreo y Evaluación

Existen diferentes herramientas de monitoreo para la infraestructura en nube, que ayudan a supervisar el estado de factores críticos como la seguridad, el rendimiento y la disponibilidad del servicio (Hoyos & Toro, 2013). Teniendo en cuenta el enfoque de la nube privada o comunitaria para la entidad militar, estas herramientas de monitoreo serían exigibles si se opta por el modelo de nube gestionada por un tercero; pero, si la nube es gestionada por el personal de TI de la entidad, estas herramientas deberán adquirirse, junto con la capacitación del personal para poder detectar cualquier anomalía y corregirla en los tiempos y modo que se requieren.

Selección de modelo y vectores de Monitoreo. El monitoreo de la infraestructura en nube debe ser parte de un sistema integrado, que consolide toda la información y permita evidenciar alertas a nivel del hardware y software de la infraestructura, que permita hacer una medición del servicio, desempeño de los servicios e identificación de problemas, contando con un sistema

efectivo para gestionar las novedades halladas con el fin de dar solución y mantener estable la infraestructura (Gutiérrez et al., 2018).

El proceso de evaluación de la nube de la entidad, puede tener diferentes vectores de análisis, partiendo desde el técnico, donde se pueden evaluar aspectos como la elasticidad, la disponibilidad de la plataforma y los servicios, la escalabilidad de acuerdo al crecimiento y demanda en los sistemas de información; también otros vectores como el económico, donde se pueden analizar datos de recursos invertidos y los necesarios para su mantenimiento y soporte y por supuesto otro vector un poco más complejo de analizar que es la experiencia del usuario, que va alineada con toda esa capacidad de almacenamiento, cómputo y procesamiento que brinda una infraestructura en nube, pero que es complejo a la hora de medir por tratarse de algo intangible y en ocasiones subjetivo.

Evaluación de continuidad. Algunos autores como Aguedo y Astrada (2019) sugieren que la gran inversión que una entidad hace para migrar a una nube propia o comunitaria, puede implicar que desde el punto de vista económico pueda considerarse un camino de una sola vía, donde pasar de nuevo a la infraestructura de datacenter en sitio sería una gran pérdida para la entidad que además dejaría estragos a nivel técnico. En cierta forma este criterio es comprensible y es una consideración que debe ser bien analizada por la entidad militar, puesto que el costo inicial para la consolidación de una nube privada o comunitaria, que es el modelo recomendado para una entidad de seguridad del estado, es considerable y por tanto retroceder sería una opción poco viable.

Fase N° 6: Mejora y Retroalimentación

El proceso de migración hacia la nube no finaliza con la migración a la misma, puesto que se requiere de una revisión periódica de su funcionamiento integral, hardware, software,

interacciones, servicio y plataforma de seguridad, que permita asegurar que la infraestructura está acorde a los requisitos y parámetros que se requieren. También es importante estudiar las mejoras que puedan afectar el entorno de la seguridad en la nube o incluso los servicios que pueden ser considerados para su funcionamiento sobre esta plataforma (Márquez et al, 2014).

Vigilancia sobre posibles mejoras. La nube es un entorno sumamente cambiante, por lo que planear las mejoras con la suficiente antelación puede ser una tarea compleja; los problemas que hoy son objeto de estudio, hace pocos años no eran ni imaginados y posiblemente lo mismo pasará dentro de un par de años cuando estemos frente a tecnologías que dejarán sin sentido lo que se ha planeado. Sin embargo, es aconsejable realizar una vigilancia sobre las métricas y los niveles definidos por la entidad para garantizar el cumplimiento de las expectativas y así no perder el horizonte que se persigue con cada sistema (Márquez et al., 2014).

Vectores de mejoras. La mejora puede darse a muchos niveles, desde una infraestructura física más robusta, un ambiente de virtualización más eficiente, mejores anchos de banda, mejor calidad de software y una seguridad más madura, entre otros; lo cierto es, que la entidad deberá mantenerse a la vanguardia y definir con cautela y una buena relación costo beneficio, que cambios vale la pena implementar, sabiendo que aportaran valor a la misión Institucional, apalancado en la tecnología y la ventaja que puede dar una infraestructura en nube madura y robustecida.

Desde luego, la mejora no puede darse sin una adecuada retroalimentación, por lo cual se recomienda que como mínimo se realice el seguimiento de los siguientes aspectos, que servirá como insumo para una más acertada planeación de mejoras.

- Vigilar el hardware del sistema de nube, analizando su rendimiento y ciclo de vida.
- Validación del licenciamiento del sistema operativo de base de la nube.
- Mantener la actualización sobre el sistema de virtualización utilizado en la nube.

- Vigilancia sobre las actualizaciones y parches para los sistemas utilizados.
- Monitoreo de la capacidad de almacenamiento con que cuenta la infraestructura.
- Monitoreo de la capacidad de procesamiento y memoria de la infraestructura.
- Dimensionamiento del posible crecimiento de los sistemas que corren sobre la nube, evitando que los recursos físicos y de software sean insuficientes.

Caso de Estudio

Para la realización del presente instrumento de ciberseguridad para la migración a la nube de una entidad militar, se tomó como caso de estudio la Fuerza Aérea Colombiana, la cual esta soportada sobre unos procesos Gerenciales, Misionales y de Apoyo para el cumplimiento de su mandato Constitucional. Sobre los procesos de apoyo, se encuentra la logística de los servicios, que contiene a su vez las actividades relacionadas con las Tecnologías de la Información y Comunicaciones, transversales a toda la Organización.

Las TIC´s dentro de la FAC han tenido una evolución importante, pasando de ser una Dirección con poco personal, a convertirse en una Jefatura, con Direcciones enfocadas en cada uno de los pilares de las tecnologías, tales como Infraestructura, Gobierno de TI, Arquitectura de sistemas de información, Apoyo al Comando y Control de operaciones aeronáuticas y seguridad de la información, lo que deja entrever la importancia que se le ha dado a nivel Institucional.

La Institución cuenta con una variedad importante de sistemas de información, donde encontramos algunos comunes a muchas organizaciones como sistemas de administración de talento humano, control y gestión de inventarios, control de material de intendencia y dotaciones, sistemas de administración académica, sistemas de gestión documental, de gestión contractual y otros más enfocados a la misión y a la actividad militar, como sistemas de control de material aeronáutico, sistemas de reportes y control de misiones, sistemas de monitoreo y reporte de

ambientes geográficos, procesamiento y análisis de información de inteligencia militar, sistemas de administración y control de aeronaves remotamente tripuladas, sistemas de vigilancia aeroespacial, entre otros, que hacen de la FAC un completo caso de estudio.

Los sistemas de información se han construido basado en una arquitectura centralizada con el fin de tener un mejor control y administración de los recursos a todo nivel. De igual forma se han adoptado las mejoras prácticas, distribuyendo los diferentes componentes de los sistemas en zonas de seguridad de la red, tales como zonas desmilitarizadas conocidas comúnmente como DMZ, zonas de granja de servidores, clúster de bases de datos, servidores de frente y de fondo, entre otras características.

Por otra parte, la Fuerza Aérea Colombiana es la única entidad militar Colombiana que hoy en día cuenta con la adopción de algún tipo de nube, por tanto, se convierte en un referente importante para analizar procesos que ayuden a proyectar el uso del clouding computing como una herramienta de alta importancia en las Fuerzas Militares Colombianas.

Capítulo 4

Respuesta al Objetivo y Pregunta de Investigación

En el presente capítulo se dará respuesta al objetivo y a la pregunta de investigación planteados en el presente trabajo de investigación; de igual forma, se darán las conclusiones obtenidas del desarrollo de la monografía y se establecerán las recomendaciones para los trabajos futuros, que podrían desencadenarse tomando como base el presente trabajo.

Respuesta al Objetivo de la Investigación

Diseñar un instrumento de ciberseguridad para la migración a la nube en entidades militares. Caso de estudio: Fuerza Aérea Colombiana.

En la ejecución del presente trabajo de investigación de logró realizar el diseño del instrumento de ciberseguridad para la migración a la nube en entidades militares, basado en el análisis de la literatura pertinente y estudio del estado del arte, posteriormente basado en el conocimiento de personal experto en ciberseguridad y Tecnologías de la Información se obtuvo recomendaciones y experiencias importantes para el desarrollo del instrumento de ciberseguridad, pudiendo elaborarlo finalmente contando además con conceptos y literatura relacionada con el tema.

Respuesta a la Pregunta de Investigación

¿Cómo diseñar un instrumento de ciberseguridad para la migración a la nube en entidades militares?

Para el diseño del instrumento de ciberseguridad, en primera instancia se analizaron las falencias procedimentales que existen en las Fuerzas Militares Colombianas y tomando como caso de uso la Fuerza Aérea Colombiana, frente a procesos de migración hacia cualquier tipo de nube

(Pública, privada, híbrida, comunitaria), por lo cual se realizó el análisis de documentación, tal como lineamientos y reglamentación de carácter Nacional, sectorial e Institucional, estándares, legislación acerca del uso de la nube, conceptos de computación en la nube con todas sus características, tipos de seguridad en la nube, para poder tener un panorama claro de las ventajas y desventajas de la adopción de la tecnología de computación en la nube para una entidad militar.

De igual forma, se recopiló información de personal experto en ciberseguridad y Tecnologías de la Información, referente a temas como problemas presentados durante procesos de migración a la nube, principales modelos de despliegue utilizados, buenas prácticas y estándares utilizados en migraciones exitosas y finalmente recomendaciones para una migración exitosa hacia la nube para una entidad militar. De esta forma se pudo establecer una ruta para la creación del instrumento de ciberseguridad.

Conclusiones

Las Fuerzas Militares Colombianas no cuentan con un instrumento de ciberseguridad que les permita planear un proceso de migración hacia cualquier tipo de modelo de despliegue de nube de forma segura y de acuerdo con el avance de las tecnologías de información y las necesidades crecientes de servicios tecnológicos por parte de clientes internos y externos de las FFMM, pronto será necesario la migración hacia cualquier tipo de nube, lo que dependerá de las necesidades y lineamientos dados por los niveles superiores.

El Comando General de las Fuerzas Militares, el Ejército Nacional y la Armada Nacional de Colombia, tienen todos sus sistemas de información en infraestructura en sitio (Centros de datos propios) y la Fuerza Aérea Colombiana tiene igualmente todos sus sistemas bajo el esquema tradicional de infraestructura en premisas excepto la suite colaborativa de Microsoft 365, para lo cual requieren de capacidades en crecimiento constante, mantenimiento, licenciamiento, actualización y entrenamiento del personal administrador, para sostener estas infraestructuras que en muchas ocasiones se quedan cortas frente a las necesidades de los usuarios.

Se realizó el análisis del estado del arte y la literatura disponible respecto al tema de la presente monografía, identificando diferentes tipos de estándares, procedimientos y recomendaciones frente a la adopción de un proceso de migración hacia la nube de forma exitosa, lo cual sirvió para establecer un comparativo entre las ventajas y desventajas del uso de la tecnología de clouding computing para una entidad militar. Dado este resultado, se puede dar por cumplido el objetivo específico número 1 planteado para el presente trabajo de investigación.

Se realizó de forma exitosa una entrevista a personal experto en estrategias de ciberseguridad y TI, logrando conocer de primera mano las principales novedades presentadas en los procesos de migración hacia la nube en que éste personal ha participado anteriormente; de igual

forma, se obtuvieron recomendaciones frente a los tipos de aplicaciones que se deben migrar hacia la nube las cuales deberían ser todas excepto las que componen el núcleo del negocio o de carácter misional, las buenas prácticas y estándares aplicables, tales como ITIL, ISO/IEC 27001, entre otras y el modelo de despliegue recomendado para una institución militar que sería el de nube privada. De esta forma, es posible dar por cumplido el objetivo específico número 2, planteado en el presente documento.

Se construyó un instrumento de ciberseguridad para migración a la nube en entidades militares, basado en la literatura y estado del arte disponible acerca del tema, basado en la opinión y recomendaciones de personal experto en estrategias de ciberseguridad y tecnologías de la Información, teniendo en cuenta estándares, reglamentación, normatividad, legislación, buenas prácticas y recomendaciones basadas en procesos de migración a la nube de otras entidades. Este instrumento se divide en fases y cada una de estas fases contiene actividades específicas, que se detallan y enumeran las tareas que se podrían realizar por parte del personal inmerso en un proceso de migración hacia la nube, con el fin de cometer la menor cantidad de errores posibles y proteger la información en todos sus estados. Así, se puede dar por cumplido el objetivo específico número 3 de la presente monografía.

Con el estudio de la tecnología de clouding computing y su posible aplicabilidad en una entidad militar, se analizan casos de usos de gran relevancia en situaciones complejas como pandemias, acceso desde ubicaciones remotas, promoción de teletrabajo, entre otras, actividades que requieren de características propias de la nube como disponibilidad y facilidad de acceso. Es necesario tener en cuenta que estos casos pueden ser frecuentes en el mediano y largo plazo y es necesario que la entidad militar este tecnológicamente preparada para afrontar estos retos y ofrecer

los servicios requeridos con calidad, garantizando el cumplimiento de la misión Institucional (Fuerza Aérea Colombiana, 2020).

De acuerdo con la literatura analizada y las recomendaciones entregadas por el personal experto entrevistado, el modelo de despliegue de nube más acertado para una entidad militar, es el de nube privada; sin embargo, la implementación de una nube privada para una entidad militar puede ser bastante costosa y por esto el proyecto puede ser inviable; por esta razón, en el presente documento se recomienda también, el uso de una nube comunitaria, utilizada por entidades afines, tales como el Ministerio de Defensa Nacional, con lo cual los costos serían asumidos por varias entidades y podría ser muchos más viable el proyecto, manteniendo la seguridad y propiedad sobre los datos y la infraestructura.

Importantes estudios referentes al uso de la nube, reflejan que en los próximos años, se podría dar un fenómeno en el cual el 50% de todas las aplicaciones de tipo empresarial que corren sobre la nube pública, se migrarán a infraestructuras de nube privada, por razones como seguridad, gobierno de la información, ahorro de costos y recuperación de la sensación de control sobre la información; lo que refuerza la recomendación realizada en la presente monografía, de la adopción de la nube en sus modelos de despliegue de forma privada o comunitaria para una entidad militar.

Recomendaciones

Las Fuerzas Militares deben hacer un análisis cuidadoso de la necesidad de abordar la tecnología de clouding computing para sus procesos digitales, tal como se planteó en el presente documento, es importante seguir unas etapas y pasos definidos previamente, con el fin de tomar las mejores decisiones en pro de la mejora en la prestación de los servicios tecnológicos y siempre protegiendo la información Institucional.

Es importante realizar mesas de trabajo conjunto de nivel sectorial, donde todas las Fuerzas Militares Colombianas y posiblemente el sector defensa (Ministerio de Defensa) expongan sus necesidades y proyecciones al respecto de una posible migración a la nube, con el fin de unificar esfuerzos y poder así dar viabilidad a un proyecto de una nube comunitaria donde converjan las instituciones, robustecida en infraestructuras de seguridad y con un talento humano altamente calificado para administrar estos servicios.

Debido al continuo desarrollo de la tecnología, el presente documento puede ser tomado como referencia para una migración a la nube para una entidad militar, pero siempre se debe realizar una vigilancia tecnológica puesto que en el transcurso de meses o pocos años, las diferentes tecnologías, procedimientos y modelos mencionados en el presente documento, pueden haber evolucionado, haber sido reemplazados o simplemente desaparecido.

Es recomendable que las entidades militares dejen de ver la nube como un concepto abstracto, peligroso y poco confiable y la empiecen a ver como lo que realmente es, un robusto sistema conformado por hardware, software, servicios y una serie de características que la hacen de gran usabilidad, y realicen comparaciones con sus centros de datos actuales, evidenciando que en última instancia todo se reduce a hardware y software; el nivel de inseguridad puede darse de igual forma en una nube o en un centro de datos en sitio, siempre que no se adopten las suficientes medidas de ciberseguridad para protegerlo.

Trabajos Futuros

Utilizar el presente instrumento para apoyar el proceso de migración hacia la nube en una entidad militar, teniendo en cuenta las recomendaciones de implementación de una nube privada o comunitaria.

Para la fase de migración enunciada en el instrumento de ciberseguridad, es posible desarrollar un marco más detallado a nivel de infraestructura, técnicas, procesos y procedimientos para temas como la réplica de servicios, migración de datos, pruebas funcionales y puesta en producción, que sirva de guía a los administradores de TI en ese nivel, ya que, debido al enfoque de la presente monografía, no se hizo mucho énfasis en este aspecto.

Referencias Bibliográficas

Abad A., & Cazar, F. (2014). *Estudio y diseño de qos para una red de internet, datos y voip*. (Trabajo de grado profesional). Universidad de Israel. http://repositorio.uisrael.edu.ec/handle/47000/899

Aguedo, R., & Astrada, E. O. (2019). *El impacto financiero de Cloud Computing en una empresa global de telecomunicaciones*. (Tesis profesional). Universidad San Ignacio de Loyola. http://repositorio.usil.edu.pe/bitstream/USIL/8984/1/2019_Aguedo-Blanco.pdf

Al-Bayati, B., Clarke, N., & Dowland, P. (2016). Adaptive behavioral profiling for identity verification in cloud computing: A model and preliminary analysis. *GSTF Journal on Computing (JoC)*, *5*(1), 21-28. DOI10.5176/2251-3043_4.4.348

Alimam, M., Bertin, E., & Crespi, N. (2017). ITIL perspective on enterprise social media. *International Journal of Information Management*, *37*(4), 317-326. DOI: 10.1016/j.ijinfomgt.2017.03.005

Alonso, Á. (2015). *Introducción al Protocolo OAuth 2.0 Securizando Servicios Web Ejemplos prácticos de uso*. http://www.dit.upm.es/~posgrado/web2015-2016 archivada/SI/2014-2015/2015-06-03-AlvaroAlonso-Transparencias.pdf

Amaya Pérez, E. J. (2016). *Gestionar centralizadamente las identidades en organizaciones*. (Trabajo de Grado Especialización). Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2726/Trabajo%20de%20grado3289.pdf?sequence=1&isAllowed=y

Amidon Lusted, M. (2016). *Bit Rot: Preserving the Documents Most Important to You*. The Rosen Publishing Group, Inc.

Barja, R. (s.f.). *Los 5 nueves: Mito o realidad.* http://www.coimbraweb.com/documentos/varios/los5nueves.pdf

Bartock, M., Scarfone, K., & Feldman, L. (2016). *Implementing trusted geolocation services in the cloud.* National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/itl-bulletin/2016/02/implementting-trusted-geolocation-services-in-the-cloud/final

Brown, N. , & Jayapriya, K. (2014). An extensive survey on QoS in cloud computing. *International Journal of Computer Science and Information Technologies*, *5*(1), 1-5. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.643.2811&rep=rep1&type=pdf

Brunette, G., & Mogull, R. (2009). *Security guidance for critical areas of focus in cloud computing v2. 1.* Cloud Security Alliance. https://wikileaks.org/sony/docs/05/docs/Cloud/csaguide.pdf

Camacho, J., & Camacho, R. (2020). *Modelo de auditoría para una red corporativa de datos para prevenir ciberdelitoS. Caso de Estudio: Banco Fondo Común*. www.dit.upm.es › ~posgrado › 2014-2015 › 2015-06-...

Carrizo, D., & Alfaro, A. (2018). Método de aseguramiento de la calidad en una metodología de desarrollo de software: un enfoque práctico. *Ingeniare. Revista chilena de ingeniería*, *26*(1), 114-129. http://dx.doi.org/10.4067/S0718-33052018000100114.

Casero, A., Loose, M. S. y Piemonti, M. G. (2019). *La traducción en la era digital.* Ponencia presentada en el III Congreso Internacional de la AAHD: Humanidades Digitales. La Cultura de los Datos, organizado por la Asociación Argentina de Humanidades Digitales y Facultad de Humanidades y Artes de la Universidad Nacional de Rosario, del 7 al 9 de noviembre de 2018, Rosario, Santa Fe, Argentina. https://rephip.unr.edu.ar/bitstream/handle/2133/16656/2019%20CASERO%2C%20LOOSE

%2C%20PIEMONTI.%20La%20traducci%C3%B3n%20en%20la%20era%20digital.pdf?sequence=3&isAllowed=y

Cassasola, M., Maqueo, M., Molina, M., Moreno, J. & Recio, M. (2014). *La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo*. Centro de Investigación y Docencia Económicas/cloudMIDDLEtrust, SL. https://cidecyd.files.wordpress.com/2014/05/la-nube-nuevos-paradigmas-de-privacidad-y-seguridad-para-un-entorno-innovador-y-competitivo.pdf

Cavalcanti, J., & Sobejano, J. (2011). *Social Media IOR: Las Relaciones como moneda de rentabilidad*. Bubok Publishing SL, 2011.

Cedeño, R. L. (2016). *Consolidación de servidores mediante la virtualización*. (Tesis Maestría). Universidad Israel. http://repositorio.uisrael.edu.ec/handle/47000/1239

Centro criptológico Nacional. (2020). *Ataques DDoS. Recomendaciones y buenas prácticas*. https://www.ccn-cert.cni.es/informes/abstracts/4925-ataques-ddos-recomendaciones-y-buenas-practicas/file.html.

Chávez Sánchez, D. I. (2017). *Perfil del nivel de gestión de las tecnologías de la información y comunicación (tic): definir el plan estratégico, definir la arquitectura de información, determinar la dirección tecnológica, definir la organización y relaciones de ti en la institución educativa Javier Heraud Perez de la provincia de Recuay, departamento de Ancash en el año 2015*. (Tesis profesional). Universidad Católica los Ángeles de Chimbote. http://repositorio.uladech.edu.pe/bitstream/handle/123456789/872/ARQUITECTURA%20DE%20INFORMACION_%20DIRECCION%20TECNOLOGICA_CHAVEZ%20_SANCHEZ_DAVID%20_INOCENCIO.pdf?sequence=1&isAllowed=y

Congreso de Colombia. (1993, 28 octubre). Ley 80 de 1993 por la cual se expide el Estatuto General de Contratación de la Administración Pública. Diario Oficial n°. 41094. http://www.secretariasenado.gov.co/senado/basedoc/ley_0080_1993.html

Congreso de Colombia. (2008ª, 16 de julio). *Ley 1221 de 2008, por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones*. Diario Oficial n° 47.052 http://www.secretariasenado.gov.co/senado/basedoc/ley_1221_2008.html

Congreso de Colombia . (2008b, 31 de diciembre). *Ley 1266 de 2008 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.* Diario Oficial. n° 47.219 http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley 1266 de 31 de diciembre 2008.pdf

Congreso de Colombia. (2009a, 5 de enero) *Ley 1273 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. Diario Oficial n° 47.223. http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

Congreso de la República. (2009b, 30 de julio). *Ley 1341 de 2009 por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones*. Diario Oficial n°. 47.426. http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

Congreso de Colombia. . (2013, 17 abril). *Ley Estatutaria N° 1621 de 2013, por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se di*. Diario Oficial. n° 48.764. http://secretariasenado.gov.co/senado/basedoc/ley_1621_2013.html

Congreso de Colombia. (2014,6 de marzo). Ley 1712 de 2014 por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Diario Oficia. n°. 49.084, http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

Corrales, C. Cilleruelo, C. & Cuevas, A. (2014). Otros.(2014). *Criptografía y Métodos de Cifrado.* http://www3. uah. es/libretics/concurso2014/files2014/Trabajos/Criptografia% 20y% 20Metodos% 20de% 20Cifrado. pdf.

Cortés García, P. (2017). *Computación en la nube. Contratos: un estudio comparativo*. (Trabajo de Grado en Documentación e Información.). Universidad de Salamanca. https://gredos.usal.es/bitstream/handle/10366/138130/TFG_InfyDoc_CortesGarcia_Pedro_SI_80_2016-2017.pdf?sequence=1&isAllowed=y

Coyla -Jarita, Y. (2019). *Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión–Filial Juliaca*. (Trabajo de Grado Profesional). Universidad Peruana Unión. https://repositorio.upeu.edu.pe/bitstream/handle/UPEU/2002/Yony_Coyla_Tesis_Licenciatura_2019.pdf?sequence=1&isAllowed=y

Creswell, J. W. (2013). *Steps in conducting a scholarly mixed methods study. DBER Speaker Series. 48.* https://digitalcommons.unl.edu/dberspeakers/4

Cruz-Chávez, M., Peralta, J., Martínez, M. & Cruz- Rosales, M. (2014). *Libro: La computadora, herramienta indispensable en diversas áreas de conocimiento.* Grid Morelo.

De Aguilera, M., & Casero-Ripollés, A. (2018). ¿ Tecnologías para la transformación? Los medios sociales ante el cambio político y social. *Revista ICONO14 Revista científica de Comunicación y Tecnologías emergentes*, *16*(1), 1-21.

DeCuir-Gunby, J. T., & Schutz, P. (2017). Developing a mixed methods proposal: A practical guide for beginning researchers. (1st Edición. SAGE Publications, Inc;

Departamento Nacional de Planeación. (2016). *CONPES 3854 Política Nacional de Seguridad Digital*. DNP. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf.

Departamento Nacional de Planeación. (2020). CONPES 3995 *Política nacional de confianza y seguridad digital*. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Donald, A. C., Oli, S. A., & Arockiam, L. (2013). Mobile cloud security issues and challenges: A perspective. *International Journal of Engineering and Innovative Technology*, *3*(1), 40-406.

Ercolani, G. (2012). Análisis del potencial del Cloud Computing para la PYMES. *Cuadernos de Gestión de Información*, *2*, 40-55.https://revistas.um.es/gesinfo/article/view/207621

Fuerza Aérea Colombiana. (2011). *Plan Estratégico Institucional 2011-2030.* https://d2r89ls1uje5rg.cloudfront.net/sites/default/files/plan_estrategico_institucional_fac.pdf

Fuerza Aérea Colombiana. (2020). *Misión y Visión Fuerza Aérea Colombiana* |FAC https://www.fac.mil.co/transparencia-y-acceso-informacion-publica/3-estructura-organica-y-talento-humano/mision-vision

Gondree, M., & Peterson, Z. N. J. (2013, Febrero). Geolocation of data in the cloud. *Proceedings of the third ACM conference on Data and application security and privacy* (pp. 25-36.). https://doi.org/10.1145/2435349.2435353

Grande, M., Cañón, R., & Cantón, I. (2016). Tecnologías de la información y la comunicación: evolución del concepto y características. *IJERI: International Journal of Educational Research and Innovation*, *6*, 218-230.

Guamán, D., Pérez, J., & Correa, R. (2020). Herramienta para la personalización y cálculo de métricas de código utilizando análisis estático: SCAT. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *E28*, 693-710.

Guerra, A. (2018). *Guía de procesos para la migración tecnológica a Cloud Computing para la empresa AV Renewable Energy SA*. (Trabajo Final de Maestría). Pontificia Universidad Católica del Ecuador

Guo, Z., & Ma, D. (2018). A model of competition between perpetual software and software as a service. *MIS Quarterly*, *42*(1), 101-120; DOI: 10.25300/MISQ/2018/13640

Gutiérrez, C. A., Almeida, R., & Romero, W. (2018). Diseño de un modelo de migración a cloud computing para entidades públicas de salud. *Investigación e Innovación en Ingenierías*, *6*(1), 10-26. DOI: 10.17081/invinno.6.1.2772

Gutiérrez, C. A. R., & Almeida, R. A. D. (2019). Ventajas de la migración a los servicios de la nube en el sector público de salud del Valle del Cauca. *Revista vínculos*, *16*(1) Revista.unidistrital.edu.co› vinculos › article › view

Hausman, K. K., Cook, S. L., & Sampaio, T. (2013). *Cloud Essentials: CompTIA Authorized Courseware for Exam CLO-001*. John Wiley & Sons.

Hernández, R. (2014). LA Investigación Cualitativa a través de entrevistas: su análisis mediante la teoría fundamentada. *Cuestiones Pedagógicas,* 23, 187-210. http://institucional.us.es/revistas/cuestiones/23/Mis_5.pdf

Hernández, A. A. E., Ramos, M. P. R., Placencia, B. M. L., Indacochea, B. G., Quimis, A. J. G., & Moreno, L. A. P. (2018). *Metodología de la investigación científica* (Vol. 15).. Área de Innovación y Desarrollo SLL.

Hogan, M. Liu, F., Sokol, A. & Tong. J. (2011). *NIST*-SP 500-291, NIST cloud computing standards roadmap. National Institute of Standards and Technology, *Special Publication 500-291*, 1-76. https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Jul5A.pdf

Horton, R. (2016). *Content Management Framework (CMF)*. https://silo.tips/download/content-management-framework-cmf

Hoyos Ospina, A., & Toro Veléz, M. (2013). *Modelo para la migración de una PYME hacia la computación en la nube*. (Trabajo de Grado Profesional). Universidad EIA. https://repository.eia.edu.co/bitstream/11190/2283/3/HoyosAndrea_2013_ModeloMigracionPyme.pdf

Hummer, M., Kunz, M., Netter, M., Fuchs, L., & Pernul, G. (2016). Adaptive identity and access management—contextual data based policies. *EURASIP Journal on Information Security, 2016,* 1 (19), 1-16. DOI: 10.1186/s13635-016-0043-2

Ibagué, S., Camacho, E., & Espindola, J. (2011). *Desarrollo y Aplicacion de Cloud Computing en Colombia. USNL.*

Infoblox. (2014). *Protecting DNS Infrastructure-Inside and Out.* https://dsimg.ubm-us.net/envelope/155383/295022/1393254893_infoblox-whitepaper-protecting-DNS-

infrastructure-inside-out-US-letter.pdf

Instituto Nacional de Tecnología de la Comunicación.(2011). *Riesgos y amenazas en Cloud Computing*. INTECO). https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

Jansen, M. (2012). Will Cloud Computing Change Standards in IT-Service Management? *Journal of Communication and Computer*, *9*(7), 813-823. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.468.8572&rep=rep1&type=pdf

Jansen, W. A., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *NIST Special Publication 800-144*, 1-80. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Joshi, C., & Singh, U. K. (2016). Performance evaluation of web application security scanners for more effective defense. *International Journal of Scientific and Research Publications (IJSRP)*, *6*(6), 660-667. http://www.ijsrp.org/research-paper-0616.php?rp=P545535

Joyanes Aguilar, L. (2018). Computación en la nube: Notas para una estrategia española en cloud computing. *Revista Del Instituto Español De Estudios Estratégicos*, (00)., 89-112 Recuperado a partir de https://revista.ieee.es/article/view/406

Junco, G., & Rabelo, S. (2018). Los recursos de red y su monitoreo. *Revista Cubana de Informática Médica*, *10*(1), 76-83. http://scielo.sld.cu/pdf/rcim/v10n1/rcim09118.pdf

Kaur, S., & Gupta, R. (2019). Enhancing Features of Cloud Computing Using Cloud Access Security Brokers to Avoid Data Breaches. *European Journal of Engineering Research and Science*, *4*(10), 185-189. https://doi.org/10.24018/ejers.2019.4.10.1518

Latorre, M. (2018). *Historia de las web, 1.0, 2.0, 3.0 y 4.*0. Universidad Marcelino Champagnat. http://umch.edu.pe/arch/hnomarino/74_Historia%20de%20la%20Web.pdf

Lehrig, S., Eikerling, H., & Becker, S. (2015 mayo). *Scalability, elasticity, and efficiency in cloud computing: A systematic literature review of definitions and metrics*. Proceedings of the 11th International ACM SIGSOFT Conference on Quality of Software Architectures (pp., 83-92). https://doi.org/10.1145/2737182.2737185

Lehto, J., Rajamäki, J., & Rathod, P. (2012). Conceptualised view on can cloud computing improve the rescue services in Finland?. *Recent Researches in Applied Computers and Computational Scienc,* S/N, 65-70. https://www.researchgate.net/publication/231117047_Conceptualised_view_on_can_cloud_computing_improve_the_rescue_services_in_Finland

López A. (2013). *Guía de seguridad de servicios DNS.* INTECO. https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/guia_de_seguridad_en_servicios_dns.pdf

Márquez, L., Rosado, D., Mellado, D., & Fernández-Medina, E. (2014). Hacia un Proceso de Migracion de la Seguridad de Sistemas heredados al Cloud. *RECSI 2014,* 191-196. https://core.ac.uk/download/pdf/32320407.pdf

Medina, L. N. (2017). *Criptografía y mecanismos de seguridad.* Fundación Universitaria del Área Andina. https://core.ac.uk/download/pdf/326423363.pdf

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *Special Publication 800-145,* 1-7. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Mesa Sectorial Cloud. (2010). *Cloud Computing, una perspectiva para Colombia*. Versión 1.0.0. http://www. interactic. com. co/dmdocuments/clud_computing. pdf.

Ministerio de Tecnologías de la Información y las Telecomunicaciones. MinTic. (2016a). *Documento – Versión actualizada del modelo de gestión IT4+*. https://www.mintic.gov.co/arquitecturati/630/propertyvalues-8170_documento_pdf.pdf.

Ministerio de Tecnologías de la Información y las Telecomunicaciones . MinTic. (2016b). Seguridad y privacidad de la información – Seguridad en la nube.. *Guía* 12, 1-31. https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

Ministerio de Tecnologías de la Información y las Telecomunicaciones MinTic. (2018). *Guía de computación en la nube – Guía Técnica*. Versión. 1.0. https://www.mintic.gov.co/portal/604/articles-75238_documento.pdf

Mohammad, A. F., & Mcheick, H. (2011). Cloud services testing: An understanding. *Procedia Computer Science*, *5*, 513-520. doi:10.1016/j.procs.2011.07.066

Montañés, E. (2019). *MFA and Identity Federations*. (Trabajo Final de Maestría. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/98946/6/edgarmontanesTFM0619memoria.pdf

Montoya, J. A., & Restrepo, Z. (2012). Gestión de identidades y control de acceso desde una perspectiva organizacional. *Ingenierías USBMed*, *3*(1), 23-34. https://doi.org/10.21500/20275846.261

Mullo Pilamunga, X. E. (2019). *Firewall para la seguridad de la red en lo laboratorios de la Universidad Estatal de Bolívar*. (Artículo Científico de Maestría). Universidad Regional Autónoma De Los Andes "UNIANDES". http://dspace.uniandes.edu.ec/bitstream/123456789/10715/1/ACTFMFG020-2019.pdf

Nazareno, G. (2018). *Virtualización de servidores. Conceptos básicos*. UE - Gobierno de España.http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/2283/Virtualizacio

n%20de%20servidores.pdf?sequence=1&isAllowed=y

Nikolov, L., & Slavyanov, V. (2018). Network infrastructure for cybersecurity analysis. *International scientific conference*."Vasil Levski]" National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria.

Ñique -Morazzani, V. A. (2016). *Implementación de solución de autenticación segura basada en doble factor en una entidad del Estado*. (Tesis profesional). Universidad San Ignacio de Loyola. http://200.37.102.150/bitstream/USIL/2481/1/2016_%C3%91ique_Implementacion_de_solucion_de_autenticacion.pdf

Páez Murcia, O. (2012). *La computación en la nube, como solución a los problemas de disponibilidad y continuidad en los servicios informáticos de la aeronáutica civil*. (Tesis de Maestrpia). Universidad Nacional de Colombia. http://www.bdigital.unal.edu.co/10439/1/940745.2012.pdf

Papazafeiropoulou, A., & Spanaki, K. (2016). Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*(6), 1251-1263.. https://doi.org/10.1007/s10796-015-9572-3

Paredes, S., Hinojosa, C., & Ruiz, J. (2016). La importancia de la Gestión de la Configuración del Software, en una Empresa de Desarrollo. *GEEKS DECC-REPORTS*, *3*(1), 31-41. file:///C:/Users/Administrador/Downloads/257-714-1-PB.pdf

Peña-López, I., & Guillén, M. (2012). *Computación en la Nube*. : Universitat Oberta de Catalunya https://pdfs.semanticscholar.org/37ae/b4917fb26bb63455e45a3497c5c7c529d67c.pdf

Prado, V. (2018). *MSData: Herramienta para la creación de subconjuntos y enmascaramiento de datos para entornos no productivos.* https://ruidera.uclm.es/xmlui/handle/10578/19035

Punithasurya, K., & Priya, S. J. (2012). Analysis of different access control mechanism in cloud. *International Journal of Applied Information Systems*, *4*(2), 34-39. https://pdfs.semanticscholar.org/bde6/915c52dbf371efc10b0d99ff1c4cbc034e06.pdf

Ramírez, H., De la Hoz, J., & Gómez, L. (s.f.). *Cloud Computing como canal de comunicación entre plataformas: Caso de estudio de HSLAB*. https://www.udi.edu.co/congreso/historial/congreso_2012/ponencias/sistemas/2-CC_Canal_Computacion.pdf

Rane, P. B., & Meshram, B. B. (2012). Transaction security for e-commerce application. *International Journal of Electronics and Computer Science Engineering*, *1*(3), 1720-1726. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.259.7340&rep=rep1&type=pdf

Rashmi, M. S., & Sahoo, G. (2012). A five-phased approach for the cloud migration. *International journal of emerging technology and advanced engineering*, *2*(4), 286-291. https://www.yumpu.com/en/document/read/16185136/a-five-phased-approach-for-the-cloud-migration-ijetae

Reddy, J. M., & Monika, J. M. (2012). Integrate military with distributed cloud computing and secure virtualization. *2012 SC Companion: High Performance Computing, Networking Storage and Analysis*, (pp. 1200-1206). DOI: 10.15224/978-1-63248-117-7-39

RedHat. (2020). *¿Qué son los proveedores de nube?* https://www.redhat.com/es/topics/cloud-computing/what-are-cloud-providers

Romero, Y . (2019). *Pentesting,¿ Porque es importante para las empresas?*. Univesidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1

Rosales, E., Castro, H., & Villamizar, M. (2011). *Unacloud: Opportunistic cloud computing infrastructure as a service.* The Second International Conference on Cloud Computing, GRIDs, and Virtualization (pp. 187-194). https://www.academia.edu/1945826/UnaCloud_Opportunistic_Cloud_Computing_Infrastructure_as_a_Service

Salvat, G., & Serrano, V. (2011). *La revolución digital y la sociedad de la información*. Comunicación Social Ediciones y Publicaciones

Sánchez, G. (2010). Los Estados y la ciberguerra. *Boletín de Información del CESEDEN*, *317*, 63-75

Sefraoui, O., Aissaoui, M., & Eleuldj, M. (2014, April). Cloud computing migration and ITresources rationalization. In *Multimedia Computing and Systems (ICMCS), 2014International Conference on (pp.* 1164-1168). IEEE. DOI:10.1109/ICMCS.2014.6911300

Sharma, M., Bansal, H., & Sharma, A. K. (2012). Cloud computing: Different approach & security challenge. *International Journal of Soft Computing and Engineering (IJSCE)*, *2*(1), 421-424. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.648.5989&rep=rep1&type=pdf

Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Identity and access management as security-as-a-service from clouds. *Procedia Computer Science*, *79*, 170-174. . Elsevier B.V. https://doi.org/10.1016/j.procs.2016.03.117

Sherry, J., Lan, C., Popa, R. A., & Ratnasamy, S. (2015, agosto). B*lindbox: Deep packet inspection over encrypted traffic.* Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication,(pp. 213-226.). https://doi.org/10.1145/2785956.2787502

Singletary, V., & Baker, E. L. (2019). Building Informatics-Savvy Health Departments: The Systems Development Life Cycle. *Journal of Public Health Management and Practice*, *25*(6), 610-611. DOI: 10.1097/PHH.0000000000001086

Sinjilawi, Y. K., Al-Nabhan, M. Q., & Abu-Shanab, E. A. (2014). Addressing Security and Privacy Issues in Cloud Computing. *Journal of Emerging Technologies in Web Intelligence*, *6*(2), 199-199. https://pdfs.semanticscholar.org/77a3/2c5e65048533580d36f5704640bb6c0a8eb5.pdf

Sobhan, R. (2019). The Concept of Cloud Accounting and its Adoption in Bangladesh. *International Journal of Trend in Scientific Research and Development (IJTSRD), 3* (4), 1261-1267. DOI:10.31142/ijtsrd24031

Souppaya, M., & Scarfone, K. (2013). Guide to enterprise patch management technologies. *NIST Special Publication*, *800*, 40. https://www.nist.gov/publications/guide-enterprise-patch-management-technologies

Tekerek, A., & Bay, O. F. (2019). Design and implementation of an artificial intelligence-based web application firewall model. *Neural Network World*, *29*(4), 189-206. http://www.nnw.cz/doi/2019/NNW.2019.29.013.pdf

Thales. (2017). *2017 Thales Data Threat Report: Security Spending Decisions Leave Sensitive Data Vulnerable Despite rise in breaches, companies still prioritizing network and endpoint solutions over encryption*. https://www.prnewswire.com/news-releases/2017-thales-data-threat-report-security-spending-decisions-leave-sensitive-data-vulnerable-300397098.html

Torres Martínez, M. Á. (2015). *DLP: prevención de fuga de información (Data Loss Prevention)*. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2883/00002325.pdf?seque

nce=1

Ureña, A., (coord). (2012). *Estudio del Clouding computing. Retos y oportunidades*. Ministerio de Industria, Energía y Turismo de España. Observatorio Nacional de Telecomunicaciones y de la SI. https://www.ontsi.red.es/sites/ontsi/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf

Varela C., Portella, J., & Pallares, L.(2017). Computación en la nube: Un nuevo paradigma en las tecnologías de la información y la comunicación. *Redes De Ingeniería*, 138-146. https://revistas.udistrital.edu.co/index.php/REDES/article/download/12485/13087

Verizon Media Platform. (2020). *Web Application Firewall Administration Guide Trademark Information About This Guide Web Application Firewall Administration Guide*. https://docs.vdms.com/pdfs/VDMS_WAF_Admin_Guide.pdf

Apéndices

Apéndice A

Entrevista a expertos en ciberseguridad y Tecnologías de la Información

Realizada por: Khristian Jaffet Morales Vargas

Universo: Expertos en ciberseguridad y TI de diferentes empresas y entidades de los diferentes sectores productivos del país.

Fecha: Lapso entre mayo y junio de 2020

Área de cobertura: Nivel Nacional

Tipo de muestreo: Expertos en ciberseguridad y tecnologías de la información.

Método: Entrevista personal mediante la herramienta Google Docs.

Metodología: Mixta (Cualitativa – Cuantitativa)

Tamaño de la muestra: Quince (15) expertos en ciberseguridad y tecnologías de la información.

Objetivo de la entrevista: Obtener información acerca del panorama de migración a la nube en diferentes entidades y sectores del país, recopilando a su vez los principales inconvenientes afrontados y canalizando recomendaciones referentes a la mejor forma para la migración a la nube de una entidad militar.

Cantidad de preguntas: 14

Ficha Técnica Entrevista a Personal Experto en Ciberseguridad y TI

Preguntas de la entrevista	Observaciones
1. ¿La entidad en la que se desempeña se encuentra en el sector?	-Público -Privado -Mixto -Otro (¿Cuál?)
2. ¿La entidad en la que se desempeña es de tipo:	-Organización Militar -Academia -Sector Defensa -Sector Financiero -Otro (¿Cuál?)
3. Actualmente se desempeña como:	-Directivo -Técnico -Asesor Externo -Otro (¿Cuál?)
4. ¿Ha participado en la adopción de la tecnología de clouding computing para un sistema Institucional o empresarial? Si la respuesta es SI explicar brevemente en cual.	
5. ¿En cuántos procesos de migración hacia la tecnología clouding computing ha participado?	-1 -2 -3 -4 o más.
6. Si la respuesta al numeral 4 fue afirmativa; ¿sabe si el proceso de migración hacia la nube se hizo basado en algún modelo que contemplara la ciberseguridad? Si la respuesta es SI explicar cuál.	
7. ¿Considera usted que hay mayor ciberseguridad en los sistemas informáticos de una Organización al usar la arquitectura en sitio o haciendo uso de algún tipo de nube (pública, privada, híbrida o comunitaria)? Justifique su respuesta.	

Preguntas de la entrevista	Observaciones
8. ¿Cuál sería el modelo de servicio de clouding computing, que recomendaría para ser adoptado por una Organización o por una Institución Militar y por qué?	-IaaS -PaaS -SaaS -Ninguna de las anteriores
9. ¿Cuál sería el modelo de despliegue de clouding computing que recomendaría para ser adoptado por una Institución Militar y por qué?	-Nube pública -Nube Privada -Nube híbrida -Nube comunitaria
10. ¿Cuál fue el principal problema afrontado en la migración hacia la nube en el(los) proceso(s) que participó y por qué?	
11. ¿En el(los) proceso(s) de migración hacia la nube en los que participó, que porcentaje de las aplicaciones de la entidad fueron migradas hacia la nube?	-0 - 24% -25% - 49% -50% - 74% -75% - 100%
12. Si la respuesta al numeral 11 no fue el 100% ¿Qué tipo de aplicaciones no fueron migradas y por qué?	-Aplicaciones Administrativas -Aplicaciones del nicho de negocio -Aplicaciones de ofimática, correo y herramientas colaborativas -Otras (¿Cuáles?) Justifique su respuesta.
13. ¿Considera importante desarrollar una herramienta de ciberseguridad (Documental) que ayude a la migración a la nube de forma segura para una Institución Militar? Justifique su respuesta.	
14. ¿Qué considera que se debería incluir esa herramienta de ciberseguridad para migración a la nube?	