Modelo de ciberseguridad en una infraestructura como servicio laaS basados en defensa en profundidad de las historias clínicas electrónicas para las entidades promotoras de salud en Colombia

Fabian Leonardo Herrera Rico

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2020

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA

MODELO DE CIBERSEGURIDAD EN UNA INFRAESTRUCTUA COMO SERVICIO (laaS) BASADOS EN DEFENSA EN PROFUNDIDAD DE LAS HISTORIAS CLÍNICAS ELECTRONICAS PARA LAS ENTIDADES PROMOTORAS DE SALUD EN COLOMBIA

ALUMNO:

FABIAN LEONARDO HERRERA RICO

DIRECTOR:

MSc GABRIEL ALBERTO PUERTA APONTE

GRUPO DE INVESTIGACIÓN
MASA CRÍTICA

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO

BOGOTÁ – COLOMBIA

2020

TMCIBER 2020
058
E.J.1
775806

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

MODELO DE CIBERSEGURIDAD EN UNA INFRAESTRUCTUA COMO SERVICIO (laaS) BASADOS EN DEFENSA EN PROFUNDIDAD DE LAS HISTORIAS CLÍNICAS ELECTRÓNICAS PARA LAS ENTIDADES PROMOTORAS DE SALUD EN COLOMBIA

ALUMNO: FABIAN LEONARDO HERRERA RICO

DIRECTOR: MSc GABRIEL ALBERTO PUERTA APONTE

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

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

BOGOTÁ – COLOMBIA

2020

DEDICATORIA.

Esta tesis se la dedico en memoria a mi Padre que desde el cielo me guio y me dio fuerzas, me enseñó con sabiduría alcanzar los sueños y propósitos en la vida, gracias por inculcarme grandes valores como el compromiso, la perseverancia y la humildad; me hubiera gustado que me acompañaras en este nuevo logro, pero donde se encuentre estará orgulloso de mi.

A mi madre que estuvo pendiente de mí y con sus oraciones para que alcanzara mi propósito.

A mi hermosa niña Maria Paula que es mi motor, mi motivación e inspiración para seguir adelante, superarme cada día más y así poder luchar para que la vida nos depare un futuro mejor.

A mi esposa por apoyarme y creer en mí, aunque hemos pasados momentos difíciles, siempre ha estado brindándome su conocimiento, amor y cariño.

AGRADECIMIENTOS.

Le doy gracias a Dios por haberme acompañado y guiado de no desfallecer en mi Maestría, por ser mi fortaleza para seguir adelante que me ha enseñado de otra manera otras lecciones de vida.

Gracias a mi pequeña María Paula que es mi orgullo y mi gran motivación, que me impulsa superarme, para tener mejores oportunidades y poderle ofrecer siempre lo mejor, no fue fácil no poderle dedicar tiempo en algunas ocasiones, y quiero ser un ejemplo para mi hija.

Gracias a mi asesor de tesis Gabriel Alberto Puerta por permitirme creer en mi idea de trabajo de grado para sacarlo adelante, por su voto de confianza y apoyarme a lo largo del desarrollo de la tesis y en sus revisiones, incondicionalmente.

Gracias a mis compañeros del curso de la Maestría por tener momentos de compartir ideas a través de una taza de café, que pudimos generar grandes debates enriquecedoras sobre temas de actualizad o Ciberseguridad en diferentes espacios, además me brindaron su confianza, apoyo y decisiones haciendo participes de alguna forma en éste proyecto.

Abstract - The medical history is a set of documents that contain the basic data, medical assessment, information and monitoring of the patient's health status throughout the care process. Nowadays, every provider of health services and / or EPS that treats a patient for the first time, must carry out the process of opening a medical history. That is, when we change EPS or attend to a different medical service, the health provider must open a new medical record, which is located in a printed file or through a decentralized information system in the health provider. This document proposes through a bibliographic review a cybersecurity architecture model in an Infrastructure as a Service (LaaS) based on in-depth defense of electronic medical records (HCE) for the health sector in Colombia, applying security controls in different layers in each ring, facilitating the understanding of the security risks to which cloud computing will be exposed, whose purpose is to prepare adequate defenses at the different barriers, minimizing the risks of the cloud to acceptable levels. From this study, the proposed model will allow a comprehensive evaluation of the Infrastructure as a Cloud Service in health sector organizations of electronic medical records, which constitutes it as a tool to facilitate decision-making from the context of the strategic planning.

Key words: Security of the information, cybersecurity, security models, Defense in Depth, Cloud security, Clinical history.

Resumen – La historia clínica es un conjunto de documentos que contienen los datos básicos, valoración médica, información y seguimiento del estado de salud del paciente a lo largo del proceso asistencial. Hoy en día todo prestador de servicios de salud y/o EPS que atiende a un paciente por primera vez, debe realizar el proceso de apertura de historia clínica. Es decir, cuando cambiamos de EPS o nos atienden algún servicio médico diferente, la prestadora de salud debe realizar la apertura de una nueva historia clínica, la cual se ubica en un archivo impreso o a través de un sistema de información descentralizado en la prestadora de salud. En este documento se propone a través de una revisión bibliográfica un modelo de ciberseguridad en una Infraestructura como Servicio (LaaS) basados en defensa en profundidad de las historias clínicas electrónicas (HCE) para las entidades promotoras de salud en Colombia, aplicando controles de seguridad en diferentes capas en cada anillo, facilitando la comprensión de los riesgos de seguridad a las que estará expuestos la computación en la nube, cuya finalidad es preparar las defensas adecuadas en las diferentes barreras, minimizando los riesgos de la nube a unos niveles aceptables. A partir de este estudio, el modelo propuesto permitirá una evaluación integral de la Infraestructura como Servicio en la Nube en las organizaciones del sector salud de las historias clínicas electrónicas, que lo constituye en una herramienta para facilitar las tomas de decisiones desde el contexto de la planificación estratégica.

Palabras claves: Seguridad de la Información, ciberseguridad, modelos de seguridad, defensa en profundidad, seguridad en la nube, historia clínica.

TABLA DE CONTENIDO

DEDICATORIA.....3
AGRADECIMIENTOS.....4
INDICE DE TABLAS.....10
LISTADO DE ABREVIATURAS.....11
1. INTRODUCCION.....13
2. DELIMITACION DEL TEMA DE INVESTIGACIÓN.....17
3. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN.....18
3.1. PREGUNTA DE INVESTIGACIÓN.....20
3.2. HIPÓTESIS.....20
4. OBJETIVOS.....21
4.1. OBJETIVO GENERAL.....21
4.2. OBJETIVOS ESPECIFICOS.....21
5. MARCO CONCEPTUAL.....22
5.1. COMPUTACION EN LA NUBE.....22
5.1.1 Tipos de Servicio en la nube.....23
5.2. SEGURIDAD DE LA INFORMACION EN LA NUBE.....26
5.2.1 Principios de la Seguridad de la Información.....28
5.3. CIBERSEGURIDAD.....29
5.4. DATOS SENSIBLES.....31
5.4.1 Historia Clínicas Electrónicas (HCE).....32
5.5. CIBERRIESGOS ASOCIADOS A LA COMPUTACION EN LA NUBE DE UNA INFRAESTRUCTURA COMO SERVICIO.....34
5.6. AMENAZAS EN LA COMPUTACION EN LA NUBE.....36
5.7. VULNERABILIDADES EN LA COMPUTACION EN LA NUBE.....40
5.8. MATRIZ DE VALORACION DE LOS CIBERRIESGOS.....43
5.8.1 Evaluación del Riesgo.....43
6. MARCO REFERENCIAL.....46
6.1. MODELOS DE SEGURIDAD.....46
6.2. MODELOS DE SEGURIDAD EN LA COMPUTACION EN LA NUBE.....47
6.2.1 Amazon Web Services (AWS).....48

6.2.2 Microsoft Azure. 49
6.2.2.1 Seguridad de la laaS en Azure. 50
6.2.2.2 Arquitectura de N-niveles 50
6.2.2.3 Marco de Arquitectura de Seguridad en Azure 50
6.3. DEFENSA EN PROFUNDIDAD 52
6.3.1 Defensa en Profundidad para entornos de computación en la nube. 55
6.4. MODELOS DE PRIVACIDAD DE HISTORIAS CLINICAS 56
6.4.1 Modelo de Sistema de Información Médica (MIS). 56
6.4.2 Desafíos de seguridad y preservación de la privacidad de la información en la computación en la nube. 57
6.4.3 Arquitectura de atención médica orientada a servicios basada en la computación en la nube... 58
6.4.4 Arquitectura del Sistema Registro Personal de Salud (PHR) en la nube. 60
7. METODOLOGÍA 62
7.1. TIPO DE INVESTIGACION 62
7.2. DISEÑO DE LA INVESTIGACION 62
7.3. FASES DE LA INVESTIGACION 63
8. MODELO DE CIBERSEGURIDAD PARA EL SECTOR SALUD 64
8.1. GESTION DE POLÍTICAS 66
8.1.1 Cumplimiento Legal. 66
8.1.1.1 Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA). 66
8.1.1.2 Ley 1581 de 2012. 68
8.1.1.3 Ley 1273 de 2009. 69
8.1.1.4 Ley 527 de 1999. 69
8.1.1.5 Ley 2015 de 2020. 70
8.1.2 Cumplimiento administrativo 70
8.1.2.1 Norma ISO 27001. 70
8.1.2.2 Norma ISO 27017. 71
8.1.2.3 Norma ISO 27018. 71
8.1.2.4 Norma ISO 27032. 71
8.1.2.5 Norma ISO 27036. 72
8.2 GESTION DE ACCESO E IDENTIDAD 73

8.2.1 Esquemas de firma digital. 74
8.2.2 Cifrado de autenticación. 75
8.3 GESTION DE INFRAESTRUCTURA 75
8.3.1 Virtualización. 76
8.4 GESTION DE APLICACIONES 77
8.4.1 Desarrollo y Diseño Seguro. 78
8.4.2 Despliegue Seguro. 79
8.4.3 DevOps. 80
8.5 GESTION DE DATOS 82
8.5.1 Cifrado de los datos en reposo. 83
9 CONCLUSIONES 84
BIBLIOGRAFIA 87

INDICE DE GRÁFICAS

Gráfica 1. Adopción de Servicios en la nube en organizaciones de salud, tomado de E-Health Reporter Latin América septiembre 2017. 15
Gráfica 2. Modelo de Referencia. 23
Gráfica 3. Administración de la computación en la nube, tomado de Microsoft Azure – 2019. 25
Gráfica 4. Seguridad de la información, tomado de la Norma ISO/IEC 17799 – 2005. 27
Gráfica 5. Norma ISO 27032:2012 Gestión de la Ciberseguridad. 31
Gráfica 6. Modelo de Seguridad de la Información en TIC. 47
Gráfica 7. Servicios disponibles en Azure tomado de Microsoft Azure – 2019. 49
Gráfica 8. Patrón de Identidad Federada. 51
Gráfica 9. Sistema avanzado de defensa contra amenazas persistentes. 53
Gráfica 10. Modelo de Defensa basado en Control de lazo cerrado. 54
Gráfica 11. Modelo MIS. 57
Gráfica 12. Arquitectura de Salud. 59
Gráfica 13. Sistema PHR entorno en computación en la nube. 61
Gráfica 14. Modelo de Arquitectura en Ciberseguridad basados en Defensa en profundidad. 64
Gráfica 15. Arquitectura de ciberseguridad basados en Defensa en Profundidad para HCE. 65
Gráfica 16. Modelo de Gestión de acceso e Identidad adaptado a partir de Cloud Security Alliance (2018). 73
Gráfica 17. Aislamiento entre recursos virtuales. 77
Gráfica 18. Fases de desarrollo y diseño seguro. 79
Gráfica 19. Pruebas de Seguridad. 79
Gráfica 20. Proceso DeVops según Microsoft – 2019. 80
Gráfica 21. Cifrado de volúmenes gestionado externamente, tomado de Cloud Security Alliance (2018). 83

INDICE DE TABLAS

Tabla 1: Guía de gestión de riesgos. 44
Tabla 2: Análisis de Ciber riesgos. 45
Tabla 3: Fases de la Investigación. 63
Tabla 4. Oportunidades de seguridad en la gestión de aplicaciones, CSA (2018). 78

LISTADO DE ABREVIATURAS

AAA: Autorización, autenticación y auditoría

ABE: Cibrado basado en atributos

API: Interfaz de programación de aplicaciones

APT: Amenazas Persistentes Avanzadas

ART.: Artículo

AWS: Amazon Web Services

CASB: Cloud Access Security Broker

CPU: Unidad Central de Procesamiento

CSA: Cloud Security Alliance

DDoS: Denegación de Servicio Distribuido

EEUU: Estados Unidos.

EPS: Entidad Promotora de Salud.

ESPAC: Control de accesso centro en **el paciente eficiente y seguro**

HCE: Historias Clínicas Electrónicas.

HIPAA: La ley de responsabilidad y Portabilidad del Seguro Médico

HL7: Health Level Seven

IDS: sistrmas de detección de Intrusos

IEEE: Instituto de Ingeniería Eléctrica y Electrónica

ISACA: Asociación de Auditoría y Control de Sistemas de Información

ISO: Organización Internacional de Normalización.

ITIL: Biblioteca de Infraestructura de Tecnologías de Información

LaaS: Infraestructura como Servicio.

MAC: Códigos de autenticación de mensaje

MIS: Sistema de Información Médica

NIST: Instituto Nacional de Estándares y tecnología

NSG: Azure Network Security Groups

OWASP: Proyecto de Seguridad de aplicaciones web abiertas

PaaS: Plataforma como Servicio

PHR: Registro Personal de Salud

PKE: Cifrado de clave pública.

SaaS: Software como Servicio

SKE: Cifrado de Clave simétrica

SO: Sistema Operativo

SSE: Cifrado simétrico de búsqueda

SSO: Inicio de Sesión unificado

TI: Tecnologías de la Información

TLS: Seguridad en la Capa de Transporte

VM: Máquinas virtuales.

VMM: Monitor de máquina virtual

XACML: Lenguaje de control de mercado extensible débil

XSS: Cross-Site Scripting

1. INTRODUCCIÓN

En Colombia, se define historia clínica como: "un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que intervienen en su atención" (Resolución número 1995, 1999, art. 1).

De igual forma esta resolución establece las características básicas que toda historia clínica debe tener: integridad (registro de todos los procedimientos realizados por un paciente), secuencialidad (registro cronológico), disponibilidad (fácil de acceso a la información) y confidencialidad (privacidad de la información). Es decir, que cualquier persona que integre un equipo de salud no puede tener acceso a la historia clínica, la información debe ser confidencial para todas las personas respecto del estado de salud, tratamientos y condiciones de salud del paciente garantizando el derecho de la intimidad.

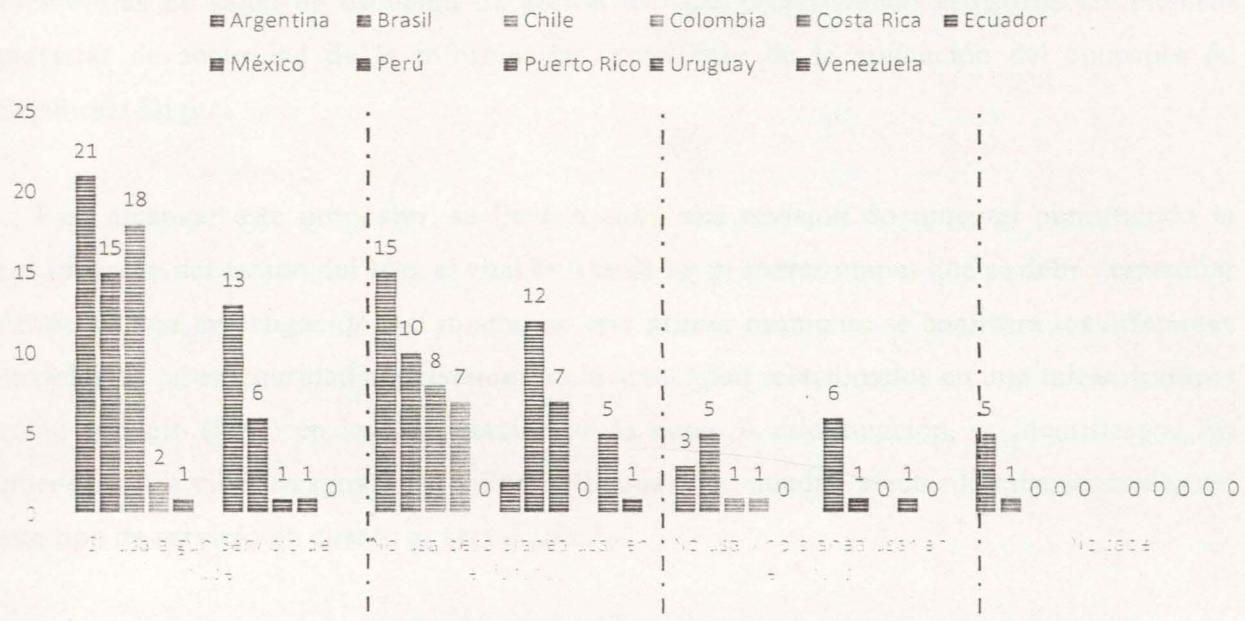
Según el reporte "Healthcare Data Breaches" en septiembre del 2017 hubo 39 incidentes de seguridad relacionados a los datos de pacientes médicos que involucraron más de quinientos (500) registros, a través de ataques de phishing y ransomware comprometiendo servidores on-premise, equipos y la exposición de la información de salud de los pacientes (HIPAA Journal, 2017).

Por lo tanto, muchas organizaciones tienen el pensamiento paradigmático de no destinar fondos para el componente de ciberseguridad, pues según la mayoría, éstos elevan los costos de esta, sin dimensionar que no contar con el presupuesto requerido para ello puede generar sobrecostos representados en la afectación de la imagen, la realización de reprocesos, riesgos en el manejo de los datos y de los recursos financieros, entre otros (Bonilla y González, 2012).

Hoy en día con la transformación digital y la modernización de la industria, la computación en la nube elimina las barreras para que las empresas puedan desarrollar los proyectos de TI, reduciendo las grandes inversiones en infraestructuras, tiempos de aprovisionamiento requerida, gastos operativos asociados a conectividad, softwares, licencias, personal especializado, entre otros; obteniendo un mayor retorno de la inversión. Gartner dice: *"En el 2020 una empresa sin servicios en la nube será tan extraña como una sin Internet hoy"*, es decir las entidades promotoras de salud tendrán una mezcla de sistemas **on- premises,** hospedados y en la nube, pero cada vez más enfocados a los servicios de computación en la nube en función de una mayor eficiencia.

Según el estudio realizado por "E-Health Reporter Latin América" de septiembre 2017 patrocinado por *everis* de once (11) países de América Latina, el 46% manifestaron que las organizaciones de salud usan actualmente servicios en la nube. Y otro 40% no lo están usando, pero se proyecta hacerlo en un futuro. Colombia muestra el mayor potencial de crecimiento en la nube en el corto y mediano plazo. Dentro de los tres (3) modelos de servicio de la computación en la nube, software como servicio (SaaS) domina las preferencias de las organizaciones en la región con un 47,6%, le sigue infraestructura como servicio (laaS) en un 26.2% y por último plataforma como servicio (PaaS) en un 13,1%.

De acuerdo con lo anterior, las Entidades Promotoras de salud se proyecta a evolucionar digitalmente en una infraestructura como servicio (laaS), la cual es un escenario desafiante permitiendo mejorar la eficiencia para acceder, analizar y compartir datos de las historias clínicas electrónicas (HCE) en las decisiones del sector salud y reduciendo los errores médicos. Así mismo, la Infraestructura como Servicio (laaS) facilita tecnologías emergentes tales como: big data analytics, computación cognitiva, telemedicina y las aplicaciones móviles para acelerar las soluciones avanzadas.



Gráfica 1. Adopción de Servicios en la nube en organizaciones de salud, tomado de E-Health Reporter Latin América septiembre 2017

No obstante, en América Latina según el estudio la adopción de la Infraestructura como servicio (laaS) en las Entidades Promotoras de Salud, continúan en una dinámica más lenta con relación a los demás continentes. Los límites que se han identificado desde preocupaciones técnicas tales como: la interoperabilidad entre las soluciones y los sistemas heredados; hasta incertidumbre con la confidencialidad, integridad, disponibilidad y no repudio de la información de las HCE.

A pesar de ello, las capacidades del entorno de la computación en la nube crean desafíos relacionados con la seguridad de las aplicaciones de datos y sus sistemas, el cual depende de los siguientes factores: gestión de identidad y acceso, prevención de perdida de datos y gestión de control de ataques de Malware. Al adoptar un entorno de Infraestructura como Servicio (laaS), el proveedor debe implementar sistemas de seguridad en su infraestructura para mitigar las amenazas, a su vez Mintic ha generado lineamientos de políticas de ciberseguridad orientadas a desarrollar estrategias que contrarresten el incremento de las amenazas informáticas que afectan a las organizaciones, de ahí que, estructurar un modelo de Ciberseguridad basados en defensa en profundidad, permitirá definir a las entidades

Promotoras de salud un esquema de acción técnico, promoviendo el uso de las mejores prácticas de seguridad de la información como base de la aplicación del concepto de Seguridad Digital.

Para alcanzar este propósito, se llevó a cabo una revisión documental permitiendo la construcción del estado del arte, el cual es una de las primeras etapas que se debe desarrollar dentro de una investigación, así mismo en este primer momento se analizará los diferentes modelos de ciberseguridad coexistentes en la actualidad relacionados en una infraestructura como servicio (laaS) en la computación en la nube. A continuación, se identificaron las amenazas, los ciber riesgos y las vulnerabilidades que puedan afectar la ciberseguridad en este tipo de servicio en cuanto al sector salud.

Por último. en el capítulo ocho (8) se definieron los elementos que conforman el modelo de Ciberseguridad en una Infraestructura como Servicio basados en Defensa en Profundidad para las Entidades Promotoras de salud en las historias clínicas (HCE), de este modo se estructura y desarrolla la temática o problemática que se va a llevar a cabo a través del modelo planteado.

2. DELIMITACION DEL TEMA DE INVESTIGACIÓN

La temática central de este proyecto, estuvo direccionada a plantear un modelo de ciberseguridad, enfocado a una infraestructura como servicio (laaS), desde las proposiciones conceptuales basadas en un sistema técnico de defensa en profundidad, mejorando la capacidad de detección y prevención de los datos clínicos, para la protección de la información, con el fin de resolver los problemas de seguridad en las historias clínicas de las entidades promotoras de salud, como lo establece la Ley de transferencia y Responsabilidad de Seguro Médico (HIPAA); la cual regula el uso en la regla de seguridad técnica, controlando el acceso a los sistemas informáticos y protegiendo la información de salud (Ley HIPAA, 1996). Desde la misma perspectiva, la ley 2015 del 2020 que determina las garantías de la privacidad y reserva de las historias clínicas de acuerdo con el artículo 7, el cual subraya que sólo la persona titular de las historias clínicas electrónicas podrá autorizar el uso a terceros para acceder a la información total o parcial, de acuerdo con la normatividad vigente, preservando la confidencialidad, integridad, disponibilidad, no repudio, autorización, identidad y autenticidad.

Ahora bien, retomando las concepciones orientadas a los sistemas técnicos de defensa en profundidad, estos fueron soportados desde una perspectiva que alude a la protección de múltiples capas desde la gestión de políticas en los siguientes niveles: gestión de identidad y acceso, gestión de infraestructura, gestión de aplicaciones y gestión de datos, que a su vez, se soportan en un enfoque por capas de seguridad a los centros de datos físicos y de los servicios de la computación en la nube protegiendo y evitando que personas no autorizadas puedan sustraer información sensible y confidencial. Este enfoque elimina la dependencia de cualquier nivel de protección único y actúa para ralentizar un ataque contra los recursos que se encuentran en la computación en la nube.

3. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

Hoy en día todo prestador de servicios de salud y/o Empresa Promotora de Salud (EPS) en Colombia que atiende a un paciente por primera vez, debe realizar el proceso de apertura de historia clínica. Es decir, cuando cambiamos de EPS o nos atienden algún servicio médico diferente, la prestadora de salud nos deben abrir de nuevo una historia clínica, la cual debe estar ubicada en un archivo impreso o a través de un sistema de información descentralizado de acuerdo con los tiempos de retención de los datos.

Desafortunadamente, la calidad de las historias clínicas no es la adecuada en el país. Gutiérrez, Ruiz, Suarez y Prieto (2018) manifiestan que, en la actualidad Colombia cuenta con sistemas de información ineficientes en las EPS. que no permiten la obtención de datos actualizados de manera eficaz y eficiente: problema que se deriva de la escasa interoperabilidad e integración de las EPS. EL no contar con una interoperabilidad lleva como consecuencia que las historias clínicas se encuentren disponibles en un solo lugar a la vez, disminuyendo de esta forma su accesibilidad y aumentando su fragmentación y duplicidad. Esto puede ser evidenciado en el tratamiento de las historias clínicas por parte del prestador de servicios de salud, este tratamiento trae consigo barreras que dificultan el proceso de atención de pacientes y a su vez presentando riesgos de pérdida de información valiosa para el ciudadano, transferencia no autorizada de datos y activos, que pueden consolidarse en sucesos de corrupción como es ejemplo el llamado cartel de la hemofilia en Bolívar, engranzaje de corrupción que se soportaba en el reporte de falsos enfermos al sistema de salud.

Debido a las razones anteriormente expuestas, el Gobierno Colombiano se vio en la necesidad de implementar un sistema de historias clínicas electrónicamente única, para cada paciente, para que de esta forma se pueda garantizar el acceso y ejercicio de los derechos a la salud y a la información de las personas, respetando el Habeas Data y la reserva de esta. Por medio de este sistema se pretende el intercambio de los elementos de datos clínicos

relevantes por las EPS, Bajo los siguientes pilares de la Seguridad; la accesibilidad, integridad, disponibilidad y confidencialidad (Ley No. 2015, 2020).

Dadas estas premisas, el proyecto de ley en cuanto a las historias clínicas electrónicas tienen grandes retos en la seguridad de la información, debido a que la gran cantidad de datos que es de carácter sensible y privado, razón por la cual, se deben generar de forma apremiante estrategias de ciberseguridad, promoviendo el uso de las mejores prácticas de seguridad de la información como base de la aplicación del concepto de Seguridad Digital. En igual grado de importancia, se resalta que el no adecuado manejo de la información relacionada con los pacientes podría tener afectaciones en sus condiciones de salud, y a su vez, en los procesos de información verídica del paciente.

De acuerdo con lo anterior. con este sistema de historias clínicas electrónicas se lleva a cabo el registro y posterior actualización de toda la información médica del paciente, el cual es clasificada como confidencial ya que su revelación puede violar el derecho a la intimidad, de ahí que, fundamentar este sistema conlleva grandes retos de ciberseguridad tales como: pérdida de la información, violación a los datos sensibles, corrupción, manejo inadecuado de la información o los malos usos y finalidades que pueden hacer sobre la misma, múltiples trámites y demoras en la atención médicas, problemas administrativos, entre otros; pero debido a la susceptibilidad y sensibilidad de la información se requieren de nuevos modelos de ciberseguridad que se puedan adaptar a las necesidades y particularidades de los datos confidenciales que faciliten medidas preventivas de los sistemas tecnológicos, permitiendo resguardar y proteger la información, buscando mantener la confidencialidad, disponibilidad e integridad de la misma.

Como soporte a lo anteriormente descrito, Dunlap y Beth (2017) refiere lo siguiente:

"*El informe señala que, a nivel organizacional, la seguridad cibernética a menudo se ve como un problema aislado de TI, y no como algo que requiere atención de alto nivel. Hasta que una organización de atención médica experimente una violación de datos, los profesionales de seguridad de la información pueden tener problemas para convencer a las*

organizaciones de que los ciberataques plantean riesgos para la atención del paciente o que las medidas proactivas pueden proteger a la organización contra daños a la reputación a largo plazo".

3.1. PREGUNTA DE INVESTIGACIÓN

A partir del punto 3 surge la siguiente pregunta de investigación: *¿De qué manera estructurar un modelo técnico de ciberseguridad en una Infraestructura como Servicio (IaaS), basados en Defensa en Profundidad, fortaleciendo la protección de las historias clínicas electrónicas custodiadas por las Entidades Promotoras de salud y que solamente permita el ingreso de los usuarios autorizados por el sistema?*

3.2. HIPÓTESIS

El diseño de un modelo de Arquitectura de ciberseguridad en una Infraestructura como servicio (IaaS) basados en defensa en profundidad de las historias clínicas electrónicas para las Entidades promotoras de Salud (EPS), contribuirá con el cumplimiento de la protección de datos sensibles de los pacientes a través de controles de seguridad, estableciendo mecanismos adecuados para proteger los datos de salud del paciente y minimizando los riesgos que se puede presentar en la violación de los datos.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Estructurar un modelo de Ciberseguridad en una Infraestructura como Servicio (laaS) basados en Defensa en Profundidad de las historias clínicas electrónicas para las Entidades Promotoras de Salud.

4.2. OBJETIVOS ESPECIFICOS

1. Revisar a nivel documental los modelos de ciberseguridad existentes.

2. Definir los elementos que conforman la Arquitectura de ciberseguridad en una Infraestructura como Servicio Basados en Defensa en Profundidad para el sector Salud.

3. Analizar los diferentes modelos de ciberseguridad de la Información coexistentes en la actualidad.

4. Identificar las amenazas, riesgos y vulnerabilidades que pueden afectar la ciberseguridad en una Infraestructura como Servicio para las Entidades Promotoras de Salud.

5. MARCO CONCEPTUAL

5.1. COMPUTACIÓN EN LA NUBE

La computación en la nube es un sistema de plataformas e infraestructuras tecnológicas que se conecta a través de la Internet a un centro de datos remoto utilizados para gestionar servicios de información y aplicaciones.

El Instituto Nacional de Estándares y Tecnología (NIST) define la computación en la nube como:

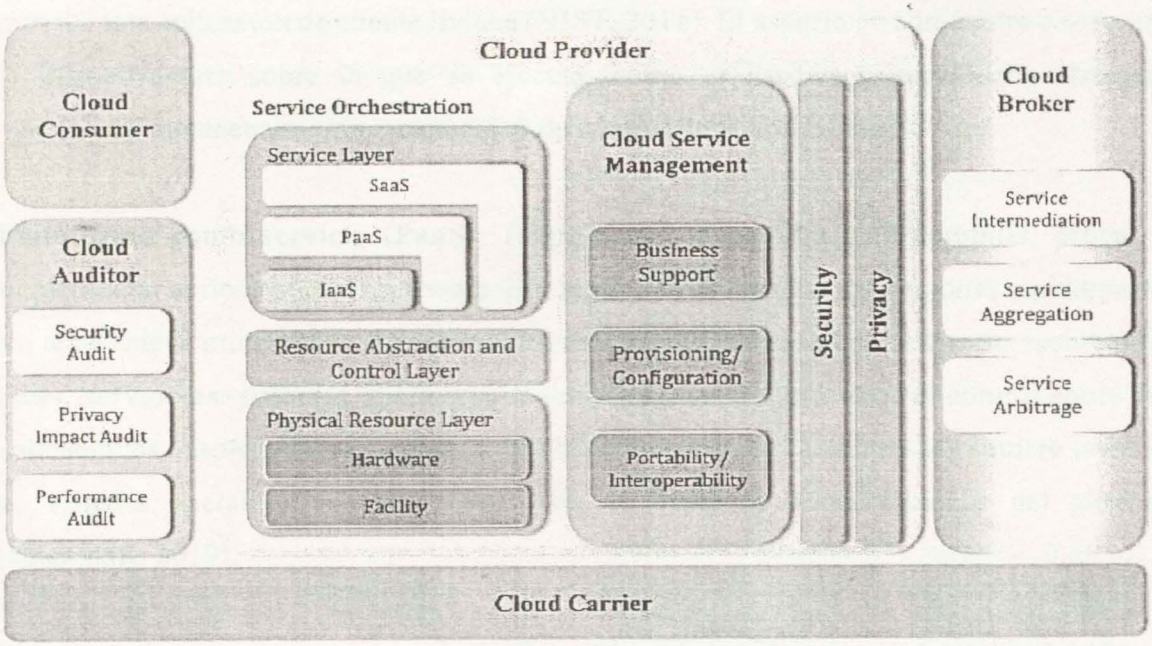
"Modelo para permitir un acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo o interacción del proveedor de servicio".

La definición de ISO/IEC 17788:2014 es muy similar: *"paradigma para permitir el acceso de red a un conjunto de recursos compartidos escalables y elásticos, físicos o virtuales con aprovisionamiento de autoservicio y administración bajo demanda".*

Por último, Microsoft define la computación de la nube así: *"consiste en alquilar recurso como espacio de almacenamiento o ciclos de CPU en los equipos de otra empresa. Solo paga por lo que usa".*

Así de esta manera, la computación en la nube es una tecnología disruptiva que tiene las ventajas de mejorar la colaboración, reducir costos, ser escalable, ser elástica, ser global y estar disponible en todo momento. Este modelo contempla todos los componentes que se pueden orquestar rápidamente, aprovisionar, implementar y desmantelar, con el fin de proporcionar un esquema de asignación y consumo similar de servicio a pedido.

La NIST presenta una visión general de la arquitectura de referencia de computación en la nube, que identifica los principales actores, sus actividades, y funciones. En la gráfica 2 representa una arquitectura genérica de alto nivel para facilitar la compresión de los requisitos, usos, características y estándares de la computación en la nube.



Gráfica 2. Modelo de Referencia.
Fuente: (Liu, Tong, Mao, Bohn, Messina, Badger y Leaf, 2011, p.3).

5.1.1 Tipos de Servicio en la nube.

Cuando hablamos de la computación en la nube, existen tres (3) categorías principales que son:

- ✓ **Infraestructura como Servicio (IaaS):** es uno de los servicios más flexibles de la nube. El objetivo es brindar un control completo sobre el hardware (servidores, máquinas virtuales (VM), almacenamiento, redes y Sistemas operativos). Consta de una instalación, hardware, una capa de abstracción, una capa de orquestación para unir los recursos y APIS para administrar de forma remota los recursos y entregarlos a los usuarios (CSA, 2018). En vez de comprar hardware se alquila (Microsoft, 2019). En este tipo de servicio es importante que el proveedor proteja otras características en la computación en la nube, tales como: la seguridad de las instancias, los métodos de autenticación de los usuarios, la

seguridad de las APIS, el almacenamiento por bloques y además de los objetos que son asignados a los usuarios.

- ✓ **Software como Servicio (SaaS):** es una aplicación administrada y alojada por el proveedor de la nube. Los usuarios acceden a ella con un navegador web, una aplicación móvil o una aplicación de cliente liviana (NIST, 2011). El usuario no administra o controla la infraestructura sobre la que se ejecuta, como el hardware, servidores, sistemas operativos, almacenamiento o capacidad de control de la aplicación.

- ✓ **Plataforma como servicio (PaaS):** Proporciona un entorno para compilar, probar e implementar aplicaciones de software. El objetivo es desarrollar aplicaciones rápidamente sin tener que administrar la infraestructura subyacente, sobre la que se ejecuta incluyendo redes, servidores, sistemas operativos o almacenamiento, pero tiene el control sobre las aplicaciones desplegadas. Es decir, al implementar una aplicación no se requiere instalar un sistema operativo o un servidor web, ni tampoco actualizaciones del sistema (Microsoft, 2019).

Con el rápido crecimiento del mercado de la computación en la nube, Microsoft resumen las ventajas de la computación en la nube, en especial para las Entidades Promotoras de salud:

a) Optimiza la inversión de recursos y disminuye costos: las organizaciones se benefician de compartir una infraestructura compleja y pagan solamente por los recursos que utilizan.

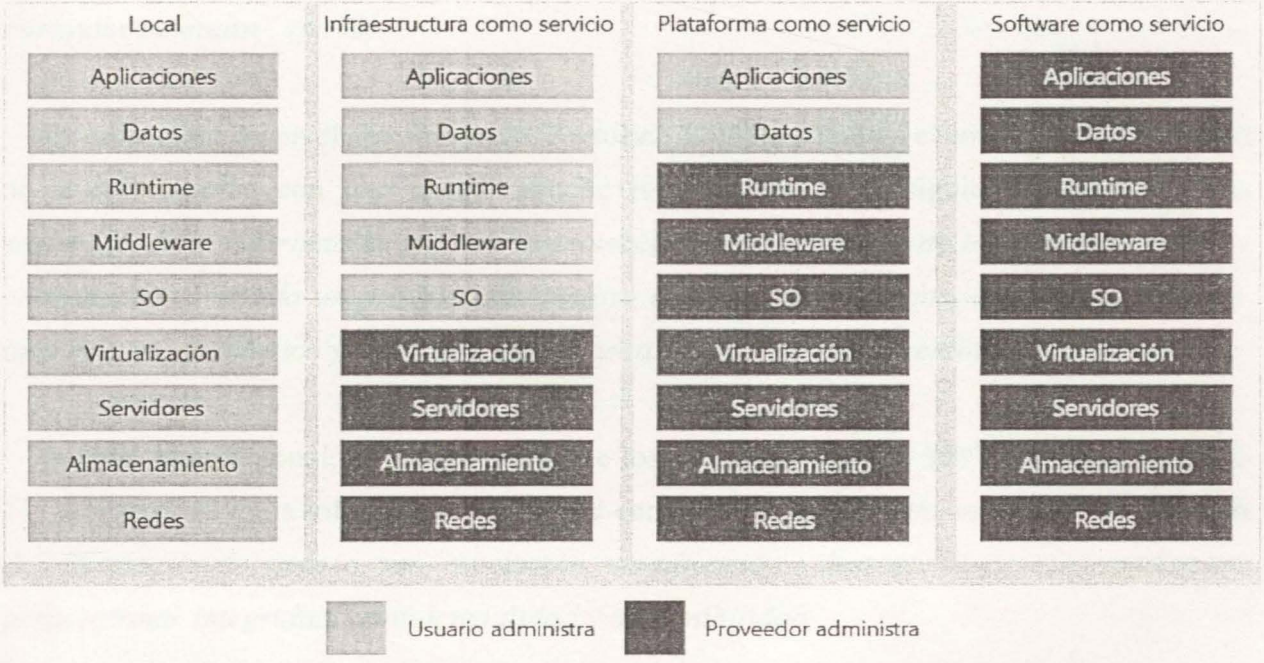
b) Permite la movilidad: puede ser utilizado a distancia, ya que los usuarios tendrán acceso a los sistemas desde cualquier lugar donde se encuentre.

c) Presenta beneficios ambientales.

d) Facilita la escalabilidad, la innovación y el desarrollo de productos; se adaptan rápidamente a negocios de crecimiento, debido a que la computación en la nube se diseñó para enfrentar aumentos grandes de carga de trabajo, incrementando la agilidad, disminuyendo los riesgos y costos.

e) Mejora la seguridad de los datos: Proporciona una administración unificada de la seguridad de infraestructura reforzando el nivel de seguridad, además de protección avanzada de amenazas en todas las cargas de trabajo. Protege de los ciberataques mediante la amplia inteligencia de amenazas con controles integrados (Microsoft, 2019).

En la gráfica 3 se muestra los aspectos para tener en cuenta, los recursos que administra el proveedor de la nube y los que el usuario administra en cada categoría de servicio en la computación en la nube:



Gráfica 3. Administración de la computación en la nube, tomado de Microsoft Azure – 2019.

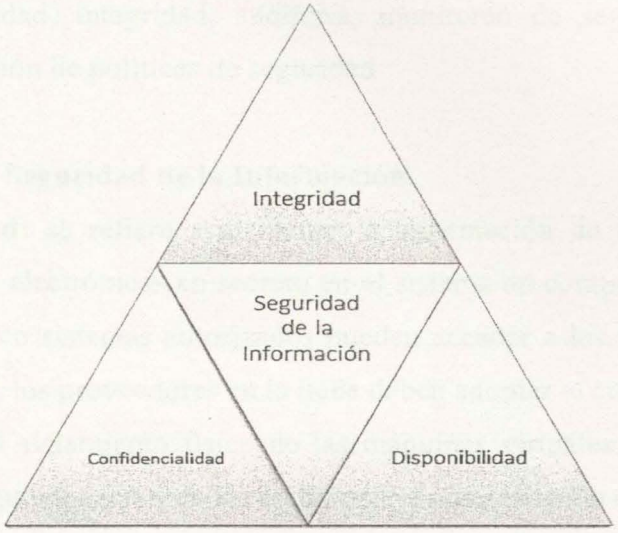
5.2. SEGURIDAD DE LA INFORMACIÓN EN LA NUBE

La seguridad de la información es el término más utilizado, ya que es un activo que brinda valor al negocio, así mismo, las Entidades Promotoras de Salud (EPS) requiere fortalecer la seguridad y privacidad de la información a través de un modelo basados en defensa en profundidad, cuyo fin es el aseguramiento de la integridad, disponibilidad y confidencialidad de la información mediante el acceso, uso y apropiación, obteniendo un adecuado manejo de la información para protegerla frente a las amenazas y vulnerabilidades que se encuentran expuestas en un ambiente de computación en la nube.

De acuerdo con lo anterior, la ISO 27001 (2016) define la seguridad de la Información: *"La preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización"*. Desde otra óptica, Ramio (2006) afirma que: *"La Seguridad hace referencia a un conjunto de métodos y herramientas utilizados para proteger la información y los sistemas informáticos ante cualquier amenaza" (p. 50).*

En consonancia con el anterior autor, Bertolin (2008) profundiza el concepto de Seguridad de la Información con una mirada mucho más amplia en la siguiente dirección: *"La seguridad de la Información implica la protección de los sistemas de información, redes, y computadores, siendo un proceso que incluye aspectos tecnológicos, de gestión, humano, informático, económico y legal abarcando así aspectos físicos, del entorno y humano".*

A nivel internacional, el código de ley de los EE. UU. (sección 3542, capítulo 35, título 44) la seguridad de la información se define como: "*proteger la información y los sistemas de información del acceso, uso, revelación, modificación o destrucción no autorizada para proporcionar integridad, confidencialidad y disponibilidad".*



Gráfica 4: Seguridad de la información, tomado de la Norma ISO/IEC 17799 - 2005

El modelo de seguridad de la computación en la nube se debe establecer con los tres pilares fundamentales que son: confidencialidad, integridad y disponibilidad. La confidencialidad es la política de privacidad de la computación en la nube para que los datos en tránsito o en reposo garanticen la confidencialidad de los datos al evitar la divulgación no autorizada. La integridad se describe como mantener un sistema de software en un estado legítimo predefinido, se trata de la validación del origen de los datos, detecta la alteración de los datos y determina si el origen de los datos ha cambiado. La disponibilidad se refiere a negar el acceso ilegítimo a recursos de la Computación en la nube y prevenir riesgos externos, amenazas y ataques (Manjusha y Ramachandran, 2015). Desde un punto de vista más amplio, en la norma ISO/IEC 17799:2005 se define la **Seguridad de la Información** como la preservación de su confidencialidad, su integridad y su disponibilidad.

Dependiendo del tipo de información manejada y de los procesos realizados por una organización, ésta podrá conceder más importancia a garantizar la confidencialidad, la integridad o la disponibilidad de sus activos de información, protegiéndolos en la computación en la nube. Así mismo, los sistemas basados en la nube deben abordar los requisitos de seguridad tales como: autenticación, autorización, disponibilidad,

confidencialidad, identidad, integridad, auditoría, monitoreo de seguridad, respuesta a incidentes y administración de políticas de seguridad

5.2.1 Principios de la Seguridad de la Información.

a. **Confidencialidad:** se refiere a mantener la información de los pacientes de las historias clínicas electrónicas en secreto en el sistema de computación en la nube y solo los usuarios o sistemas autorizados pueden acceder a los datos. Para lograr la confidencialidad, los proveedores en la nube deben adoptar el cifrado en reposo de la información y el aislamiento físico de las máquinas virtuales. Este principio está asociado con la autenticación de los usuarios. La autenticación electrónica establece confianza de la identidad del paciente. En el entorno de la computación en la nube, el usuario requiere confiar en las aplicaciones ofrecidas por las Entidades Promotoras de salud que maneja y mantiene los datos de los pacientes de manera segura (Mushtaq, Akram, Khan, Shahzad & Ullah, 2017).

b. **Integridad:** significa protegerse contra modificación o destrucción incorrecta de la información, e incluye garantizar el no repudio y la autenticidad de la información. La integridad de los datos involucra tres actores principales que son: el proveedor de los servicios en la nube; el propietario de la información y el auditor que asegura la integridad de los datos (NIST, 2018).

c. **Disponibilidad:** asegura que los servicios o recursos deberían estar disponibles a los usuarios en cualquier momento de su requerimiento sin demoras. Dado que una solución de seguridad eficaz protege los componentes del sistema, garantizando la disponibilidad del recurso directamente relacionada con la seguridad de la información (Gupta, 2018).

d. **No repudio:** proporciona una prueba de participación en una acción al establecer que la clave privada de un usuario se usó para firmar digitalmente una transacción

comercial electrónica. Esto comprueba que el usuario especifico realizo una tarea particular (Gupta, 2018).

e. **Autorización:** Describe las acciones que pueden realizar en un sistema una vez cuando se haya identificado y autenticado. Estas acciones pueden incluir lectura, escritura o ejecución de archivos o programas. La autorización se asocia con los privilegios o permisos para el uso del sistema que a su vez son definidos por un administrador del sistema (Vargas, 2018).

f. **Identidad:** La seguridad de la identidad mantiene la integridad, la confidencialidad de los datos y las aplicaciones al tiempo lo que hace que el acceso se encuentre disponible para los usuarios apropiados. El soporte para las capacidades de la administración de la identidad tanto para los usuarios como para los componentes de infraestructura es un requisito importante para la computación en la nube y la identidad tiene que administrarse de manera que se construya la confianza (Velez & Zlateva, 2011).

g. **Autenticidad:** Es el atributo generado en un mensaje de datos, cuando existe certeza sobre la persona que lo ha elaborado, emitido, firmado o cuando existe la certeza respecto de la persona a quien se atribuya el mensaje de datos (Decreto No. 1413, 2017, p. 4).

5.3. CIBERSEGURIDAD

La ciberseguridad consiste en la protección de la información digital en los sistemas interconectados. La ciberseguridad se encuentra dentro de la seguridad de la información. Según Information Systems Audit and Control Association, la ciberseguridad es definida como "*protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados*", (ISACA,2018).

Le & Hoang (2016) sugieren la siguiente definición:

"la Ciberseguridad puede ser considerada como sistemas, herramientas, procesos, prácticas, conceptos y estrategias para prevenir y proteger el ciberespacio de la interacción no autorizada a través de agentes con elementos del espacio para proteger y defender la confidencialidad, integridad, disponibilidad y otras propiedades del espacio y sus recursos protegidos" (p.3).

La organización Internacional de Normalización (ISO) ha creado el estándar ISO/IEC 27032:2012 para la gestión de la ciberseguridad, que brinda un marco seguro para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos. Ésta norma describe el ciberespacio como un entorno virtual, el cual no existe en una forma física, un mundo resultante de la aparición de la Internet y la interacción de personas, software y las organizaciones, el cual son respaldadas por todo tipo de dispositivos tecnológicos y de comunicación distribuidos a nivel mundial, por lo cual se ha convertido en un entorno muy complejo.

La norma ofrece fortalecer el estado de la ciberseguridad usando los puntos técnicos y estratégicos relevantes y sus relaciones con otros dominios de la seguridad, tales como:

a. La Seguridad en las Redes.
b. Seguridad en Internet.
c. Seguridad de la Información.
d. Seguridad de las Aplicaciones.
e. Protección de la información de la infraestructura critica

Gráfica 5: Norma ISO 27032:2012 Gestión de la Ciberseguridad

La relación entre ciberseguridad y otros dominios de la seguridad es bastante compleja como se visualiza en la gráfica No. 5, por ejemplo, algunos servicios de la infraestructura crítica como el sector salud, no afecta la ciberseguridad directamente. Sin embargo, la falta de ciberseguridad podría tener un impacto negativo en la disponibilidad de los sistemas de información de la infraestructura crítica. Por otro lado, la disponibilidad y el funcionamiento del ciberespacio depende de los servicios de Infraestructura crítica, tal como la Infraestructura de la red de telecomunicaciones.

5.4. DATOS SENSIBLES

Hoy en día la privacidad sufre un impacto proveniente de diferentes ámbitos a lo que se refiere a los datos sensibles. El derecho de la privacidad ha sido amparado por la ley protegiendo a la persona individual y preservando la inviolabilidad del domicilio y demás información relevante. Es decir, que estos no podrán ser utilizados por otros sin el consentimiento de la persona. Así, es necesario establecer cuáles de estos datos pueden ser

proporcionados a un tercero o cuales un individuo posee esos datos personales pudiendo oponerse a su uso.

De acuerdo con la Ley 1581 de 2012, título III, articulo 5 se entiende por datos sensibles: *"Aquellos que afectan con la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos".*

La protección de los datos personales debe cumplir las personas naturales y jurídicas que dispongan de bases de datos. es un mandato legal establecido en la Ley. para el cumplimiento de los requisitos de recolección. administración. tratamiento y transmisión de datos. De este modo, las políticas públicas sobre la protección van enlazados con el creciente desarrollo tecnológico, exigiendo mayores garantías en el tratamiento de los datos.

Con los avances tecnológicos se han transformado los registros de información de pacientes en las Entidades Promotoras de salud (EPS) en formato digital, almacenándose en servidores, pero con una proyección hacia la computación en la nube, donde se simplifica los procesos en las instituciones médicas garantizando rentabilidad, disponibilidad y oportunidad en los tratamientos. Pero la información médica y tratamientos de los pacientes es un nicho importante para los ciberdelincuentes por la información sensible y delicada, con serias consecuencias para la seguridad del paciente, elegibilidad en términos de aseguramiento e impacto en sus finanzas.

5.4.1 Historia Clínicas Electrónicas (HCE).

Se define como historia clínica electrónica el registro integral y cronológico de las condiciones de salud del paciente, que se encuentra contenido en sistemas de información y aplicaciones de software con capacidad de comunicarse, intercambiar datos y brindar

herramientas para la utilización de la información refrendada con firma digital del profesional tratante. Su almacenamiento, actualización y uso se efectúa en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad y acceso, de conformidad con la normatividad vigente (Ley No. 2015, 2020, p. 1).

Según Jerez (2019) la comisión séptima del senado de la república aprobó, en primer debate, un proyecto de Ley buscando un proceso de sistematización y digitalización de todas las historias clínicas electrónicas del país, contando con un único registro que se pueda consultar los documentos de todos los pacientes, garantizando la eficiencia en la atención médica y poner a disposición de los médicos los datos de los pacientes, modernizando el sistema de salud. Con todo lo anterior, se debe mantener los tres pilares de la seguridad con el fin de que los datos de los pacientes no sean expuestos al público y sean tratados de una manera profesional y ética, a través de los médicos o las personas que requieran esta información para el uso de tratamientos y progreso del paciente.

Según la ISO/TR 20514:2005 se define el HCE como un depósito de información sobre el estado de salud del paciente en forma procesable a través de los sistemas computaciones. El propósito principal del HCE es proporcionar un registro documentado de la atención que respalde el presente y futuro del paciente, así mismo su evolución y el tratamiento médico. Esta documentación proporciona un medio de comunicación entre los médicos que contribuyen a la atención del paciente, además contiene la información del progreso y retroceso para cada paciente (ISO/TR 20514, 2005).

Además el HCE formulan políticas y normas de cumplimiento por las entidades que integran el sistema de salud regulando la calidad de los servicios de obligatorio cumplimiento por todas las entidades promotoras de salud, implantando modelos con el diligenciamiento de las historias clínicas en el sistema nacional de salud en Colombia, así mismo las características básicas que deben tener tales como: la integridad, secuencialidad, racionalidad

científica, disponibilidad y oportunidad, manteniendo la reserva legal (Resolución número 1995, 1999).

5.5. CIBERRIESGOS ASOCIADOS A LA COMPUTACIÓN EN LA NUBE DE UNA INFRAESTRUCTURA COMO SERVICIO

Un ciber riesgo es un ataque que implica pérdida financiera, daño de la reputación de la organización o interrupción del negocio resultado de una falla en sus sistemas de una información (Parra, 2015). De acuerdo con Eling & Schnell (2016) un ciber riesgo está constituido por los siguientes elementos:

- ✓ Una actividad no autorizada.
- ✓ Un agresor. Aquel usuario individual o colectivo que busca hacer daños a la organización o un objetivo.
- ✓ Una vulnerabilidad.
- ✓ Un ataque.
- ✓ Una consecuencia. Los efectos que se generan basados en las intencionalidades de los ciberdelincuentes.

La adopción de servicios basados en la computación en la nube tiene asociados nuevos ciber riesgos, debido a las nuevas tecnologías que se están utilizando. Por ello, es necesario identificar los ciber riesgos para la gestión y minimización del impacto en una infraestructura como servicio para las Entidades Promotoras de salud, los ciber riesgos son:

a. **Pérdida de Gobierno:** Incluye el control de las políticas y los procedimientos operativos que afectan a la infraestructura como servicio de la computación en la nube de la organización. En su tesis doctoral Rebollo propone un marco ISGCloud que se integra con cualquier tipo de nube basándose en los procesos de gobierno de TI tales como: Evaluar-Dirigir-Monitorizar y Comunicar. Así mismo, cubre las diferentes etapas del ciclo de vida del gobierno (Rebollo, 2014, p. 128):
   - ➢ Planificación y Definición Estratégica.

- Análisis de Seguridad Cloud.
- Diseño de Seguridad Cloud.
- Implementación o Migración del servicio
- Operación segura del Cloud
- Terminación del servicio.

b. **Fallos en el aislamiento:** Una característica de la computación en la nube son los recursos compartidos. Aunque no es común, el fallo de los mecanismos que separa el almacenamiento, memoria, enrutamiento y la reputación entre los diferentes clientes puede generar riesgos (Bouchaala, Ghazel, Saidane & Kamoun, 2017, p. 306). Como con cualquier servicio compartido, los Tenant no están totalmente aislados en una computación en la nube. Muchos proveedores de servicios en la nube utilizan la virtualización para separar clientes, lo que incluye compartir máquinas virtuales, ofreciendo más protección que dentro de un servidor, pero aún no proporcionan aislamiento completo (Tari, Yi, Premarathne, Bertok & Khalil, 2015, p.32).

c. **Cumplimiento y conformidad:** Migrar a la nube puede crear riesgos para obtener la certificación de la organización si el proveedor de servicios no puede proporcionar pruebas de cumplimiento (de España, 2011, p.16).

d. **Comprometer la interfaz de gestión:** se puede plantear un riesgo mayor porque se accede a ella a través de Internet y facilita el acceso a mayores conjuntos de recursos, permitiendo el acceso a usuarios no autorizados (NIST, 2011).

e. **Protección de datos:** Puede ser difícil para los clientes verificar el procedimiento de gestión de datos del proveedor de servicios en la computación en la nube. Los datos que se almacenan en entornos Cloud suelen residir en equipamiento compartido por múltiples clientes. Por ello, las organizaciones que gestionan datos confidenciales en la nube deben preocuparse por la forma en que se accede a dichos datos y garantizar que la información se encuentre almacenada de forma segura (de España, 2011, p.25).

f. **Eliminación de datos incompleta o insegura:** Debido a los múltiples contratos de arrendamiento y la reutilización de recursos de hardware, hay un mayor riesgo que la información no sea eliminada completamente, adecuadamente o de una manera oportuna (ISACA, 2015, p. 151).

g. **Infiltrado malicioso:** Los arquitectos de las soluciones en la nube tienen funciones de alto riesgo. Un infiltrado malicioso puede causar en la infraestructura como servicio un daño de alto grado comprometiendo la información sensible de los pacientes. Por esta razón se debe implementar políticas por roles específicos para cada usuario. Las actividades maliciosas se pueden repercutir sobre: la confidencialidad, la integridad y la disponibilidad de todos los tipos de datos, los servicios, sobre la organización y la confianza del cliente (Salazar & Verónica, 2013).

5.6. AMENAZAS EN LA COMPUTACIÓN EN LA NUBE

Los entornos en la nube enfrentan demasiadas amenazas debido a la gran cantidad de datos almacenados en los servidores de la computación en la nube, el cual los proveedores se convierten en un objetivo atractivo. Dentro de las amenazas comunes enfocadas a una infraestructura como servicio (laaS) para las Entidades Promotoras de salud (EPS) en cuanto a historias clínicas electrónicas, donde la Cloud Security Alliance (CSA) las enumera de la siguiente manera:

a. **Violación de Datos:** Afecta la confidencialidad, disponibilidad e integridad de los datos sensibles de los pacientes y de la organización. Se deben cifrar los datos en reposo, ya que si son robados por el atacante no podrán ser usados. La violación de datos se puede definir como la violación de seguridad en la que se copian, transmiten, visualizan roban, destruyen, alteran o usan de forma no autorizada datos sensibles, protegidos o confidenciales, los cuales pueden ser almacenados, trasmitiéndose o ser procesados de cualquier otra forma (Galmés, 2016, p.13).

b. **Pérdida de Datos:** Puede ocurrir debido a fallas de hardware o ataques maliciosos en el sistema, comprometiéndose los datos, derivando pérdida de imagen de la compañía, daños económicos, problemas legales, entre otros; afectando la disponibilidad. Se deben implementar políticas de respaldo para superar este tipo de amenazas (Hendre & Joshi, 2015, p. 1082). CSA en su encuesta ha enumerado que la pérdida de datos es la segunda amenaza más importante en la computación en la nube con casi el 91% de los inquilinos en la nube. La pérdida de datos ocurre principalmente a ataques internos que incluyen la eliminación de datos, la corrupción de datos y la pérdida de la clave de cifrado de datos (Zhu, Hill & Trovati, 2016, p. 221).

c. **Secuestro de la cuenta de servicio:** Este tipo de ataque es bastante conocido, técnicas como el phishing y la explotación de fallas de seguridad de las aplicaciones permite a los ciberdelincuentes tener acceso a la información, afectando la confidencialidad, autenticación, disponibilidad e integridad de los usuarios. Los hackers pueden robar los datos personales de los usuarios, los datos sensibles de los pacientes, como las credenciales bancarias. Se deben implementar políticas de detección de fraude y antiphishing para reducirlos. En un entorno de computación en la nube, si un atacante obtiene las credenciales de un usuario puede acceder a manipular datos, devolver información falsificada o redirigir a otros usuarios a sitios maliciosos (González, 2016, p. 43).

d. **Denegación del servicio:** Impiden a que los usuarios legítimos accedan a sus datos, además es una forma sencilla y efectiva de hacer caer una red. El atacante puede cambiar la clave de cifrado o puede poner lento el sistema para que los usuarios no puedan utilizar los servicios, afectando la disponibilidad. Un atacante que planea un DDoS, podría enviar muchas peticiones ficticias para lograrlo. Este ataque podría generar una utilización de los recursos de memoria, procesamiento, uso de disco duro y ancho de banda de la red (Díaz, 2014). Para evitar este tipo de ataques, los usuarios

y los proveedores de la nube deben desarrollar un mecanismo para que los atacantes no puedan distinguir los patrones de comunicación

e. **Abusos de los servicios en la nube:** Los usuarios pueden hacer un mal uso de las propiedades de la nube para piratear otros datos de la organización. Además, puede presentar un inadecuado control de otorgamiento de permisos, creando el riesgo de un mal uso de la nube (Peña, 2011). Los proveedores de la nube deben protegerse contra los usuarios que accedan a los datos de pacientes de otros usuarios.

f. **Problemas de compartir tecnología:** Cualquier vulnerabilidad en los diferentes sistemas que gestionan compartir tecnología en la nube, como puede ser el hypervisor, puede significar una violación de los datos almacenados de los usuarios, además de comprometer al sistema de la computación en la nube. En el 2012, un fallo en el hypervisor en la plataforma Xen, permitió a los atacantes obtener derechos de administración del sistema y así ejecutar código arbitrario accediendo a las cuentas de los usuarios y sus datos (Galmés, 2016, p.15). Dicha amenaza afecta la confidencialidad, disponibilidad e integridad. Esta estrategia de uso compartido debe implementarse en todos los dominios de la computación en la nube, además monitorear el sistema en las Entidades Promotoras de salud (EPS).

g. **Amenazas persistentes avanzadas (APT):** Especialmente está diseñado por varios vectores de ataques complejos y que permanece oculta durante un periodo de tiempo prolongado, es sigiloso, lo que significa que es silencioso y se esconde de antivirus o escaneo de redes, regenerándose hasta alcanzar el objetivo (Chandra, Challa y Pasupuleti, 2015). Es la combinación de diferentes amenazas tales como: amenazas de día cero, amenazas polimórficas y amenazas combinadas.

Las APT se pueden realizar en seis (6) pasos que son:

- ✓ **Reconocimiento:** Recopila la información de la organización de las Entidades Promotoras de salud, cuentas de acceso y demás información que pueda ser dirigido para ser utilizado en intrusión.
- ✓ **Intrusión:** Se logra cuando convence a un usuario, médico o paciente de que abra un archivo adjunto o haga click en un enlace que no debe abrir, infectando el sistema.
- ✓ **Whale Phishing:** A través de un correo electrónico que parece de una persona conocida o una multinacional con el fin de robar los datos y la información de las Entidades Promotoras de salud (EPS).
- ✓ **Explotación:** El cibercriminal roba y extrae la información de historias electrónicas clínicas de los pacientes que se encuentra en la nube de forma sigilosa. En esta etapa, el intruso establece la persistencia y el control total de la infraestructura como servicio en la nube.
- ✓ **Black Door:** Después de que logra la intrusión, se establece de una forma remota para que el atacante pueda continuar moviéndose por la red en la infraestructura como servicio en la nube comprometida.
- ✓ **Comando y Control:** Mantiene un acceso total de la infraestructura como servicio (Chandra, Challa y Pasupuleti, 2015, p.3).

En el documento *"Intelligence based Defense System to Protect from Advanced Persistent Threat by means of Social Engineering on Social Cloud Platform"* Chandra, Challa y Pasupuleti (2015) dicen que las APT se clasifican principalmente en seis (6) tipos que son:

- ✓ Infectado por un virus al navegar por un sitio web.
- ✓ Ataque dirigido por correo electrónico.
- ✓ Inducción a través de archivos descargados.
- ✓ Infectado con virus a través de un medio como USB.
- ✓ Ataques distribuidos de denegación de servicio.
- ✓ Ataques avanzados.

5.7. VULNERABILIDADES EN LA COMPUTACIÓN EN LA NUBE

Las vulnerabilidades representan un grado de exposición, un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad. En las plataformas Cloud los sistemas e infraestructuras comparten la seguridad, pudiendo tener deficiencias y debilidades en las configuraciones e inclusive por el uso inadecuado de los usuarios finales en la nube (Vargas, 2018, p. 28).

En la computación en la nube se puede obtener el acceso a través de tres rutas de ataque. El primero explota las vulnerabilidades en los mecanismos de control de acceso a la nube. El segundo comienza robando credenciales válidas de un usuario en la computación de la nube en algún lugar fuera de ella. La tercera ruta de ataque comienza con el cibercriminal usando credenciales válidas y acceso legítimo previo a la computación de la nube (Gonzales, Kaplan, Saltzman, Winkelman, & Woods, 2015).

Según Alvarez (2012) las vulnerabilidades que existen y que se pueden presentar en la computación en la nube son:

a. **Vulnerabilidades AAA:** El módulo de control de acceso contiene mecanismos de gestión de identidad, autenticación, autorización y auditoría (AAA). En la computación de la nube los usuarios y sus activos se encuentran en un perímetro de seguridad diferente. Se deben tener cuidado especial en la autenticación, autorización y las cuentas del sistema que los proveedores de servicios que van a usar. Un mal diseño de los sistemas AAA podrían resultar que los usuarios no autorizados tengan acceso a los recursos de una infraestructura como servicio en la computación en la nube. Un atacante podría explotar algunas vulnerabilidades de la gestión de identidad y el modelo de control de acceso, mecanismos débiles de recuperación de contraseña, lenguaje de control de marcado extensible débil (XACML), entre otros (Bouchaala, Ghazel, Saidane & Kamoun, 2017, p. 306).

b. **Acceso remoto al manejo de interfaz:** Los proveedores de servicios de la nube exponen un conjunto de interfaces de software o API que se utilizan para interactuar con los servicios en la nube. El proveedor de servicios publica estas API regularmente. Un atacante puede estudiar estas API y aprovechar las vulnerabilidades para lanzar ciberataques (Hendre & Joshi, 2015, p. 1082).

c. **Vulnerabilidades de Hypervisor:** En entornos de virtualización los hypervisores se usa para controlar los recursos físicos asignados para cada máquina virtual. La explotación de las capas de las máquinas virtuales puede resultar la exposición de los datos sensibles de las historias electrónicas clínicas existentes en el sistema de una infraestructura como servicio. Desde otra perspectiva, Bouchaala, Ghazel, Azouz y Kamoun (2017) aportan a este mismo punto sustentando de la siguiente manera:
   - ✓ El uso compartido de imágenes de máquinas virtuales puede crear riesgos de seguridad, publicando en el directorio compartido una imagen que podría contener un malware.
   - ✓ Las máquinas virtuales en el mismo host se deben aislar lógicamente para evitar la violación de datos, explotando los ataques entre máquinas virtuales y las fugas de datos.
   - ✓ El usuario puede restaurar el estado previo de una máquina virtual, propagando errores de configuración tales como: volver a habilitar cuentas deshabilitadas y almacenar contraseñas anteriores.
   - ✓ Para permitir la comunicación entre máquinas virtuales, el proveedor de servicios virtualiza la red, pero se pueden presentar algunos ataques tales como: Denegación del servicio (DoS) y spoofing.

d. **Vulnerabilidades en el cifrado de la comunicación:** Mientras que la información de las historias electrónicas se transmite a través de la Internet o entre diferentes medios, es posible que un cibercriminal pueda capturar y robar los datos debido a la mala autenticación. Muchos sistemas fallan debido a errores en la implementación. Algunos sistemas no aseguran que el texto plano se destruya después de encriptarse.

Otros sistemas usan archivos temporales para proteger contra la perdida de datos durante un bloqueo del sistema o usan memoria virtual para aumentar la memoria disponible (Álvarez, 2012).

e. **Vulnerabilidades en aplicaciones Web:** Las aplicaciones en la nube heredan las mismas vulnerabilidades que las aplicaciones tradicionales. Las principales vulnerabilidades son: inyección SQL, Cross-Site Scripting (XSS), exposición de datos confidenciales, falsificación de solicitudes en sitios cruzados, entre otros. Se debe tener en cuenta que un pequeño fallo de seguridad puede llegar a comprometerse todo el sistema, por eso se debe identificar y mitigar el mayor número posible de amenazas y vulnerabilidades en una fase temprana del ciclo de vida de desarrollo de software. Un software seguro es diseñado, implementado configurando y puesto en marcha con el fin de que se cumpla algunas características esenciales, tales como que continúen operando en presencia de ataques, aísle o mitigue el daño y que se recupere lo antes posible (Barba, 2017).

f. **Seguridad en los Datos:** Para mantener la solidez de la computación en la nube, el proveedor de servicios debe crear copias de seguridad para garantizar la disponibilidad de los datos en caso de incidente intencional o no intencional; además el proveedor de servicios debe tener replicación según las regiones la información que se encuentre protegida garantizando la disponibilidad de los datos. Con esta vulnerabilidad se puede presentar perdida de datos que se puede realizar de forma voluntaria o involuntaria debido a una modificación o eliminación, violando la confidencialidad y privacidad de los datos. Hoy en día, el cifrado presenta una solución para evitar la violación de datos, otro mecanismo para resolver este problema es utilizar mecanismos de respaldo. Si algunos de estos mecanismos sufren vulnerabilidades, es riesgo de pérdida de datos aumentarán (Bouchaala, Ghazel, Saidane & Kamoun, 2017).

g. **Falta de Tecnología y Soluciones estándar:** los datos pueden estar ligados a un proveedor. Es un riesgo demasiado importante si el proveedor de servicios cesa la operación, deteniendo el uso de servicios de gestión de identidad y tecnologías de seguridad externa como la gestión federada de la identidad. Cada proveedor tiene sus propias herramientas de gestión para que el usuario administre los servicios tales como: software, sistemas operativos y hardware (González, 2016, p. 50).

5.8. MATRIZ DE VALORACION DE LOS CIBERRIESGOS

De acuerdo con los ciber riesgos planteados el activo crítico a proteger son las historias clínicas de los pacientes, ya que se encuentra información sensible y vulnerable que puede violar la privacidad de los derechos fundamentales de las personas. Como acto seguido se clasifican los riesgos de la siguiente manera:

a) **Riesgo Operativo**: Comprenden el funcionamiento y operatividad de los sistemas de información, de la definición de los procesos, de la estructura de la EPS y entre la articulación de la interoperabilidad de las Entidades promotoras de salud.

b) **Riesgos Financieros:** se relaciona con el manejo de los recursos que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos y le manejo de los bienes.

c) **Riesgos legales:** Se asocia con la capacidad de la EPS para ejecutar la normatividad y requisitos legales con el fin de cumplir con la protección de la información sensible de las HCE.

5.8.1 Evaluación del Riesgo.

Una vez definido los ciber riesgos, las vulnerabilidades, las amenazas y el activo de información, se calcula el nivel de riesgo y el tratamiento a aplicar a través del modelo

planteado, según el siguiente mapa de riesgos definido en la guía de gestión de riesgos de Mintic:

PROBABILIDAD	IMPACTO			
	Menor	Moderado	Mayor	Catastrófico
Improbable	Bajo	Bajo	Medio	Alto
Posible	Bajo	Medio	Medio	Alto
Probable	Medio	Medio	Alto	Alto
Casi Seguro	Medio	Alto	Alto	Alto

Tabla 1: Guía gestión de riesgos
Fuente: Mintic

Teniendo en cuenta lo anterior, se presenta a continuación el análisis de los ciber riesgos identificados anteriormente con controles preventivos que se presentan en el modelo de ciberseguridad propuesto:

RIESGO		Principio afectado	Impacto	Control
Identificación	Clasificación			
Pérdida de Gobierno	Legal Financiero	Confidencialidad Integridad No repudio Identidad Autenticidad	Alto	Gestión de Políticas: Control de las políticas y procedimientos de Seguridad de la EPS. regulándose bajo le Ley HIPAA y Ley 1581 de 2012.
Fallos en el aislamiento	Operativo	Confidencialidad Integridad	Alto	Gestión de Infraestructura y Gestión de aplicaciones: Limitar el acceso a máquinas virtuales, aislar las máquinas virtuales que se ejecutan en la misma máquina física.
Cumplimiento	Legal	Confidencialidad No repudio	Alto	Gestión de Políticas: Se debe regular con la ley HIPAA y Ley 1581 de 2012.
Comprometer la interfaz de Gestión	Operativo	Confidencialidad Identidad Autenticidad Integridad	Alto	Gestión de acceso e identidad: garantizar un proceso de autenticación, autorización e identidad.
Violación de Datos	Legal Financiero	Confidencialidad Integridad Disponibilidad	Alto	Gestión de Datos: cifrar el servidor de almacenamiento monitorear la utilización en la nube. Los datos se deben firmar digitalmente durante el almacenamiento y la verificación de la integridad de realiza antes de usar los datos.
Infiltrado malicioso	Operativo	Confidencialidad Integridad Disponibilidad Identidad	Alto	Gestión de Políticas: Implementación de políticas por roles específicos para cada usuario.

Abuso de los servicios en la nube	Legal	Confidencialidad Identidad	Alto	Gestión de Datos: cifrar el servidor de almacenamiento monitorear la utilización en la nube. Los datos se deben firmar digitalmente durante el almacenamiento y la verificación de la integridad de realiza antes de usar los datos.
Problemas de compartir tecnología	Operativo	Confidencialidad Integridad Disponibilidad	Alto	Gestión de Infraestructura y Gestión de aplicaciones: Limitar el acceso a máquinas virtuales, aislar las máquinas virtuales que se ejecutan en la misma máquina física. Además, se deben realizar un despliegue seguro de nuevas funcionalidades al sistema.

Tabla 2: Análisis de ciber riesgos
Fuente: Creación propia

6. MARCO REFERENCIAL

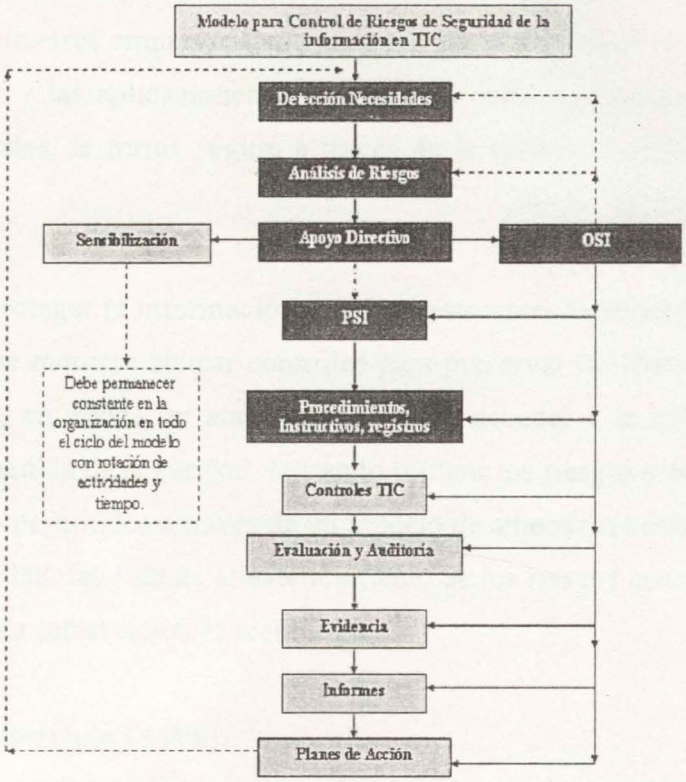
6.1. MODELOS DE SEGURIDAD

Los modelos de seguridad se han convertido en un esquema de acción estratégico del negocio, mediante el cual se establece diferentes directrices de seguridad de la información en cada uno de los procesos de la organización, de acuerdo con ello Gómez (2007) establece que un modelo de seguridad de la información es un diseño que promueve la utilización de mecanismos efectivos y sólidos para la definición e implementación de controles.

Por otra parte, Milicevic & Goeken (2011) en su investigación "*Application of models in Information Security Management*" afirma que un modelo de seguridad de una empresa debe relacionarse e integrarse con modelos como COBIT, ITIL, ISO 27001 (p. 3). Esta vinculación permitirá integrar diferentes modelos como una herramienta útil con el fin de diseñar un modelo que se adapte a la naturaleza de la organización.

Burgos & Campos (2012), plantean un modelo para facilitar la obtención de un adecuado nivel de control de riesgos en Tecnologías de la Información y Comunicación (TIC) permitiendo disminuir o evitar las fallas en los sistemas, redes, Internet y los activos de información (p. 234).

Con el propósito de enfrentar correctamente los ciberataques, se deben establecer modelos de ciberseguridad con un nivel adecuado de controles externos e internos como lo plantea Burgos, de manera que se pueda abarcar todos los procesos que se manejan por medio de las TICS en una organización. Estos controles deben estar abalados por políticas, procedimientos e instructivos que permitan operar de manera clara y precisa para asegurar el correcto cumplimiento de los controles.



Gráfica 6: Modelo de Seguridad de la Información en TIC
Fuente: (Burgos & Campos, 2012, p. 249)

6.2. MODELOS DE SEGURIDAD EN LA COMPUTACIÓN EN LA NUBE

Al utilizar modelos de arquitectura de seguridad en la computación en la nube, el cliente coloca los activos de la organización bajo la custodia del proveedor de servicios en la nube, al hacerlo el cliente cede el control de estos activos y así le transfiere la responsabilidad de la seguridad y el cumplimiento normativo de estos activos al proveedor de servicios en la nube. Esto crea riesgos, que han hecho que algunas empresas duden en suscribirse a los servicios ofrecidos en la computación en la nube (Catteddu y Hogben, 2009). Los proveedores ofrecen certificaciones de seguridad con el fin de asegurar la calidad de sus controles de mitigación de riesgos.

Es así como, en el artículo ***"Pratical Methods for Securing the Cloud"*** escrito por Edward G. Amoroso y publicado por ***"IEE COMPUTER SOCIETY"***, se plantean métodos y

soluciones prácticas para proteger la infraestructura y los servicios en la nube. La solución más común es con perímetros empresariales para proteger el contenido de la nube, con este enfoque, los servicios y las aplicaciones son accesibles solo para usuarios que han sido debidamente autenticados de forma segura a través de la Internet Corporativa (Amoroso, 2014).

Por lo tanto, para proteger la información y la infraestructura tecnológica a través de un modelo de seguridad se requiere aplicar controles para preservar los datos, teniendo varias medidas de seguridad, en donde un atacante que desee acceder a la información deberá vulnerar más de una medida de seguridad, logrando mitigar los riesgos y bloquear el acceso a usuarios que no están permitidos a través de un modelo de amenazas basados en un modelo de defensa en profundidad, facilitando el entendimiento de los riesgos que estarán expuestos en un sistema y/o en una infraestructura tecnológica.

6.2.1 Amazon Web Services (AWS).

Este proveedor de computación en la nube brinda confidencialidad, integridad y disponibilidad de los datos del cliente. Los recursos de TI están disponibles a bajo costos, además no se requiere una inversión inicial de infraestructura. AWS proporciona flexibilidad en términos de cantidad de recursos que los clientes requieran. Con la computación en la nube de AWS se implementan miles de servidores sin demora, por lo tanto, AWS permite el desarrollo, la implementación y el despliegue rápido de una aplicación a nivel mundial a un costo mínimo.

AWS tiene una seguridad de red que se controla y administra adecuadamente, teniendo en cuenta los siguientes puntos:

- Arquitectura de red segura.
- Puntos de acceso seguros.
- Protección de transmisión.
- Segregación corporativa de Amazon.
- Diseño tolerancia a fallas.

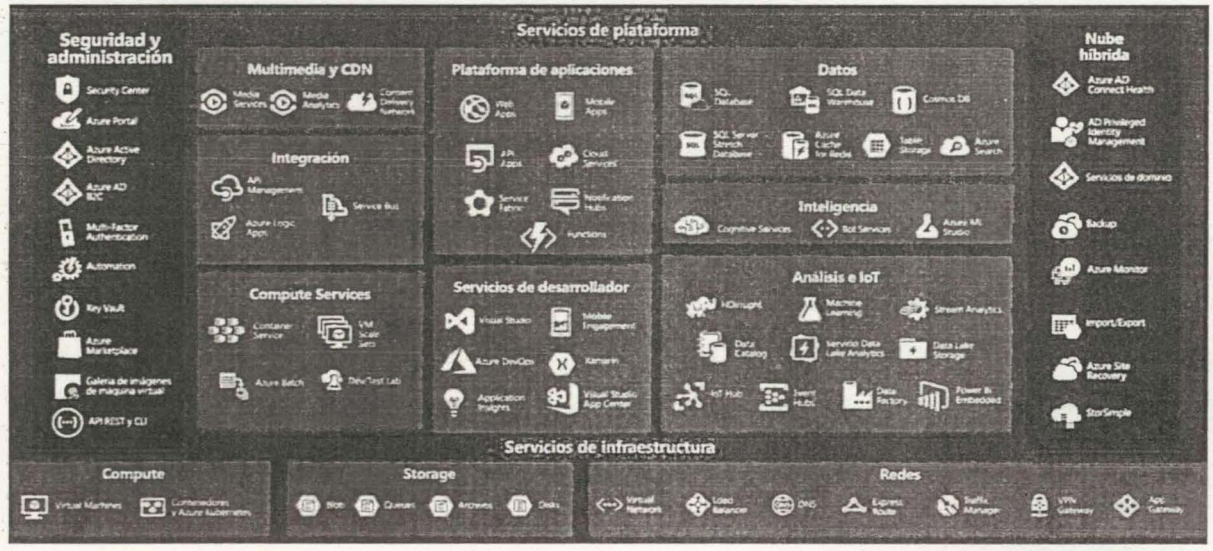
- Monitoreo y protección de redes.

Estos servicios de seguridad proporcionados por AWS son la razón que los clientes generan confianza al brindarles dichos servicios, el cual debería ser el objetivo principal de la computación en la nube (Narula & Jain, 2015).

6.2.2 Microsoft Azure.

Azure es la plataforma informática en la nube de Microsoft. Proporciona más de 100 servicios, desde ejecutar aplicaciones en máquinas virtuales hasta explorar paradigmas de software, como bots inteligentes, inteligencia artificial y aprendizaje automático que se puede comunicar naturalmente con los usuarios mediante la vista, el oído y la voz. También facilita soluciones de almacenamiento que crecen dinámicamente para dar cabida a grandes cantidades de datos (Microsoft, 2019).

Azure cumple con los siguientes requisitos de seguridad: privacidad, cumplimiento, gestión de identidad y acceso e Infraestructuras seguras. Los servicios de plataforma e Infraestructura, además sus características disponibles en Azure son los que se visualizan en la gráfica 7:



Gráfica 7: Servicios disponibles en Azure tomado de Microsoft Azure - 2019

6.2.2.1 Seguridad de la laaS en Azure.

Los usuarios en Azure desean tener el control total de sus implementaciones, por lo general utilizan Infraestructura como Servicio (laaS) para sus soluciones. Azure brinda funciones de seguridad para proteger dichas implementaciones. Las máquinas virtuales deben protegerse a través de instalaciones que puedan filtrar las solicitudes en su propia red, en lugar de que las solicitudes sea la que tenga que actuar. En cualquier caso, es necesario proteger las máquinas virtuales de modo que las solicitudes no autorizadas ni siquiera puedan llegar. Es una buena idea quitar el acceso a internet de las máquinas virtuales. También es una buena práctica limitar la accesibilidad de los servicios de escritorio remoto desde Internet. Una buena opción es permitir únicamente que los recursos internos para RDP accedan a las máquinas virtuales que utilicen opciones de VPN de Azure

6.2.2.2 Arquitectura de N-niveles

Es una arquitectura tradicional para aplicaciones empresariales. Las dependencias se administran mediante la división de capas que realizan funciones lógicas, lógicas de negocios y accesos a datos. Una arquitectura de n niveles divide una aplicación en capas lógicas y niveles físicos. Una aplicación con n niveles puede tener una arquitectura de capa cerrada o una arquitectura en capa abierta. Esta arquitectura se implementa normalmente como aplicaciones de infraestructura como servicio (laaS), donde cada nivel se ejecuta en un conjunto independiente de máquinas virtuales (Microsoft, 2020).

6.2.2.3 Marco de Arquitectura de Seguridad en Azure

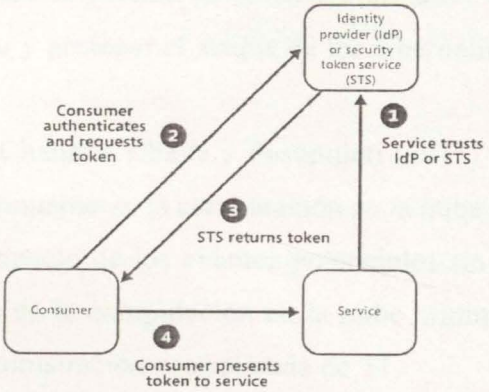
El marco de arquitectura es un conjunto de principios que pueden usar para mejorar la calidad de una carga de trabajo, el cual consta de cinco pilares de la arquitectura que son: costo, DevOps, resistencia, escalabilidad y Seguridad. En este estudio nos enfocaremos en los modelos de seguridad que constituye uno de los temas más relevantes de una arquitectura, ya que protege las aplicaciones y los datos frentes a amenazas.

Las aplicaciones en la nube están expuestas en Internet, más allá de los límites locales de confianza, a menudo están abiertas al público y pueden dar servicios a usuarios que no son

de confianza. Se debe diseñar e implementar aplicaciones de forma que se les proteja frente a ataques malintencionados, restringiendo el acceso solo a los usuarios autorizados, protegiendo la información sensible y confidencial.

Por lo anterior, teniendo una vista de arquitectura de seguridad se deben tener en cuenta tres (3) patrones de seguridad para la protección de la infraestructura tecnológica y los datos:

1. Identidad Federada: la autenticación se delega a un proveedor de identidad externo. Puede simplificar el desarrollo, minimizar los requisitos de administración de usuarios y mejorar la experiencia del usuario de la aplicación. En la siguiente gráfica si visualiza el patrón de identidad federada cuando una aplicación requiere acceder a un servicio que requiere autenticación. Se puede separar la autenticación de la autorización.



Gráfica 8: Patrón de Identidad Federada
Fuente: (Microsoft, 2020).

2. Gatekeeper: Protege aplicaciones y servicios mediante una instancia de host dedicada que actúa como agente entre los clientes y la aplicación o servicio, valida y sanea las solicitudes y datos entre ellos. Esto puede proporcionar una capa adicional de seguridad y limitar la superficie de ataque de sistema.

3. Valet Key: Usa un toquen que proporciona a los clientes acceso directo restringido a un recurso específico, con el fin de descargar la transferencia de datos desde la

aplicación. Esto es especialmente útil en aplicaciones que usan sistemas o colas de almacenamiento que se encuentra en la nube.

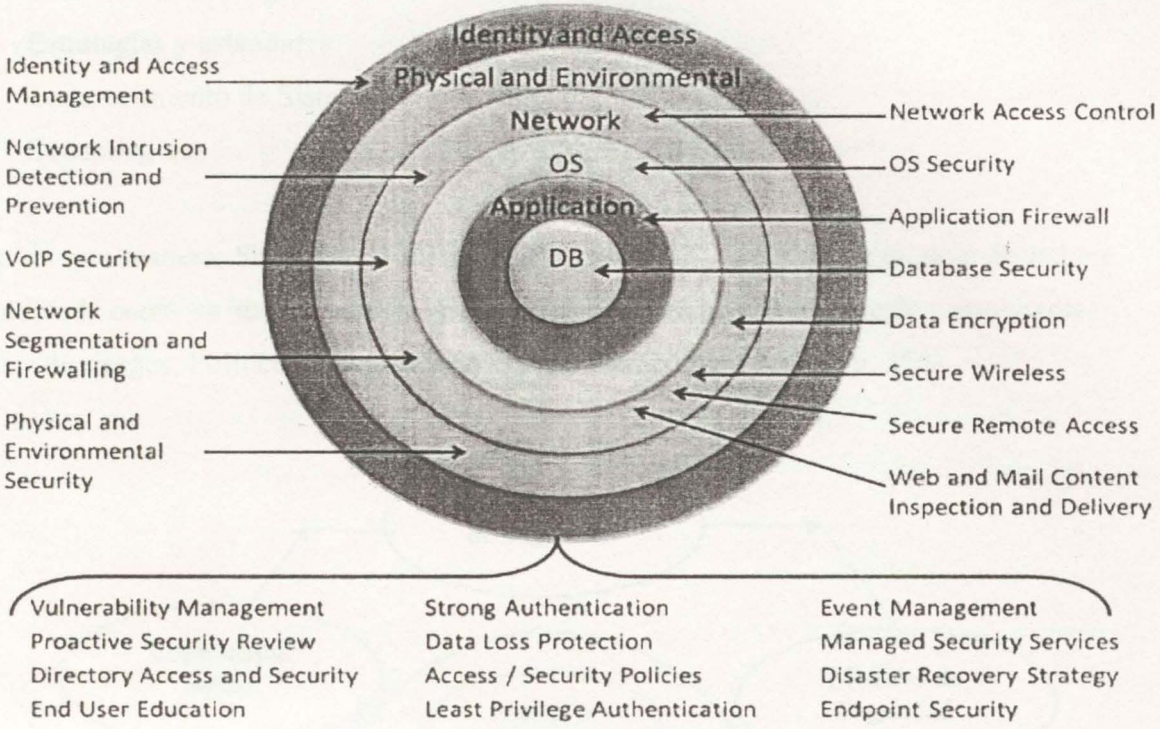
6.3. DEFENSA EN PROFUNDIDAD

El origen del concepto de "Defense in Depth" provienen de los militares, protegiendo varias líneas de defensa, retardando el ataque del enemigo. Cada línea de defensa es autónoma, la perdida de una línea de defensa debilita la otra, donde cada una dispone de diferentes medios frente a los diferentes ataques ocasionados.

La defensa en profundidad es un procedimiento de protección que resiste diferentes métodos de ataque a través de múltiples capas. tales como: aplicaciones. almacenamiento de datos. red. arquitectura de seguridad lógica y física. La defensa multicapa se encuentra más protegida en comparación con el sistema de defensa individual. La defensa en profundidad tiene como objetivo detectar y proteger el ataque de los ciberdelincuentes.

Según lo postulado por Chandra, Challa y Pasupuleti (2015) la estrategia de defensa en profundidad monitorea continuamente la computación en la nube disminuyendo el avance de los ataques, limitando el impacto de los eventos potenciales sin brindar una seguridad por completa. La virtualización de la computación en la nube minimiza el riesgo al mejorar la seguridad a través de la administración centralizada de TI.

En la siguiente gráfica se puede observar, como los datos que son la información real, son lo que se tratará de proteger con las demás capas. Así también se muestra que es vital que se posean políticas, procedimientos y una seguridad física que proteja la organización.



Gráfica 9: Sistema avanzado de defensa contra amenazas persistentes
Fuente: (Chandra, Challa y Pasupuleti, 2015, p. 4).

La gestión de acceso e identidad es el primer anillo de seguridad hacia la computación en la nube, es decir se deben brindar los permisos a los recursos autorizados por la organización, brindando técnicas criptográficas para la seguridad de los datos proporcionando confidencialidad en la información.

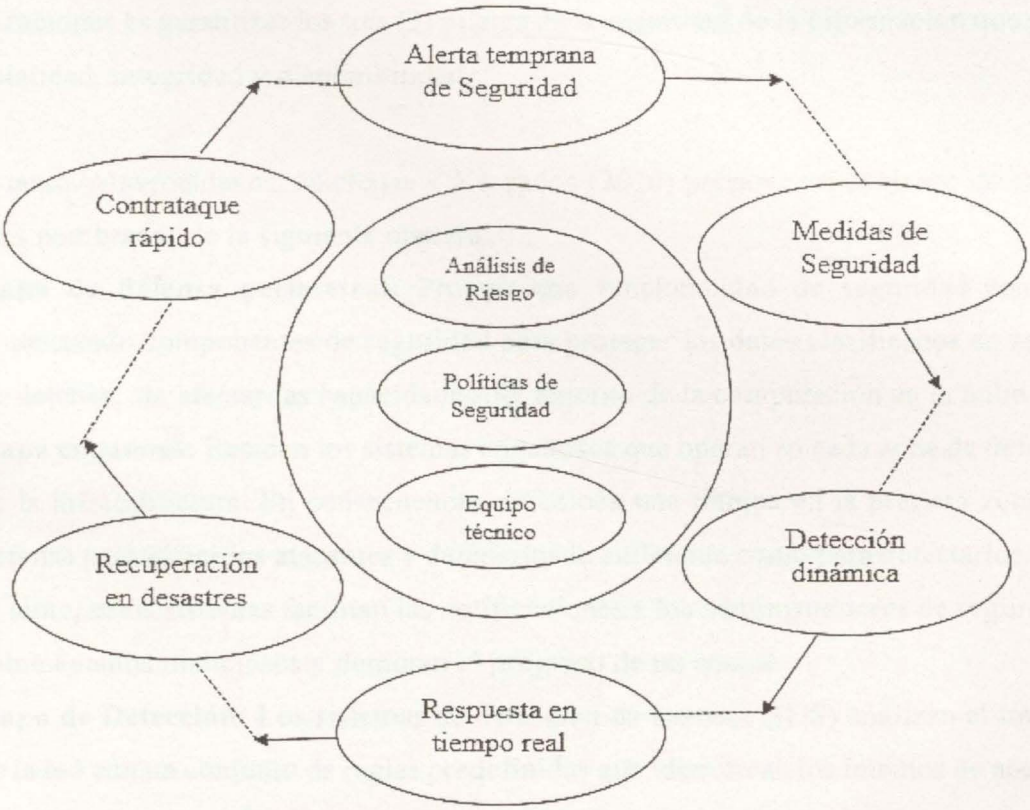
Por otro lado, Yaping, Jiahua, Yong & Zengyu (2009) afirma que:

"Un modelo de defensa en profundidad no solo debe disponer de un método de prevención activa; sino que también debe mejorar la capacidad de detección y prevención, siendo necesario considerar un modelo de defensa en profundidad que contemple las mejores prácticas de seguridad de la Información ".

El concepto de diseño de un modelo en la computación en la nube exige que la organización trabaje sobre cuatro (4) aspectos:

- ✓ Evaluación de riesgos.
- ✓ Estrategias y estándares.
- ✓ Endurecimiento de Sistemas.
- ✓ Zonas seguras.

Así de esta manera, Shengjian, Haiyan, & Fengni (2013), propone un modelo de red en profundidad, como se muestra en la gráfica 10. Éste incluye tres aspectos importantes: Análisis de riesgos, Política de Seguridad y equipo técnico de recursos (p. 355).



Gráfica 10: Modelo de Defensa basado en Control de lazo cerrado
Fuente: (Shengjian, Hayyan & Fengni, 2013)

Este modelo de defensa basado en Control de lazo cerrado incluye seis (6) técnicas de defensa que son: Alerta Temprana de Seguridad (W), Medidas de Seguridad (P), Detección Dinámica (D), Respuesta en Tiempo Real (R), Recuperación de Desastres (RP) y

Contraataque rápido (C). El modelo destaca tres (3) aspectos importantes: Alerta Temprana de Seguridad (W) y Medidas de Seguridad (P) puede ser aplicado antes de que ocurra el ciberataque; Detección Dinámica (D) y Respuesta en Tiempo Real (R) puede ser aplicado mientras el ataque ocurre; por último, Recuperación de Desastres (RP) y Contraataque rápido (C) puede ser aplicado después de que ocurre el ataque.

6.3.1 Defensa en Profundidad para entornos de computación en la nube.

La seguridad de este paradigma informático se ve afectada por los modelos de implementación, los modelos de servicio y el tipo de servicio final. El objetivo principal de las organizaciones es garantizar los tres (3) pilares de la seguridad de la información que son: confidencialidad, integridad y disponibilidad.

Por lo tanto, Mavroeidakos, Michalas y Vergados (2016) propone un conjunto de capas funcionales nombradas de la siguiente manera:

a. **Capa de defensa perimetral:** Proporciona funcionalidad de seguridad central, orquestando componentes de seguridad para proteger los datos clasificados en zonas de defensa, sin afectar las capacidades del entorno de la computación en la nube.
b. **Capa engañosa:** Residen los sistemas engañosos que operan en cada zona de defensa de la infraestructura. En consecuencia, se coloca una trampa en la primera zona de defensa para atraer los atacantes y detenerlos lo suficiente como para detectarlos. Por lo tanto, estos sistemas facilitan las notificaciones a los administradores de seguridad sobre eventos maliciosos y demoran el progreso de un ataque.
c. **Capa de Detección:** Los sistemas de detección de intrusos (IDS) analizan el tráfico de la red con un conjunto de reglas predefinidas que identifican los intentos de ataque.
d. **Capa de Criptografía:** Los procesos criptográficos se incorporan en el entorno de la nube como la criptografía de curva elíptica. Al detectar la intrusión, se puede tomar las medidas adecuadas para mitigar la amenaza. En el caso, que el cibercriminal modifique el sistema criptográfico, los datos quedaran inutilizable. Además, el protocolo TLS debe utilizarse para lograr un cifrado de extremo a extremo.

Además de los mecanismos de seguridad en cada capa, para cubrir adecuadamente las necesidades de seguridad de un entorno de la computación en la nube, es crucial definir una secuencia de políticas. Se tiene que establecer las pautas necesarias para enfrentar ataques en caso de detección y el tiempo de respuesta requerido (Mavroeidakos, Michalas & Vergados, 2016).

6.4. MODELOS DE PRIVACIDAD DE HISTORIAS CLÍNICAS

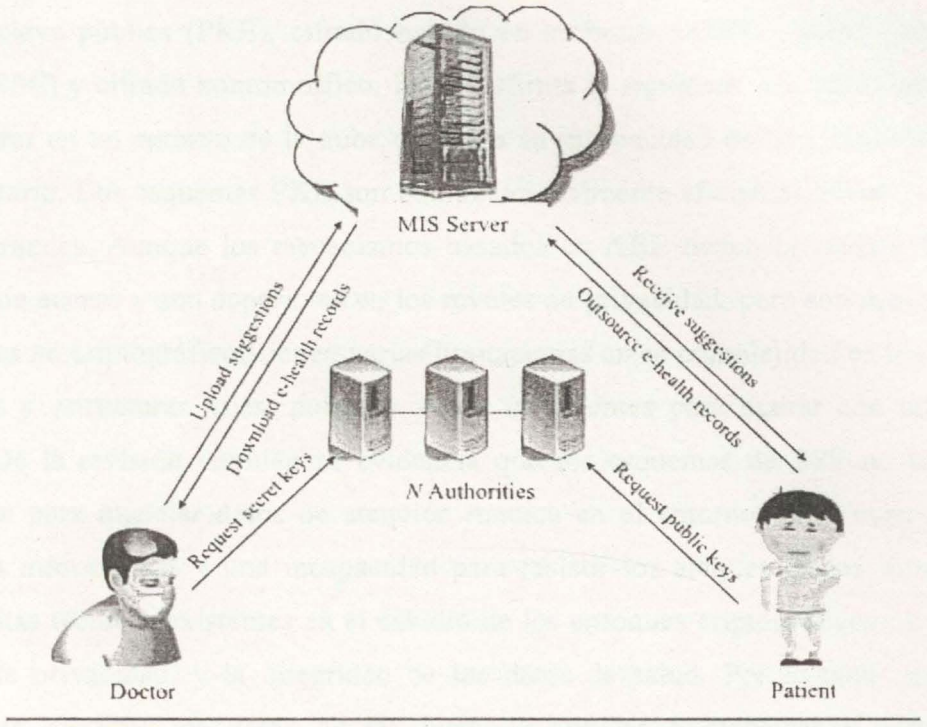
Los aspectos relacionados con la privacidad de los datos clínicos es un aspecto importante a tener en cuenta, el cual se debe tomar las medidas necesarias para asegurar la protección de la información, por lo tanto, se revisarán algunos modelos de seguridad y privacidad para sistemas de información clínicos usando diferentes técnicas para proteger los datos sensibles de salud de los pacientes.

6.4.1 Modelo de Sistema de Información Médica (MIS).

Guo, Li y Zheng (2017) plantea en su documento: "Privacy-Preserving Medical Information Systems using Multi-authority content-based Encryption in cloud" Cuatro (4) partes:

- ✓ **Servidor MIS:** Es un servidor de almacenamiento en la nube, que se encarga de almacenar los registros de salud electrónicos cifrados.
- ✓ **Autoridades:** son varias organizaciones tales como: hospitales, centros médicos, clínicas, entre otros del sector salud, que son responsables de intercambiar la información del paciente.
- ✓ **El paciente:** Crea, administra y controla sus registros de salud electrónica.
- ✓ **Doctor o médico:** Puede acceder a la información.

El modelo MIS se ilustra en la gráfica 11:



Gráfica 11: Modelo MIS
Fuente: (Guo, Li y Zheng, 2017, p.273)

En el anterior esquema, las autoridades comparten una función secreta pseudoaleatoria y lo mantienen secreto entre ellos. Para preservar la privacidad del paciente y el médico en MIS en el entorno de la computación en la nube, la clave se genera de acuerdo con el protocolo de emisión de clave anónima, el nombre y el contenido se protege simultáneamente, así de esta manera se evita la fuga de la privacidad. Dicha propuesta es un cifrado basado en contenido de múltiples autoridades sin autoridad central que es responsable de emitir claves públicas y privadas a los pacientes, por lo tanto, se puede descifrar todo el texto cifrado en el sistema.

6.4.2 Desafíos de seguridad y preservación de la privacidad de la información en la computación en la nube.

Chenthara, Ahmed, Wang y Whittak (2019) en su documento "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing" proporciona un estudio detallado de los enfoques criptográficos tales como: Cifrado de clave simétrica (SKE),

cifrado de clave pública (PKE), cifrado basado en atributos (ABE), cifrado simétrico de búsqueda (SSE) y cifrado homomórfico. Donde afirma lo siguiente: los esquemas SKE no pueden operar en un entorno de la nube debido a su incapacidad de administrar múltiples roles de usuario. Los esquemas PKE son computacionalmente eficientes debido a tamaños de claves grandes. Aunque los mecanismos basados en ABE tienen la ventaja de definir estructuras de acceso y son superiores en los niveles de privacidad, pero son muy costosos. Los enfoques no criptográficos tienen varias limitaciones en su complejidad en los procesos para definir y estructurar roles, políticas y son ineficientes para operar con un entorno dinámico. De la revisión también se evidencia que los esquemas de SSE no se utilizan ampliamente para manejar datos de atención medica en el entorno de la nube debido a limitaciones informáticas y una incapacidad para resistir los ataques de los intrusos. Sin embargo, estas técnicas existentes en el estudio de los enfoques criptográficos no logran la seguridad, la privacidad, y la integridad de los datos de salud. Por lo tanto, existe una necesidad de proteger los datos de las historias clínicas electrónicas y fortalecer la infraestructura de seguridad en la atención médica para garantizar la confidencialidad del paciente.

6.4.3 Arquitectura de atención médica orientada a servicios basada en la computación en la nube.

Rizvi, Wang y Chen (2018) proponen una arquitectura de servicios compuesta por cuatro (4) capas que son:

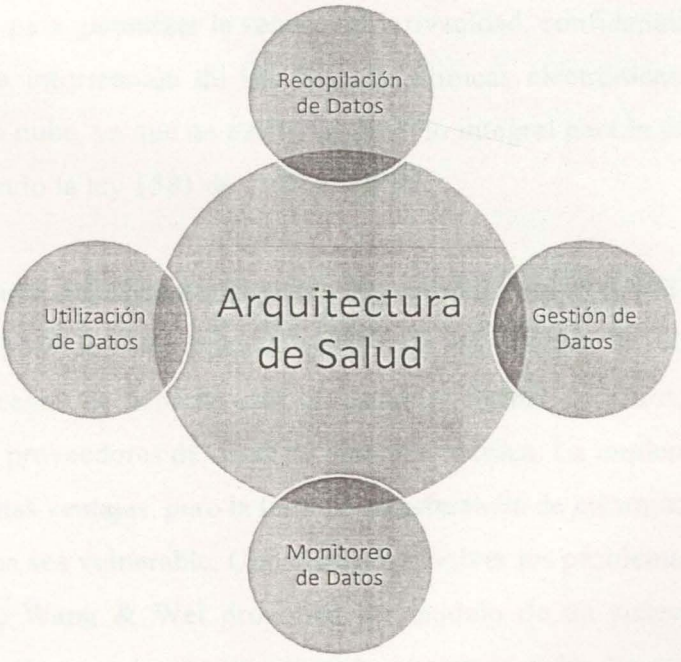
a. **Capa de aplicación en tiempo real de la nube:** El primer componente de esta capa considera la situación exacta del paciente. Al acceder a la actualización instantánea del paciente, es fácil de analizar la condición y tomar medidas según las circunstancias. El médico puede examinar las actividades de cualquiera de sus pacientes y puede advertirle si la situación es perjudicial para el paciente.

b. **Capa de Servicio:** Proporciona la necesidad de cualquier sistema. Está dividido en dos subcapas que son: Capa de servicio en la nube que es para el cuidado de la salud,

hay diferentes servicios disponibles tales como: Red como un servicio, información como un servicio, Cooperación como un servicio, datos como un servicio e infraestructura como un servicio (Rizvi, Wang & Chen, 2018). Y otra subcapa que es servicios web en la que se puede obtener información útil del paciente.

c. **Capa de infraestructura de la nube:** Proporciona herramientas analíticas para administrar y manipular los datos. Esta capa contiene dos módulos que son los siguientes: Servicio GIS, que se relacionan con los registros médicos Gestiona la información del paciente antes de que sea manipulada en el almacenamiento de la nube. Computación en la nube, es uno de los mecanismos para manipular los datos acumulados de diferentes fuentes (Rizvi, Wang & Chen, 2018).

d. **Capa de Salud:** la capa de atención medica consta de cuatro (4) módulos. como recopilación de datos, gestión de datos, monitoreo de datos y utilización de datos. la arquitectura se observa en la gráfica 12.



Gráfica 12: Arquitectura de Salud
Fuente: (Rizvi, Wang & Chen, 2018).

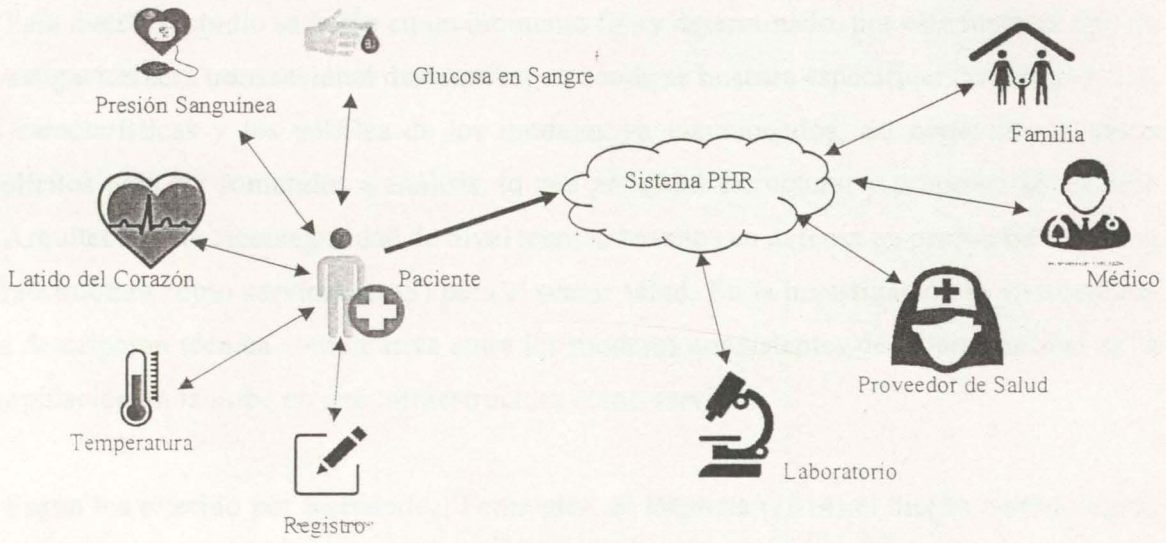
Esta propuesta incorpora cuatro capas entre las cuales la funcionalidad de la cuarta (4) capa es responsable de hacer una asociación entre las corporaciones de atención médica al almacén de la nube, y hacer que los expertos clínicos analicen los datos para sacar conclusiones de los datos. Además, las primeras tres capas están procesando los datos recopilados en la nube de diferentes fuentes para que tengan un formato estructurado. Los datos procesados son analizados por los médicos. También, podemos decir que este sistema incorpora la integración del mecanismo de computación en la nube junto con tecnologías emergentes como: Big Data, Analytics y sistemas inteligentes, lo que lo hace un modelo preciso y distintivo. Por último, este modelo también presenta problemas relacionados con la seguridad y la privacidad de la información de los pacientes.

Una de las soluciones es superar todas esas limitaciones introduciendo un sistema de historias clínicas electrónicas controlado personalmente, en el que el paciente es el dueño de la información clínica y de consentimiento universal de los datos para todos los interesados como los médicos, enfermeras, farmacéuticos, científicos, excepto en emergencias o solicitado por la fiscalía según lo que establece la ley. Con el modelo que se plantea tiene un enfoque potencial para garantizar la seguridad, privacidad, confidencialidad, disponibilidad e integridad de la información de las historias clínicas electrónicas en el entorno de la computación en la nube, ya que no existe un modelo integral para la protección de los datos sensibles cumpliendo la ley 1581 de 2012 e HIPPA.

6.4.4 Arquitectura del Sistema Registro Personal de Salud (PHR) en la nube.

PHR es una aplicación electrónica de gestión de información de salud médica, donde los registros se almacenan de acuerdo con un estándar formal de HIPAA y HL7 que fueron adoptados por los proveedores de salud de atención médica. La implementación del PHR en la nube tiene muchas ventajas, pero la falta de transferencia de información de manera segura hace que el sistema sea vulnerable. Con el fin de resolver los problemas de seguridad, Chen, Chiang, Liu, Lai, Wang & Wei proponen un modelo de un sistema de cifrado seguro orientado al paciente en entornos de computación en la nube, basado en emparejamiento

bilineal sobre la curva elíptica (2016). En la gráfica se representa el modelo de arquitectura del PHR.



Gráfica 13: Sistema PHR entorno en computación en la nube
*Fuente: (*Chen, Chiang, Liu, Lai, Wang & Wei, 2016)

El sistema PHR orientado al paciente tiene grandes ventajas como la reducción de costos, compartir información de manera exitosa, ser escalable. Los usuarios pueden utilizar un protocolo de transferencia mejorando la comunicación con la autoridad de confianza. En consecuencia, puede brindar información correcta y proteger los datos de ser revelados. La idea principal es que el receptor seleccione el mensaje deseado bajo las condiciones que el remitente no puede saber qué mensaje es elegido por el receptor, mientras que éste tampoco puede conocer el contenido de otros mensajes excepto el que se elija *(*Chen, Chiang, Liu, Lai, Wang & Wei, 2016).

7. METODOLOGÍA

7.1. TIPO DE INVESTIGACIÓN

Para nuestro estudio se harán en un momento fijo y determinado, por esta razón el tipo de investigación será transeccional descriptiva, en donde se buscará especificar las propiedades, las características y los perfiles de los modelos ya mencionados, así como los procesos implícitos para ser sometidos a análisis, lo que permitirá estructurar y proponer un modelo de Arquitectura de ciberseguridad de nivel técnico basados en defensa en profundidad en una infraestructura como servicio (IaaS) para el sector salud. En la investigación se va a realizar una descripción técnica comparativa entre los modelos coexistentes de ciberseguridad de la computación en la nube en una infraestructura como servicio.

Según los referido por Hernández, Fernández, & Baptista (2014) el diseño metodológico planteado para este proceso de investigación se orienta desde una perspectiva no experimental la cual se realiza sin manipular deliberadamente variables. Es decir, se trata de estudios en los que no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para analizarlos. Para esta propuesta observaremos y consultaremos información relevante acerca de los modelos de arquitectura de ciberseguridad de la información digital enmarcado en la computación en la nube en una infraestructura como servicio orientado al sector salud.

7.2. DISEÑO DE LA INVESTIGACIÓN

El diseño de la investigación está interconectado a la metodología que se utilizó para lograr los objetivos específicos. La investigación se efectúo por etapas, de acuerdo con las mejores prácticas y estándares internacionales sobre seguridad de la información y datos sensibles en la computación en la nube.

7.3. FASES DE LA INVESTIGACIÓN

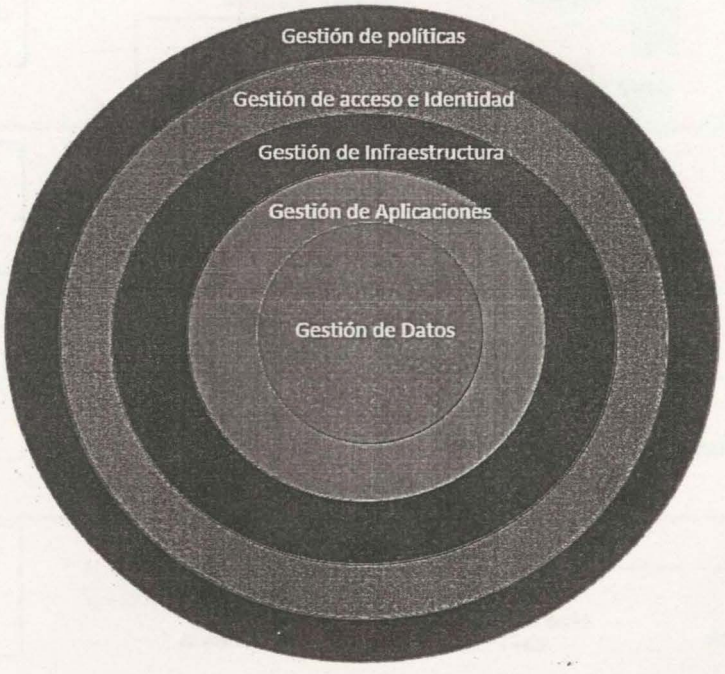
Para el desarrollo de la investigación y cumplimiento de los objetivos planteados de llevará a cabo las siguientes fases de investigación:

FASE	DESCRIPCION
Acopio bibliográfico	Detecta y consulta la bibliografía que puedan ser útiles para este estudio, así como extraer y recopilar la información relevante y necesaria que atañe nuestra investigación.
Revisión bibliográfica	Consulta los documentos en el sistema de bibliotecas tales como IEEE, SCOPUS, revistas indexadas y de carácter científico e investigativo, con el fin de evaluar los datos consultados.
Análisis de la Información	Clasificación y caracterización de la información encontrada en los documentos en los sistemas de bibliotecas.
Organización del material	Organizar el material y la información más relevante para la elaboración del estado del arte respecto al tema seleccionado.
Diseño del Modelo	Planteamiento del modelo de Arquitectura de ciberseguridad en una infraestructura como servicio (laaS) basados en defensa en profundidad para el sector salud, respecto a las historias electrónicas clínicas, con el fin de proteger la información sensible de los pacientes enfocados en los pilares de la seguridad de la información.

Tabla 3: Fases de la Investigación

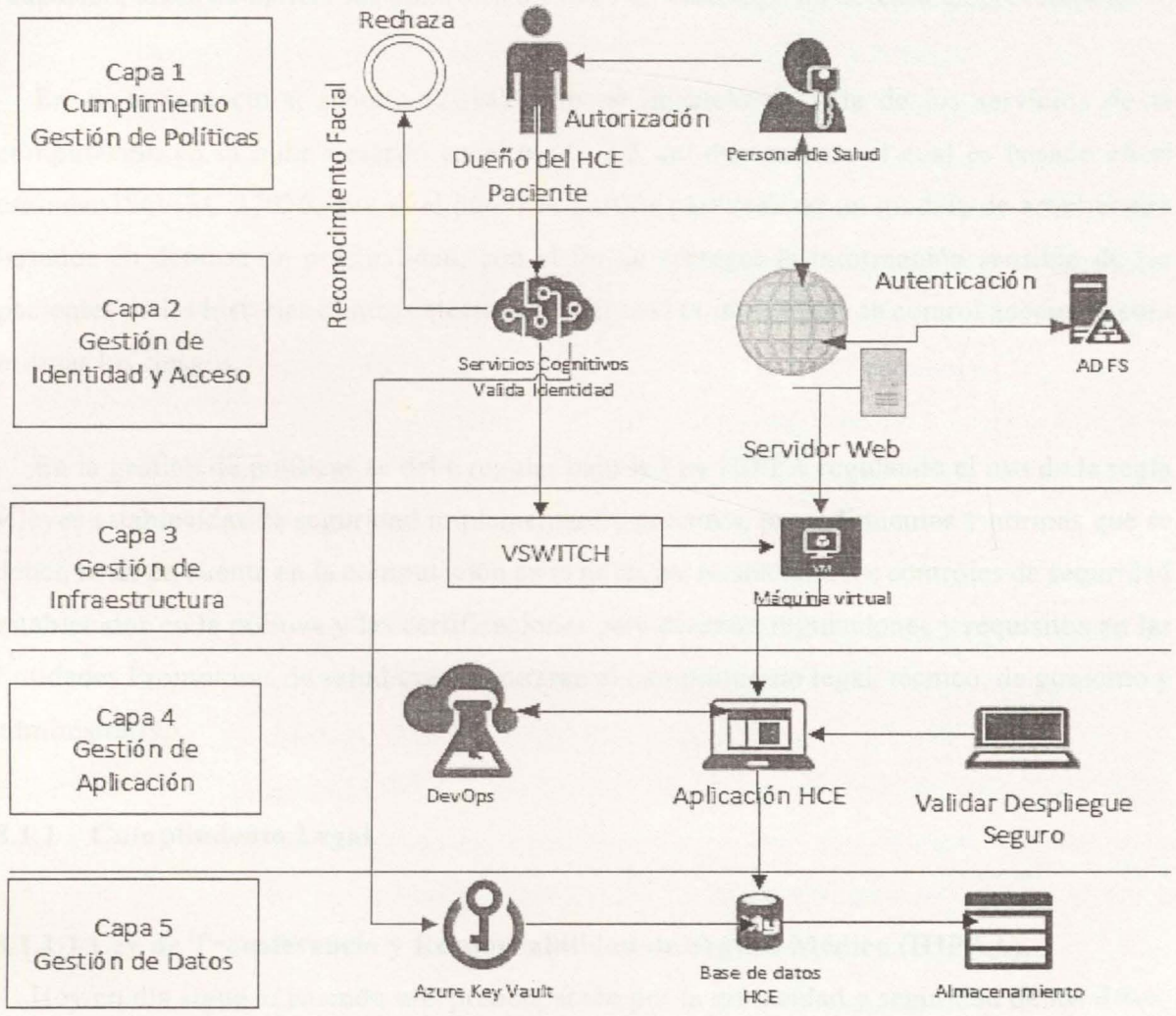
8. MODELO DE CIBERSEGURIDAD PARA EL SECTOR SALUD

De acuerdo al proyecto de ley que se pretende impulsar en Colombia facilitando, agilizando y garantizando el acceso a los derechos de salud y a la información de los pacientes en el país, combatiendo la corrupción y fomentando la competitividad de las organizaciones en el sector salud, es decir si un médico atiende a un paciente en la zona costa del país y por cuestiones diferentes el mismo paciente necesita atención médica en otra zona de Colombia, pueda ser atendido y además el médico conozca el estado general de salud del paciente, eso se puede lograr conociendo la historia clínica digitalmente, así lo manifestó el senador Carlos Fernando Motoa. Pero no todo el mundo debe poder acceder a la información de las historias clínicas, se debe plantear un modelo con controles de ciberseguridad basados en defensa en profundidad para una Infraestructura como Servicio (IaaS), con el fin de proteger los datos de los pacientes dando cumplimiento a la Ley 1581 de 2012, así mismo regularse bajo las pautas de la LEY HIPAA de EE. UU. para la atención médica y divulgación de la información sensible de salud. El modelo general se define de la siguiente manera:



Gráfica 14: Modelo en Ciberseguridad basados en Defensa en profundidad. Creación del autor.

El modelo se basó en el marco de arquitectura de Seguridad de Azure y los patrones de diseño de seguridad con una arquitectura de capa cerrada, además con una vista de arquitecto, orientado a los sistemas técnicos en defensa en profundidad basándose en estándares y mejores prácticas de organizaciones internacionales reconocidas sobre seguridad de la información, los cuales deben garantizar los pilares fundamentales de la seguridad que son: Confidencialidad, integridad, disponibilidad y no repudio. El modelo de ciberseguridad se plantea con las siguientes capas de defensa, y se visualiza en la siguiente gráfica:



Gráfica 15: Modelo en Ciberseguridad basados en Defensa en profundidad para HCE. Creación del autor.

8.1. GESTIÓN DE POLÍTICAS

Es la primera capa de defensa en profundidad que se establecen los procesos y procedimientos internos, el cual son los componentes que respaldan la gestión de la política, de forma que estos documentos se encuentren alineados a la estructura de gobierno de seguridad de los servicios de computación en la nube en la organización del sector salud, bajo el estándar ISO/IEC 27000. Se deben integrar con otras áreas tales como legal, cumplimiento, diversas áreas de TI, entre otras; con el fin de participar en el proceso de redacción, antes de aplicar los controles técnicos en cada capa de defensa en profundidad.

En su tesis doctoral rebollo (2014) propone un ciclo de vida de los servicios de la computación en la nube descrito en el punto 2.5 del documento. el cual es basado en el estándar ISO/IEC 27036. que es el punto de partida para realizar un modelo de arquitectura basados en defensa en profundidad, con el fin de proteger la información sensible de los pacientes de las historias clínicas electrónicas, el cual es un entorno de control adecuado para mitigar los riesgos.

En la gestión de políticas se debe regular bajo la Ley HIPPA regulando el uso de la regla y leyes establecidas de seguridad implementando procesos, procedimientos y normas que se deben tener en cuenta en la computación en la nube, así mismo con los controles de seguridad establecidos en la política y las certificaciones para diversas regulaciones y requisitos en las Entidades Promotoras de salud que aseguraran el cumplimiento legal, técnico, de gobierno y administrativo.

8.1.1 Cumplimiento Legal.

8.1.1.1 Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA).

Hoy en día sigue existiendo una preocupación por la privacidad y seguridad de los datos, debido a que los usuarios están empleando la computación en la nube para datos menos confidenciales, y no se aprovecha por completo las ventajas que ofrece la computación en la

nube, así de este modo el historial de los pacientes que se encuentran bajo esta tecnología debe regularse bajo las pautas del HIPAA. Esta ley de EE. UU. establece los requisitos para el uso, divulgación y protección de la información de salud de los pacientes, aplicándose a todas las entidades de atención médica que manejan información sensible de los pacientes (Ley 104-191 de 1996).

Desde la misma perspectiva esta ley regula el uso y la divulgación en cuatro (4) áreas generales:

a. **Regla de Privacidad:** reglamenta el uso y la divulgación de la información de salud protegida por entidades cubiertas, resguardando la confidencialidad de los pacientes. Estas entidades cubiertas pueden facilitar la información para el tratamiento o las operaciones de atención médicas sin la autorización por escrito del paciente. Así mismo, pueden divulgar la información de salud si se solicita a través de una orden judicial. La regla de la privacidad requiere que las entidades cubiertas notifiquen a las personas sobre el uso de la información protegida y realicen un seguimiento de las divulgaciones, además documenten las políticas y procedimientos de privacidad. Los pacientes tienen derecho a acceder a toda la información protegida relacionada con su salud y autorizar la entrega a través de un método seguro.

b. **Regla de Seguridad:** Es un complemento de la regla de la privacidad. Se establece en tres (3) tipos de seguridad
   - ✓ **Administrativa:** Se deben desarrollar e implementar políticas y procedimientos necesarios, identificando cuales usuarios tienen accesos a la información de salud electrónica que se encuentra protegida y restringirla a solo aquellos que la requieran para su función laboral. Además, se deben realizar auditorías internas para revisar las operaciones con el objeto de identificar las violaciones de seguridad.
   - ✓ **Físicas:** Se debe controlar el acceso físico a los datos protegidos. El acceso a los servidores que contiene la información debe ser controlado y

monitoreado. Si las organizaciones utilizan proveedores deben estar completamente capacitados en la protección de la información de Salud.

- ✓ **Técnico:** Controla el acceso a los sistemas informáticos, permitiendo proteger las comunicaciones que contiene la protección de la información de Salud que son transmitidas electrónicamente a través de las redes abiertas. Los datos dentro de un sistema no se deben borrar, ni modificarse de manera no autorizada. Para garantizar la integridad de los datos y autenticidad de la información debe utilizarse firmas digitales y autenticación de mensajes (Assistance, 2003).

c. **Regla de identificadores únicos:** Las organizaciones cubiertas por el HIPAA como los proveedores, los centros de atención médica y los grandes planes de salud deben usar el identificador único, con el fin de corroborar a las entidades de atención médica inscritas con el HIPAA.

d. **Regla de Cumplimiento:** Las organizaciones en EE. UU. deben cumplir según lo establecido del HIPPA, la cual puede establecer sanciones monetarias y civiles por violar dicha ley (Microsoft, 2019).

8.1.1.2 Ley 1581 de 2012.

La ley 1581 de 2012 regula el tratamiento de datos personales tiene por objetivo desarrollar el derecho constitucional que tiene toda persona conocer, actualizar y rectificar las informaciones contenidas en cualquier base de datos. En el artículo dos (2) establece los ámbitos de la aplicación sobre los principios y disposiciones de ley que serán aplicable a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamientos por entidades de naturaleza pública o privada. Así mismo, en el artículo nueve (9) el titular de la información autorizará el tratamiento de los datos personales y sensibles, la cual debe ser obtenida por cualquier medio que pueda ser objeto de consulta posterior. Por último en el artículo diecinueve (19) establece que la entidad de ejercer la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos,

garantías y procedimientos es la superintendencia de industria y comercio, haciendo uso de sus funciones de autoridad de protección de datos.

Por esta razón, la ley 1581 de 2012 protege el tratamiento de los datos de salud definiendo los principales criterios de seguridad y confidencialidad de la información, que se encuentre siempre disponible para quien esté autorizado para el manejo de los datos, además se debe garantizar que esa información se mantenga integra y no se pueda modificar.

La ley obliga a las organizaciones de salud a revisar internamente el uso de los datos sensibles y personales contenidos en sus sistemas de información y replantear las políticas para el manejo de la información y fortalecimiento en temas de seguridad de las herramientas, se deben definir los fines y medios para el tratamiento de los datos y los deberes que se adscriben a los principios de la administración de datos y a los derechos de la intimidad del dueño de la información personal.

8.1.1.3 Ley 1273 de 2009.

A través de la ley 1273 de 2009 se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos", preservando integralmente los sistemas que utilizan las tecnologías de la información y las comunicaciones. Esta ley establece lineamientos de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos personales y de los sistemas informáticos. Esta Ley obliga a las organizaciones a prestar atención al tratamiento de equipos informáticos, así como el tratamiento de los datos personales teniendo en cuenta que se debe velar por la seguridad de la información sensible y personal (Ley 1273, 2009).

8.1.1.4 Ley 527 de 1999.

Esta ley se definió y reglamentó el acceso y uso de los mensajes de datos, del comercio electrónico y las firmas digitales, estableciendo las entidades certificadoras. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella

tiene la intensión de acreditar este mensaje de datos y de ser vinculado con el contenido del mismo (Ley 527, 1999).

8.1.1.5 Ley 2015 de 2020.

La ley 2015 de 2020 tiene por objeto regular la interoperabilidad de la Historia Clínica Electrónica a través de la cual se intercambiarán los elementos de datos clínicos relevantes, así como los documentos y expedientes clínicos del estado de salud de los pacientes. A través de las historias clínicas se facilitará, agilizará y garantizará el acceso y ejercicio de los derechos a la salud y a la información de las personas, respetando el Hábeas Data y la reserva de la información. Los prestadores de servicios de salud estarán obligados a diligenciar y disponer los datos, documentos y expedientes de la historia clínica en la plataforma de interoperabilidad que disponga el gobierno Nacional. Todas las prestadoras de servicios de salud seguirán teniendo la responsabilidad de guardar y custodiar las historias clínicas de los pacientes en sus propios sistemas tecnológicos de acuerdo con las leyes vigentes. En el artículo ocho (8) parágrafo uno (1) la información suministrada en la HCE no podrá ser modificada sin que se quede registrada la modificación. El ministerio de salud y de la protección social reglamentará el acceso a la información por parte del personal distinto al equipo de salud, en el marco de interoperabilidad de la HCE, lo cual deberá garantizar la privacidad y reserva de la historia clínica electrónica (Ley 2015, 2020).

8.1.2 Cumplimiento administrativo

8.1.2.1 Norma ISO 27001.

La primera versión de la norma fue publicada en octubre del 2005 y fue actualizada en el 2013 con su versión más reciente. En esta norma establece los requisitos para implementar, operar, monitorear, verificar y mejorar los sistemas de gestión de seguridad de la información (SGSI), indicando los controles de seguridad de las organizaciones. Este es la única norma certificable de la familia ISO 27000 (Vargas, 2018).

8.1.2.2 Norma ISO 27017.

Es de la misma familia de la ISO 27001, pero la norma 27017 brinda controles para los proveedores de servicios y usuarios en la computación en la nube, donde se especifica las funciones y responsabilidades entre las partes, con el fin de que los servicios que se presten en la computación en la nube sean tan seguros como todos los datos que se guarden. La norma brinda 37 controles para tener en cuenta relacionado a: responsabilidades entre el proveedor y el cliente, la disolución de contratos, protección virtual del cliente configuración de las máquinas virtuales, procedimientos administrativos, seguimientos de las actividades y alineación del entorno de red (Alcatara, 2019).

8.1.2.3 Norma ISO 27018.

Ésta norma proporciona unas buenas prácticas para garantizar la seguridad de la computación en la nube en el cumplimiento de las obligaciones legales en materia de tratamientos de los datos personales proporcionando a los usuarios una herramienta para verificar y auditar los niveles de cumplimiento de las regulaciones establecidas por el proveedor de servicios de la computación en la nube, garantizando que los datos no serán usados para fines distintos de lo especificado a menos que haya un consentimiento explícito según lo establecido en la ley, la solicitud de divulgación de los datos personales por parte de las autoridades administrativas o judiciales. En relación con las medidas de seguridad de la información, se contempla que todo el personal del proveedor de servicios deben firmar un acuerdo de confidencialidad para el cumplimiento de las leyes y regulaciones sobre protección de datos o privacidad, y seguridad (Alcatara, 2019).

8.1.2.4 Norma ISO 27032.

Es un nuevo estándar de ciberseguridad que fue publicado en Julio del 2012 por la organización Internacional de Normalización (ISO). Se definieron unas guías centrado en dos áreas: por un lado, se cubrieron los espacios no cubiertos por las normas anteriores de seguridad, en la cual aparece nuevos ataques en lo que se denomina un Marco de Ciberseguridad.

El marco de ciberseguridad se desarrolla en cuatro (4) áreas:

- ✓ **Prevención:** Implantación de medidas y controles.
- ✓ **Protección y detección:** Implementa controles destinados a la gestión de seguridad y la monitorización de eventos.
- ✓ **Respuesta y comunicación:** Estar preparados antes posibles incidentes relacionados con la ciberseguridad.
- ✓ **Recuperación y aprendizaje:** Acciones para restaurar los sistemas y servicios relacionados con el ciberespacio.

El proceso de esta metodología se desarrolla en cinco (5) fases:

1. Entendimiento de la organización.
2. Análisis de Riesgo.
3. Plan de Acción.
4. Implantación.

Con la norma ISO/IEC 27032 se pretende garantizar que los intercambios de información en la red sea de una manera efectiva combatiendo a los ciberataques y a los cibercriminales.

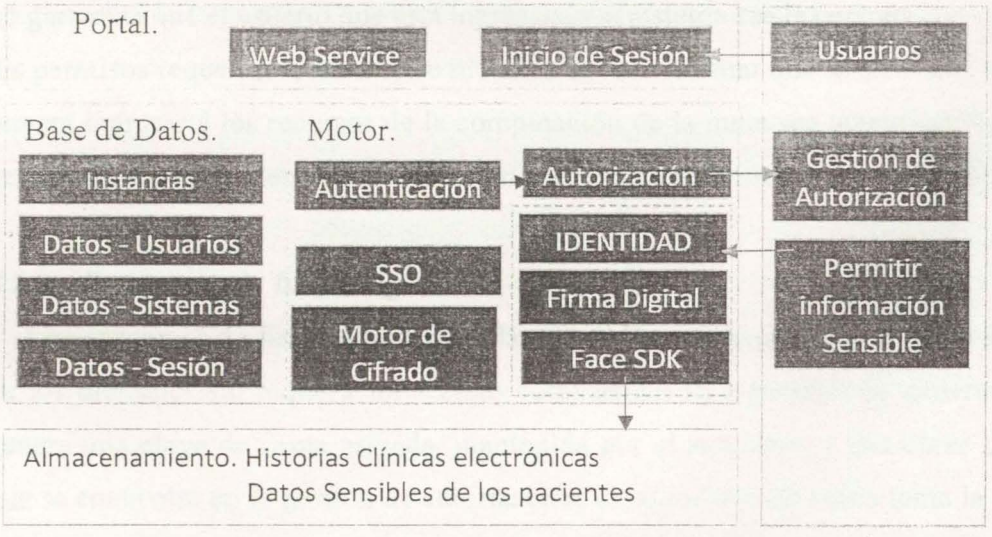
8.1.2.5 Norma ISO 27036.

Esta norma específica los requisitos fundamentales de seguridad de la información para definir, implementar, operar, monitorear, revisar, mantener y mejorar las relaciones entre proveedores y compradores. Estos requisitos cubren cualquier adquisición y suministro de productos y servicios, como fabricación o ensamblaje, adquisición de procesos comerciales, componentes de software y hardware, adquisición de procesos de conocimiento, servicios de compilación, operación, transferencia y computación en la nube. Para cumplir con estos requisitos la entidad debería tener inicialmente varios procesos fundamentales, ente los procesos incluyen: gobernanza, gestión empresarial, gestión de riesgos, gestión de recursos operativo y humanos y seguridad de la información.

8.2 GESTIÓN DE ACCESO E IDENTIDAD

La segunda capa de defensa en profundidad es la gestión de acceso e identidad el cual se decide si el usuario tiene el permiso apropiado para ingresar a la información de las historias clínicas electrónicas, identificando la necesidad real de manejar la información y verificar la intensión del usuario, luego de una comprobación exitosa, el usuario solicitante recibirá la información apropiada, la gestión de acceso e identidad debe evolucionar digitalmente ya no es solamente autenticación de nombre de usuario y contraseña, lo que significa que se debe adoptar métodos y tecnologías emergentes como una autenticación sólida a través de aprendizaje automático. El sistema comprenderá diferentes roles de los usuarios y permisos en la infraestructura de la siguiente manera: Médicos, enfermeras, administradores y pacientes. Pero los dueños de los datos en el sistema serán del paciente, salvo en algunas excepciones. Gartner define la Gestión de identidades y control de acceso como: *"la disciplina en seguridad que habilita a las diferentes identidades acceder a los recursos adecuados en el momento oportuno y por la razón necesaria"*. La gestión de acceso e Identidad mantiene la integridad y confidencialidad de los datos sensibles de las historias clínicas electrónicas haciendo que el acceso se encuentre disponible para los usuarios autorizados.

La siguiente gráfica se muestra la arquitectura de la Gestión de acceso e identidad:



Gráfica 16. Modelo de Gestión de acceso e Identidad adaptado a partir de Cloud Security Alliance (2018).

- ✓ **Usuarios:** Son los Médicos, enfermeras, administradores, pacientes que requieren ingresar a la información del paciente, se definen por roles y tienen diferentes privilegios.
- ✓ **Portal:** Es la página web donde permite que los usuarios inicien sesión y pueden ingresar a los módulos internos de la información de los pacientes.
- ✓ **Bases de Datos:** Almacena los datos de la cuenta, los datos del usuario, la información de identidad, los datos de administración del sistema y los archivos de registros.
- ✓ **Motor:** Es el módulo central de la gestión de acceso e identidad, que permite el inicio de sesión único (SSO), la autenticación, la gestión de autorizaciones, el motor de cifrado y permite el acceso a las historias clínicas electrónicas aprobado y autorizado por los pacientes según la ley 1581 de 2012, confirmando la identidad real del paciente.
- ✓ **Gestión de autorización:** lleva un registro, control y monitoreo en tiempo real de las autorizaciones realizadas por el sistema a los profesionales de las Entidades Promotoras de salud y a los pacientes.

Hoy en día la autenticación del usuario está cambiando de enfoque, el uso de contraseñas no garantiza que el usuario que está ingresando al sistema sea la persona correcta y que tenga los permisos requeridos, así de este modo se debe confirmar que la identidad del usuario que intenta ingresar a los recursos de la computación de la nube sea autentica. Por esta razón la gestión de acceso e identidad debe ser un proceso de autenticación, autorización e identidad.

8.2.1 Esquemas de firma digital.

Los esquemas de firma digital son claves públicas análogas, que preservan la integridad de los mensajes sin requerir un secreto compartido. El algoritmo de generación de claves genera una clave de firma privada, mantenida por el remitente y una clave de verificación que se encuentra en la gestión de autorización. El algoritmo de firma toma la clave de firma secreta y el mensaje produciendo una firma digital. El algoritmo de verificación toma el

mensaje, la firma y la clave de verificación pública y acepta la firma si la información no ha sido alterada. Una propiedad útil de las firmas digitales es el no repudio, lo que significa que el firmante de un mensaje no puede negar haberlo hecho (Aldemar, Crampton, &Martin, 2015).

8.2.2 Cifrado de autenticación.

El cifrado autenticado combina las propiedades de confidencialidad del cifrado, con las propiedades de integridad de los códigos de autenticación del mensaje (MAC) y las firmas digitales, asegurando así que el mensaje recibido no haya sido leído por las entidades no autorizadas y no haya sido alterado desde su creación por el remitente. Los métodos integrados para lograr esto en la configuración simétrica combinan un cifrado de bloque con un MAC o utilizan un modo de operación autenticado especial para un cifrado de bloques. Los esquemas de cifrado autenticados son más eficientes que las combinaciones manuales de mecanismos separados de privacidad e integridad (Aldemar, Crampton, &Martin, 2015).

8.3 GESTION DE INFRAESTRUCTURA

La seguridad de la Infraestructura es un punto importante para el funcionamiento en la computación en la nube, ya que es la base para que un usuario de servicios en la nube pueda implementar los recursos necesarios, pueda gestionar y prestar servicios de salud tales como las historias clínicas electrónicas de una Entidad Promotora de Salud (EPS).

Uno de los elementos importantes de la gestión de infraestructura es el hypervisor el cual se conoce como Virtual Machine Monitor (VMM) permitiendo ejecutar y crear múltiples máquinas virtuales en un único host de hardware. Es un módulo importante de virtualización que supervisa y gestiona los sistemas operativos que se puede compartir recursos virtualizados ejecutándose en un solo sistema (Mushtaq, Akram, Khan, Khan, Shahzad & Ullah, 2017, p. 187).

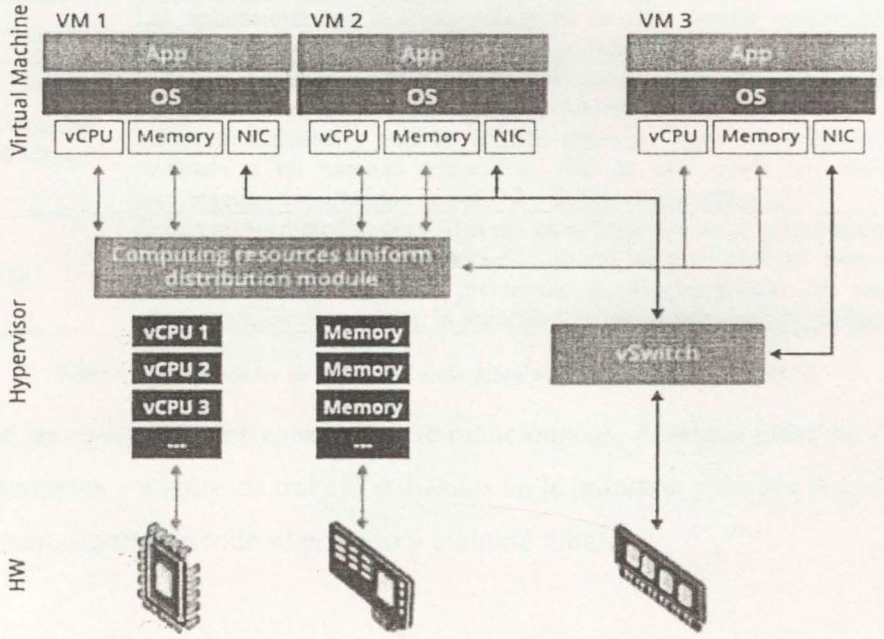
Otro de los elementos importantes es el Multi-tenan que se refiere a las características de los recursos de la computación en la nube que se comparten, incluido los datos, las memorias y los programas. Los múltiples clientes es similar como una multitarea que comparten algunos recursos de procesamiento comunes como la CPU y si no se asegura con controles de seguridad podrían presentar amenazas de confidencialidad y privacidad (Mushtaq, Akram, Khan, Khan, Shahzad & Ullah, 2017, p. 191).

Para tener una buena gestión de la infraestructura es una muy buena práctica limitar el acceso a Internet a las máquinas virtuales, además limitar la accesibilidad de los servicios de escritorio remoto desde la red externa (Internet), también tener un servidor de acceso implementando todas las restricciones de seguridad proporcionando conexiones seguras a otros servidores.

8.3.1 Virtualización.

La virtualización es un elemento importante de la computación en la nube que consiste en la entrega de recursos informáticos compartido a través de software y que son entregados como un servicio de demanda por medio de la Internet (González, 2016). Esta capa maneja y gestiona cuatro (4) recursos principales que son: CPU, Memoria, Red y almacenamiento, así podrá dinámicamente repartir los recursos entre todas las máquinas virtuales definidas.

Para que no se presente el fallo de aislamiento y sea explotado la vulnerabilidad de los hypervisores mencionados en el punto 5.7 del documento, el hypervisor debe aislar las máquinas virtuales que se ejecutan en la misma máquina física para evitar el robo de datos y los ataques maliciosos, es decir los usuarios finales solo pueden acceder a los recursos asignados a sus propias máquinas virtuales garantizando un aislamiento seguro de las máquinas virtuales. El hypervisor se gestiona de forma centralizada, garantizando que cada máquina virtual obtenga recursos físicos independientes (Chen, 2018, p. 38). La siguiente gráfica se muestra el aislamiento de las máquinas:



Gráfica 17: Aislamiento entre recursos virtuales.
Fuente: (Chen,2018, p.38)

Para gestionar mejor la infraestructura se puede proporcionar grupos de seguridad permitiendo a los usuarios controlar la interconexión y el aislamiento entre máquinas virtuales (MV), es decir las MV en el mismo grupo pueden comunicarse entre sí, si están en diferentes grupos no se podrán interconectar (Bouchaala, Ghazel, Saidane & Kamoun, 2017).

8.4 GESTIÓN DE APLICACIONES

La gestión de las aplicaciones es muy amplio y complejo, debido a que inicia desde el diseño de la aplicación y la detección de amenazas, hasta el mantenimiento, la protección y el aseguramiento de las aplicaciones en producción. La seguridad de las aplicaciones ha evolucionado tan rápido a medida que las implementaciones de aplicaciones continúan avanzando van surgiendo nuevos procesos, patrones y tecnologías. De acuerdo con la tercera capa de seguridad de defensa en profundidad *"Gestión de Infraestructura"* se tienen oportunidades para mejorar la seguridad en la gestión de las aplicaciones, la cual se relacionan en la siguiente tabla:

OPORTUNIDADES	*DESCRIPCION*
Entornos aislados	Las aplicaciones en la computación en la nube pueden aprovechar redes virtuales y otras estructuras para entornos virtuales
Máquinas virtuales independientes	El uso de arquitecturas de microservicios permiten mejorar la seguridad. En la computación en la nube los desarrolladores pueden implementar muchas máquinas virtuales y con un tamaño reducido, cada máquina virtual está dedicada a un servicio específico. Así de este modo se reducen los ciberataques, soportando controles de seguridad más granular.
DevOps	Es una nueva metodología y filosofía en el desarrollo de aplicaciones, centrada en la automatización e implantación de aplicaciones DevOps abre muchas oportunidades en seguridad mejorando el endurecimiento del código, la administración de cambios, la seguridad de las aplicaciones en producción.

Tabla 4. Oportunidades de seguridad en la gestión de aplicaciones, CSA (2018).

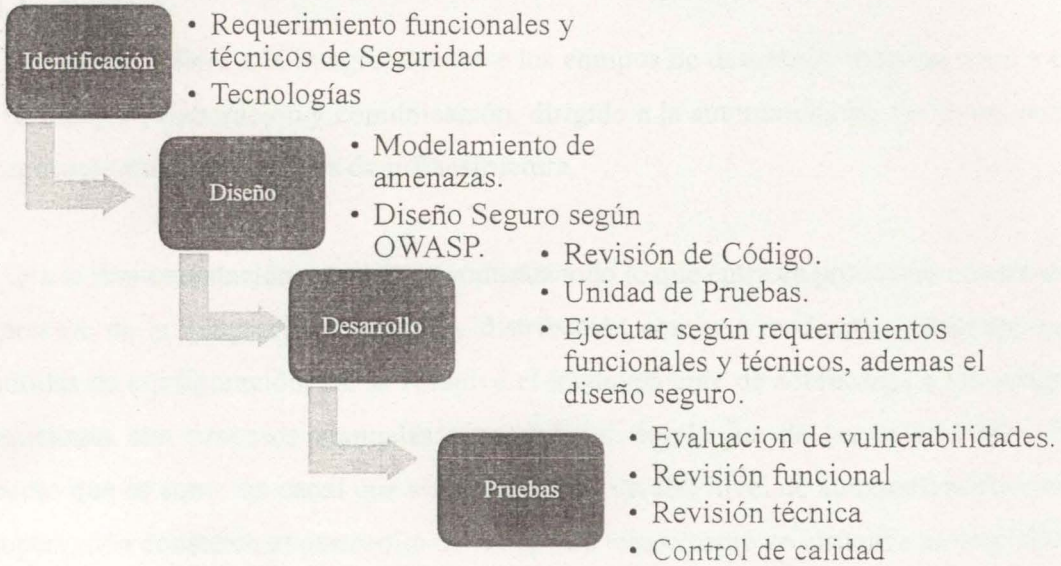
Además de las oportunidades anteriormente mencionadas, debemos tener en cuenta una serie de componentes y marcos de trabajo utilizados en la industria para que la gestión de las aplicaciones sean seguras en todo el proceso y ciclo de vida.

8.4.1 Desarrollo y Diseño Seguro.

En el desarrollo y diseño seguro se debe tener en cuenta varios elementos claves para identificar las funcionalidades de seguridad del sistema tales como: el diseño de protocolo de seguridad, el diseño de control de acceso e identidad, el control de concurrencia, la tolerancia a fallos y la recuperación de fallos. Así mismo, la implementación se puede identificar patrones de diseño de seguridad (Barba, 2017).

El proveedor de la nube requiere proteger sus aplicaciones desde el hilo interno y externo, desde el diseño hasta la puesta en marcha del aplicativo en todo su ciclo de vida. Es importante definir el proceso de seguridad y la gestión de políticas sobre el software, permitiendo al negocio desafíos para los usuarios que utilizan la computación en la nube y los proveedores que prestan dicho servicio.

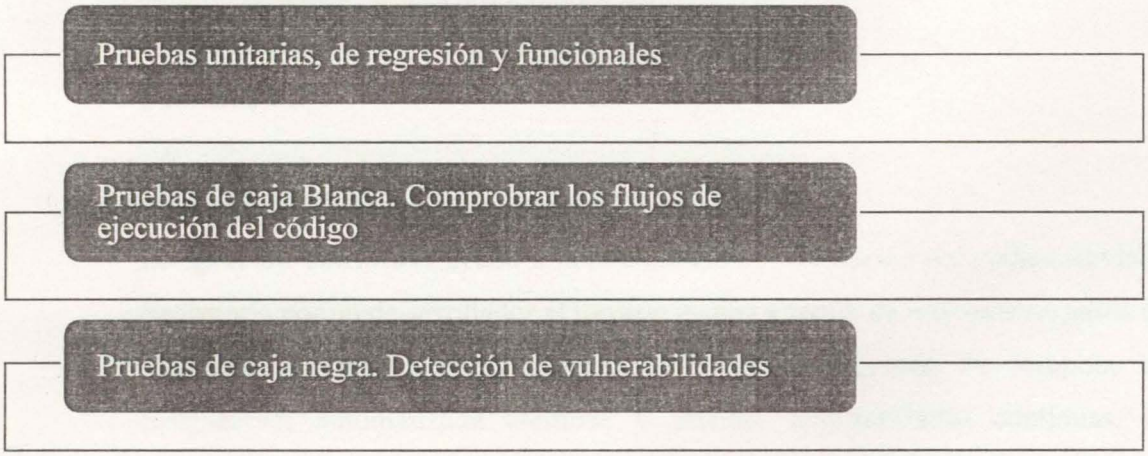
Se tienen las siguientes fases para una mejor seguridad en la gestión de las aplicaciones, además tener un diseño seguro en la computación en la nube.



Gráfica 18: Fases de desarrollo y diseño seguro.
Fuente: (CSA, 2018)

8.4.2 Despliegue Seguro.

Dado que el despliegue automático tiende ser mayor en ambientes de computación en la nube, las cuales se integran en el flujo de despliegue y se efectúa fuera del control directo de los desarrolladores. Para realizar un despliegue seguro, se debe realizar una serie de pruebas de seguridad en la gestión de la aplicación integrándose en la etapa de desarrollo y despliegue, deberían estar orientadas a la construcción de casos de prueba basados en la simulación de un atacante y el conocimiento del software y hardware típico, estas pueden ser:

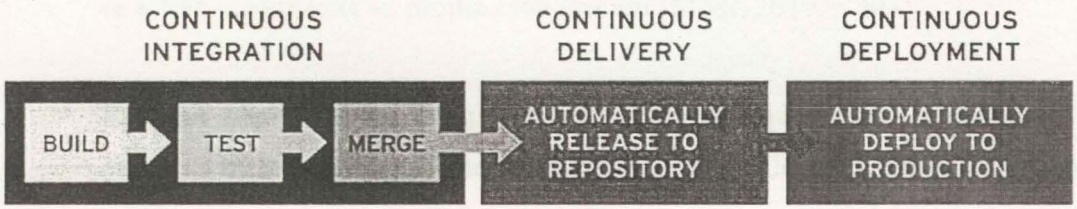


Gráfica 19: Pruebas de Seguridad.
Fuente: (CSA, 2018)

8.4.3 DevOps.

DevOps se refiere a la integración entre los equipos de desarrollo y operaciones a través de una mejor colaboración y comunicación, dirigido a la automatización de la implantación de aplicaciones y operaciones de infraestructura.

Con la implementación automática continua todo lo que entra en producción es creado por el proceso de la integración continua y distribución continua mediante código aprobado y plantillas de configuración, así se resuelve el inconveniente de sobrecarga a los equipos de operaciones con procesos manuales retrasando el despliegue de las aplicaciones. Es un proceso que es como un canal que se incorpora en un alto nivel de automatización continua y supervisión constante al desarrollo de las aplicaciones, como se visualiza en la gráfica:



Gráfica 20: Proceso DeVops según Microsoft - 2019

Los principios básicos de DevOps son:

- ✓ Agilidad.
- ✓ Automatización.
- ✓ Colaboración
- ✓ Comentarios.

Las prácticas principales son las siguientes:

- ✓ **Integración continua:** ayuda a la compilación y validación del código enviado /registrado por un desarrollador al llevarlo a cabo a través de una serie de pasos de validación La integración continua crea flujos se procesos. Se compone de compilación automatizada continua y pruebas automatizadas continuas. El resultado final de la integración continua son los paquetes de implementación que

se puede usar mediante la implementación continua para realizarlos en múltiples entornos (Modi, 2019, p 64).

- ✓ **Administración de configuraciones.**

- ✓ **Implementación continua:** se refiere a la capacidad de implementar aplicaciones y servicios empresariales en entornos de preproducción, implementar las aplicaciones y configurarlas Después de realizar varias validaciones, como pruebas funcionales y pruebas de rendimiento en un entorno de preproducción, el entorno de producción de aprovisiona, se configura y la aplicación se implementa a través de la automatización. Cuando la integración continua ha realizado su trabajo, al generar los paquetes desplegables finales, la implementación continua se activa y comienza su propia canalización (Modi, 2019, p 64).

- ✓ **Entrega continua:** es la capacidad de generar paquetes de aplicación de una manera que se pueda implementar fácilmente en cualquier entorno. Para generar artefactos que se pueden implementar fácilmente, se debe usar la integración continua para generar los artefactos de la aplicación, se debe usar un entorno nuevo o existente para implementar estos artefactos y realizar pruebas funcionales, pruebas de rendimiento y pruebas de aceptación del usuario mediante la automatización. La entrega continua incluye la integración y la implementación continuar en un entorno para validaciones finales (Modi, 2019, p 64).

- ✓ **Aprendizaje continuo.** Es posible crear aplicaciones empresariales excelentes e implementarlas automáticamente en el entorno de producción Es de suma importancia que los comentarios en tiempo real sobre el comportamiento de la aplicación se transmitan como comentarios al equipo de desarrollo tanto de los usuarios finales como del equipo de operaciones. El aprendizaje continuo ayuda a que la aplicación sea robusta y resistentes a los fallos. Ayuda a garantizar que la aplicación cumpla con los requisitos del usuario (Modi, 2019, p 64). La

arquitectura y el diseño de una aplicación deben construirse teniendo en cuenta la supervisión, la auditoría y la telemetría.

Con la implementación de DevOps las Entidades Promotoras de Salud (EPS) pueden crecer más rápidamente satisfaciendo las expectativas, aumentando la calidad, capacidad y servicios que brindará las HCE a través de la innovación y mejoras continua.

8.5 GESTIÓN DE DATOS

En la Gestión de políticas se debe definir qué tipos de datos y almacenamientos serán permitidos en las historias clínicas electrónicas para el acceso de las diferentes categorías de usuarios tales como: paciente, médicos, enfermeras, administradores, entre otros; además donde estará la ubicación para el permiso correspondiente. Además, el proveedor de la computación en la nube debe garantizar la integridad, confidencialidad y disponibilidad de los datos en reposo.

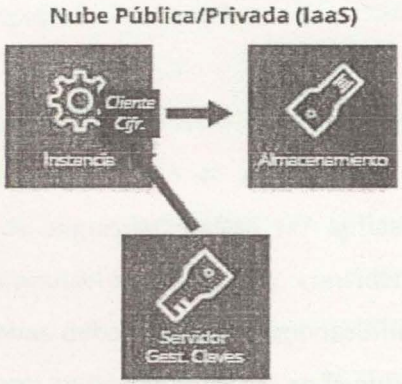
Por otro lado, el almacenamiento en la computación en la nube depende de la gestión de la infraestructura virtualizada con escalabilidad, elasticidad, recursos medidos e interfaces accesibles. El almacenamiento en la nube ofrece un entorno de almacenamiento multi-tenant apropiado para los datos no estructurados (Mushtaq, Akram, Khan, Khan, Shahzad & Ullah, 2017).

Para evitar la fuga de datos, se deben cifrar en el servidor de almacenamiento y monitorear la utilización en la nube y cualquier tipo de transferencia de datos a través de herramientas tales como Cloud Access Security Broker (CASB). La computación de la nube debe garantizar el aislamiento de los datos y el acceso seguro de la información. Los datos se deben firmar digitalmente durante el almacenamiento y la verificación de integridad se realiza antes de usar los datos.

8.5.1 Cifrado de los datos en reposo.

Como las historias clínicas manejan información sensible, cuando no se esté utilizando se debe mantener cifrado la información y los datos, con el fin de que no se puedan leer fácilmente cuando un cibercriminal llega a las historias clínicas electrónicas.

Para que el almacenamiento y volúmenes se mantenga cifrado utilizamos tres (3) componentes en el sistema de infraestructura que son: los datos, el motor de cifrado y el gestor de claves. Los datos es la información que se está cifrando, el motor de cifrado es el proceso matemático de cifrado. Finalmente, el gestor de claves manejan los passwords para el cifrado.



Gráfica 21. Cifrado de volúmenes gestionado externamente, tomado de Cloud Security Alliance (2018).

Para el sector salud se utilizará el método de cifrado gestionado externamente, el cual el motor de cifrado se ejecuta en la instancia, pero las claves son administradas en el datacenter de la organización (On-premise) y son ejecutadas a la instancia a pedido, como se visualiza en la gráfica 21. Es un esquema de almacenamiento seguro en la computación en la nube para la privacidad de la información de historias clínicas electrónicas de salud, el cual es un privilegio de control de acceso centrado en el paciente eficiente y seguro (ESPAC). Este esquema se basa en la política de texto cifrado, el atributo y la identidad (Saharan & Somani, 2015).

9 CONCLUSIONES

De acuerdo con la iniciativa del proyecto de ley que se pretende impulsar en el país para implementar las Historias Clínicas Electrónicas (HCE) con el fin de facilitar, agilizar y garantizar el acceso a la información de la salud de los pacientes, es de vital importancia garantizar la seguridad de la información y el cumplimiento de la protección de datos sensibles de los pacientes. Por esta razón, son aspectos importantes lo relacionado con la autenticación, autorización e identidad, para el acceso a las historias clínicas electrónica del paciente y de todas las capas compuestas para el control de la información mediante una adecuada estrategia a través de la gestión de políticas, permitiendo formular una serie de controles para garantizar la integridad, confidencialidad y disponibilidad de la información de los datos sensibles en la computación en la nube.

A través de los diferentes modelos de servicios investigados de la computación en la nube sirven como base para formular un modelo de arquitectura de la información, logrando deducir que los mecanismos de seguridad deben ser aplicados para proteger los datos sensibles almacenados en la computación en la nube, considerando un trabajo colaborativo entre las dos partes, ya que ambas deben asumir responsabilidades, así mismo a través de métodos y garantías que se utilizan en la computación en la nube, se exigen a los proveedores el manejo de la información de acuerdo a lo que se establece en las leyes.

Esta investigación se centró en definir barreras de protección y controles de la información sensible de las historias clínicas electrónicas como se establece en la Ley de transferencia y responsabilidad de seguro médico (HIPPA) de EEUU y la ley 1581 de 2012, además los diferentes estándares a nivel internacional que puede implicar, minimizando el impacto de los ciberataques mediante un modelo de control de capas en una infraestructura como servicio (laaS), desde la perspectiva de seguridad y gestión en cada una de las capas, protegiéndose contra las diferentes vulnerabilidades de la computación en la nube.

El modelo propuesto permite que la infraestructura como servicio (IaaS) se ejecute en entornos seguros en la nube, a través de un gobierno que establece políticas de seguridad brindando lineamientos para una operación segura en la computación en la nube como primera barrera de control. Como segunda capa se propone un submodelo de gestión de acceso e identidad que es un proceso de autenticación, autorización e identidad permitiendo a los usuarios a la información del HCE distinguiendo los derechos de acceso basados en la autorización del paciente de la información sensible del estado de salud otorgando el acceso respectivo al sistema, de lo contrario deben ser revocados. Así mismo, las demás capas se tienen diferentes controles de ciberseguridad con el fin de minimizar algún ataque u robo de la información del paciente hasta la última capa con el submodelo de cifrado de datos en reposo. La privacidad de los pacientes se preserva en los controles de seguridad en cada una de las capas y reduciendo los derechos de accesibilidad a los datos sensibles del HCE. A partir de los modelos existentes, este enfoque brinda una mejor protección técnica de la información del paciente. Es un modelo de referencia que se puede adaptar a un entorno de computación en la nube para una infraestructura como servicio en Entidades Promotoras de salud que manejan información de historias clínicas electrónicas (HCE).

Por otro lado, La computación en la nube es una tecnología emergente que brinda muchos beneficios para las organizaciones del sector salud. Sin embargo, a pesar de traer demasiadas ventajas, plantea muchos desafíos de seguridad en la adopción de la computación en la nube. Explicamos el modelo detallado de la arquitectura de computación en la nube en la que se exploraron esquemas de arquitectura, tipos de servicio, componentes de la nube y seguridad en la nube. La virtualización es una tecnología que es la base de la prestación de una infraestructura como servicio a través de la Computación en la nube. Por lo tanto, la seguridad en un entorno de virtualización debe estar asegurado.

Las limitaciones actuales del modelo proviene del uso de cifrados en tránsito de la información de las HCE, así como las amenazas desconocidas. Esas limitaciones son muy significativas para cualquier organización de la salud donde los datos del paciente pueden ser capturados o filtrados. Es por eso que el uso de un cifrado seguro mientras los datos estén en

tránsito es muy crítico. Esto puede ser un nuevo tema de investigación, el cual no se encuentra contemplado en este proyecto de investigación.

Por último, con la prevalencia de dispositivos móviles, como una investigación futura en la computación en la nube se puede utilizar en los dispositivos móviles para que las HCE se pueda revisar, en lugar de limitar el servicio a un único dispositivo terminal como el computador.

BIBLIOGRAFIA

[1] Alcantara Ramirez, M. A. (2019). Estrategia de adaptación de un sistema de gestión de la seguridad de la información universitario a computación en la nube.

[2] Alderman, J., Crampton, J., & Martin, K. M. (2015). Cryptographic tools for cloud environments. In Guide to security assurance for cloud computing (pp. 15-30). Springer, Cham.

[3] Alvarez Velasquez, E. A. (2012). Seguridad En La Nube. Revista de Información, Tecnología y Sociedad, 7.

[4] Amoroso, E. (2014). Practical Methods for Securing the cloud. IEEE Computer Society.

[5] Amoroso, E. (2014). Practical Methods for Securing the cloud. IEEE Computer Society.Assistance, H. C. (2003). Summary of the hipaa privacy rule. Office for Civil Rights.

[6] Bertolin, J. (2008). Seguridad de la Información. Redes. Informática y Sistemas de Información. Madrid. Editorial Parainfo.

[7] Bonilla, S. M., & González, J. A. (2012). Modelo de seguridad de la información.

[8] Bouchaala, M., Ghazel, C., Saidane, L. A., & Kamoun, F. (2017, October). End to end cloud computing architecture based on a novel classification of security issues. In 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA) (pp. 303-310). IEEE.

[9] Burgos, J., & Campos, P. (2012). Modelo para seguridad de la Información en TIC. Universidad del Bío - Bío, 1-20.

[10] Catteddu, D. and Hogben, G. (2009). Cloud computing: Benefits, risks, and recommendations for information security. Heraklion, Greece: ENISA.

[11] Chandra, J. V., Challa, N., & Pasupuleti, S. K. (2015). Intelligence based defense system to protect from advanced persistent threat by means of social engineering on social cloud platform. Indian Journal of Science and Technology, 8(28).

[12] Chen, K. (2018). Guideles on effectively Managing Security Service in the Cloud. Cloud Security Alliance (CSA), p.39.

[13] Chen, S. W., Chiang, D. L., Liu, C. H., Chen, T. S., Lai, F., Wang, H., & Wei, W. (2016). Confidentiality protection of digital health records in cloud computing. Journal of medical systems, 40(5), 124.

[14] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-Health solutions in cloud computing. IEEE access, 7, 74361-74382.

[15] Cloud Security Alliance (2018). Guía de Seguridad de Área crítica para la computación en la nube v4.0.

[16] Colombia. Ministerio de Salud. (1999). Resolución 1995 de 1999, julio 8 de 1999: Por la cual se establecen normas para el manejo de la historia clínica.

[17] de Bogotá, C. D. C. (2012). Ley 1581 de 2012.

[18] de España, G. (2011). Ministerio de Industria, Turismo y Comercio. (2011). INTECO-CERT RIESGOS Y AMENAZAS EN CLOUD COMPUTING Recuperado el, 10.

[19] Dunlap, S. y Beth, L. (2017) Healthcare cybersecurity is due for a checkup. New Hampshire Business Review. Recuperado de: http://www.nhbr.com/July-21-2017/Healthcare-cybersecurity-is-due-for-a-checkup/

[20] Díaz Cely, L. (2014). Problemas de seguridad de la computación en la nube (Bachelor's thesis, Universidad Piloto de Colombia).

[21] Eling, M. & Schnell, W. (2016) What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance. 17(5). 474-491. Doi: https://doi.org/10.1108/JRF-09-2016-0122

[22] Galmés, A. (2016). Sobre la Seguridad del almacenamiento en la nube. Máster interuniversitario de Seguridad de las Tecnologías de la Información y de las comunicaciones. Universitat Oberta de Catalunya.

[23] Gómez, Á. (2007). Enciclopedia de la seguridad informática. México

[24] Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2015). Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. IEEE Transactions on Cloud Computing, 5(3), 523-536.

[25] Guo, R., Li, X., & Zheng, D. (2017, June). Privacy-preserving medical information systems using multi-authority content-based encryption in cloud. In International Conference on Cloud Computing and Security (pp. 268-279). Springer, Cham.

[26] Gupta, B. B. (Ed.). (2018). Computer and cyber security: principles, algorithm, applications, and perspectives. CRC Press.

[27] Gutiérrez, I. S. R., Pérez, D. F. R., Suárez, V., & Prieto, J. D. (2018). Historias clínicas digitales desde la perspectiva colombiana: seguridad, calidad y gestión del dato. Revista Inventum, 13(24), 22

[28] Hendre, A., & Joshi, K. P. (2015, June). A semantic approach to cloud security and compliance. In 2015 IEEE 8th International Conference on Cloud Computing (pp. 1081-1084). IEEE.

[29] Hernández, L. F. (2016). Aspectos de seguridad informática en la utilización de cloud computing.

[30] Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación. Journal of Chemical Information and Modeling (Vol. 53). https://doi.org/10.1017/CBO9781107415324.004

[31] Himss, ``E-Health Reporter Latin America" Salud en la nube: Evolución hacia el nuevo paradigma en América Latina. Septiembre 2017. [Online]. http://ehealthreporter.com/wp-content/uploads/2017/09/Reporte-Salud-en-la-nube.pdf

[32] H. Journal, ``Summary of September 2017 healthcare data breaches," HIPAA J., Oct. 2017. [Online]. https://www.hipaajournal.com/september-2017-healthcare-data-breaches/

[33] Ing. Peña Ibarra, José Ángel, Cloud Computing, Conferencia Anual ISACA Monterrey 2011 pp 14 [online], Disponible desde Internet: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20111202%20Cloud%20Computing.pdf

[34] «ISACA» 2018. [En línea]. Available: https://cybersecurity.isaca.org/state-of-cybersecurity. [Último acceso: agosto 2018]

[35] «ISACA» (2015). Fundamentos de Ciberseguridad, USA.

[36] ISO 27000. (25 de noviembre de 2016). Sistema de gestión de la Seguridad de la Información. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

[37] ISO /IEC 17799. (15 de junio 2005). Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. Obtenido de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

[38] ISO/TR 20514:2005. Health informatics — Electronic health record — Definition, scope and context Obtenido de http://tc215.behdasht.gov.ir/uploads/244_514_ISO_TR_20514_2005(E).pdf

[39] Jerez, D. (2019). Historia clínica electrónica pasa su primera prueba en el senado. Bogotá, Colombia: RCN Radio. https://www.rcnradio.com/politica/historia-clinica-electronica-pasa-su-primera-prueba-en-el-senado

[40] Le, N. T., & Hoang, D. B. (2016, December). Can maturity models support cyber security?. In 2016 IEEE 35th international performance computing and communications conference (IPCCC) (pp. 1-7). IEEE.

[41] Ley No. 2015. El Ministerio de salud y Protección Social. Bogotá. Colombia. 31 de Enero 2020

[42] Ley No. 1273. El Ministerio del Interior y de Justicia. Bogotá. Colombia. 5 de Enero 2009.

[43] Ley No. 527. El Ministerio de Tecnologías de la Información y Comunicaciones. Bogotá. Colombia. Agosto 18 de 1999.

[44] Ley HIPAA - Health Insurance Portability and Accountability. Ley Pública 104 – 191, EEUU. 21 de Agosto 1996

[45] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. NIST special publication, 500(2011), 292.

[46] Manjusha, R., & Ramachandran, R. (2015). Secure authentication and access system for cloud computing auditing services using associated digital certificate. Indian Journal of Science and Technology, 8, 220.

[47] Martínez-Santander, C. J., & Cruz-Gavilánez, Y. D. L. N. (2018). Tendencias tecnológicas y desafíos de la seguridad informática. Polo del Conocimiento, 3(5), 260-279.

[48] Mavroeidakos, T., Michalas, A., & Vergados, D. D. (2016, April). Security architecture based on defense in depth for Cloud Computing environment. In 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 334-339). IEEE.

[49] Milicevic, D., & Goeken, M. (2011). Application of Models in Information Security Management. Research Challenges in Information Science (RCIS), 1-6.

[50] Microsoft Azure Fundamentas, AZ-900T01, 2019. https://docs.microsoft.com/es-es/learn/modules/welcome-to-azure/3-tour-of-azure-services

[51] Microsoft, 2019. HIPAA and the HITECH Act United States. https://docs.microsoft.com/es-es/microsoft-365/compliance/offering-hipaa-hitech

[52] Modi, R., (2019). Azure para arquitectos. Segunda Edición. Implementar diseño en el Cloud , DevOps, Contenedores, IoT y soluciones sin servidor en el Cloud público.

[53] Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud computing environment and security challenges: A review. International Journal of Advanced Computer Science and Applications, 8(10), 183-195.

[54] Narula, S., & Jain, A. (2015, February). Cloud computing security: Amazon web service. In 2015 Fifth International Conference on Advanced Computing & Communication Technologies (pp. 501-505). IEEE.

[55] Olivares, G. E. (2017). Modelo de amenazas, una ténica de análisis y gestión de riesgo asociados a softwares y aplicaciones (Bachelor's thesis, Universidad Piloto de Colombia).

[56] Ramio, J. (2006). Seguridad Informática y Criptografía., Versión 4.1 Libro Electrónico

[57] Rebollo Martínez, O. (2014). Marco para el Gobierno de la Seguridad de la Infornación en servicios Cloud Computing.

[58] Rizvi, S. Q. A., Wang, G., & Chen, J. (2018, December). A service oriented healthcare architecture (SOHA-CC) based on cloud computing. In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (pp. 84-97). Springer, Cham.

[59] Saharan, S., & Somani, G. (2015). Security of cloud-based storage. In Guide to Security Assurance for Cloud Computing (pp. 65-81). Springer, Cham.

[60] Salazar, M., & Verónica, C. (2013). Análisis de los riesgos técnicos y legales de la seguridad en Cloud Computing (Master's thesis, ESPAÑA/Escuela Técnica Superior de Ingenieros de Telecomunicaciones-Universidad Autónoma de Madrid/2013)

[61] Shengjian, L., Hayyan, Y., & Fengni. (2013). Design of network security early-warning system base on network defense in Depth model. IEEE, 355-359

[62] States, T.U., Cybersecurity policy, in National Security Presidential Directive 54/Homeland Security Presidential Directive 23. 2008.

[63]Tari, Z., Yi, X., Premarathne, U. S., Bertok, P., & Khalil, I. (2015). Security and privacy in cloud computing: vision, trends, and challenges. IEEE Cloud Computing, 2(2), 30-38.

[64] Vargas Barrios, P. J. (2018). Modelo de seguridad para plataformas colaborativas de e-ciencia sobre cloud computing.

[65] Yaping, J., Jianhua, Z., Yong, G., & Zengyu, C.(2009). A method of in Depth Defense for Network Security Base don Immunity Principles. IEEE.

[66] Velev, D., & Zlateva, P. (2011). Cloud infrastructure security. In Open Research Problems in Network Security (pp. 140-148). Springer, Berlin, Heidelberg.

[67] Zhu, S. Y., Hill, R., & Trovati, M. (Eds.). (2016). Guide to security assurance for cloud computing. Springer.

BIBLIOTECA CENTRAL DE LAS FF. MM.
"TOMAS RUEDA VARGAS"
201003850