UNIVERSIDAD NACIONAL DEL CALLAO

ESCUELA DE POSGRADO

UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

“ESTRATEGIA DE ADAPTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION UNIVERSITARIO A COMPUTACION EN LA NUBE”

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERIA DE SISTEMAS

MANUEL ABELARDO ALCANTARA RAMIREZ

CALLAO, 2019

PERU

UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

ESCUELA DE POSGRADO

MAESTRIA EN INGENIERIA DE SISTEMAS

RESOLUCION DEL COMITE DIRECTIVO Nº 026-2019-UPG-FIIS

JURADO EXAMINADOR

Mg. LOYO PEPE ZAPATA VILLAR	PRESIDENTE
Dra. ERIKA JUANA ZEVALLOS VERA	SECRETARIO
Mg. JOSE ANTONIO FARFAN AGUILAR	VOCAL

ASESOR: Mg. VICTOR EDGARDO ROCHA FERNANDEZ

Nº DE LIBRO DE ACTA DE SUSTENTACION 01-SPG-FIIS-UNAC-2012
FOLIO 23
Nº DE ACTA DE SUSTENTACION 002-2019-UPG-FIIS
FECHA DE APROBACION DE LA TESIS 01 DE MARZO DE 2019

DEDICATORIA

A: María Julia Ramírez de Alcántara,

Jacoba Sigüeñas Paredes,

Manuel Hipólito Alcántara García,

Por guiar siempre mí camino.

AGRADECIMIENTO

A Dios por haberme bendecido con su apoyo y a mis familiares que siempre me alentaron para lograr este objetivo.

ÍNDICE

LISTADO DE TABLAS

LISTADO DE FIGURAS

LISTADO DE ABREVIATURAS

CISA: Certified Information Systems Auditor

CISM: Certified Information Security Management

CISSP: Certified Information Systems Security Professional)

CMMI: Capability maturity model integration- Modelo integral de madurez y de capacidades

COBIT: Control Objectives for Information and related Technology

CSI: Comité de seguridad de la información

CSSLP: Certified Secure Software Lifecycle Profesional

IaaS: Infrastructure as a Service

IEC: International Electrotechnical Commission - La Comisión Electrotécnica Internacional

IFIP: International Federation for Information Processing – Federación Internacional de procesamiento de la información

ISACA: Information Systems Audit and Control Association - Asociación de Auditoría y Control de Sistemas de Información

ISC^{2}: International Information Systems Security Certification Consortium - El Consorcio internacional de Certificación de Seguridad de Sistemas de Información,

ISM3: Information Security Management Maturity Model.

ISO: International Organization for Standardization -Organismo internacional de normalización

ISSA: Information Systems Security Association

IT: Information Technology – Tecnologías de la información

ITIL: Technology Infrastructure Library - La Biblioteca de Infraestructura de Tecnologías de Información

PaaS; Platform as a Service

PHVA: Planificar-Hacer-Verificar-Actuar – Cilclo de Deming

SaaS: *S*oftware as a Service

SANS: SysAdmin Audit, Networking and Security Institute

SGSI: Sistema de gestión se la seguridad de la información

SI: Sistema de información

SSCP: Systems Security Certified Practitioner

GLOSARIO DE TÉRMINOS

Para guiar esta investigación, se considera pertinente considerar un glosario de términos que incluya las principales definiciones sobre seguridad de la información en la nube, presentadas en orden alfabético.

Activo: Se asigna un valor dentro la institución y compete resguardarlos, considérese entonces a los bienes, a los derechos tangibles y también intangibles que posee una institución. Algunos ejemplos de activos son: bienes inmuebles, inversiones, cuentas por cobrar, patentes, instalaciones, maquinarías, documentos, etc.

Administración de riesgos: Todas las actividades necesarias para identificar los riesgos, analizarlos y tomar medidas de protección para mitigarlos.

Amenaza: Todo lo relacionado con un incidente no deseado, que podría actuar sobre un activo y causarle daño.

Análisis de impacto: Constituye la evaluación del daño causado por la materialización de una amenaza.

Análisis de riesgo: Formado por todas las actividades que se realizan sistemáticamente con el objetivo de identificar fuentes de riesgo, estimar y valorar su impacto.

Ataques: Tipos y naturaleza de inestabilidad en la seguridad de la información causado por una amenaza

Control de riesgo: Tiene por objetivo la implementación apropiada del tratamiento de riesgos, en base al cumplimiento de las políticas, siguiendo los estándares y procedimientos establecidos.

Contra medidas: Cualquier acción o proceso que reduce la vulnerabilidad de los activos de información

Criticidad: Constituye el nivel de importancia que un recurso de información tiene para una institución

Evaluación de riesgo: Procesos que permiten identificar, cuantificar, documentar las amenazas, evaluar el nivel de exposición que tiene la institución debido a cada riesgo asumido. Constituye la base para definir las políticas.

Incidente de la seguridad de la información: Es un evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida, relevante para la seguridad, que tiene probabilidad significativa de comprometer procesos y amenazar la seguridad de la información.

Identificación de riesgo: Proceso mediante el cual se identifican las amenazas, las vulnerabilidades, las posibilidades de cristalización de las amenazas, el impacto sobre los activos de información asociados a los riesgos, teniendo en cuenta también la interdependencia entre estos elementos y los factores que influyen.

Impacto: Debe entenderse como los resultados y consecuencias de que se materialice una amenaza

Información: Es definida como cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida, almacenada, obtenida a partir de los datos de la organización y considerada como elemento esencial para el funcionamiento de las diferentes áreas organizacionales.

Gestión de Riesgos: Es un conjunto de procesos efectuados por la dirección, las jefaturas, el personal administrativo y docente de la institución, destinados a proveer una seguridad razonable sobre el logro de los objetivos de la institucionales. La gestión de riesgos está diseñada para contar con el entorno interno apropiado para desarrollar una adecuada determinación de objetivos, implementar una oportuna identificación, evaluación, tratamiento y control de riesgos, elaborar los reportes pertinentes y efectuar un adecuado monitoreo.

Monitoreo de riesgo: Consiste en implementar un conjunto de actividades con el objeto de percatarse del adecuado funcionamiento del sistema de gestión de riesgos usando reportes de deficiencias y acciones de corrección.

Normas: Establecer los límites permisibles de acciones y procesos para cumplir con las políticas

Objetivo de control: Es lo que se pretende obtener cuando se implementen los controles adecuadamente para proteger los activos.

Políticas: Declaración de alto nivel sobre la intención y la dirección de la gerencia

Proceso crítico: Es el proceso considerado indispensable para la continuidad de las actividades y servicios de la organización, y cuya falta o

ejecución deficiente puede tener impactos significativos (económico, académico, operacional o de imagen) para la institución.

Riesgo: Es la posibilidad de que ocurra un hecho realizado por una amenaza y que aprovechando una vulnerabilidad impacte de forma negativa en los objetivos de la institución.

Riesgos de operación: Es la posibilidad de pueda ocurrir pérdidas debido a las deficiencias en los procesos internos, en la tecnología de información, en las personas, ocasionado por eventos externos adversos.

Riesgo de tecnología de información: Son los riesgos de operación asociados a los sistemas informáticos y a la tecnología relacionada a dichos sistemas y que pueden afectar el normal desarrollo de las operaciones y servicios dentro de la institución.

Riesgo residual: El riesgo que permanece después de que se han implementado contra medidas y controles

Salvaguarda: Una salvaguarda o contramedida es cualquier actividad o ente que ayuda a detener las amenazas sobre los activos de información.

Seguridad de la información: Es una disciplina que contempla la protección y resguardo de los atributos de confidencialidad, integridad y disponibilidad de los activos de información. Para conseguir este objetivo se diseñan políticas, se establecen procedimientos, se diseña una estructura organizacional adecuada y se usa las herramientas apropiadas para tal fin.

Servicios críticos provistos por terceros: Son los servicios relacionados a procesos críticos provistos por otras personas o entidades externas a la

organización, cuya realización podría ser razonablemente desarrollada por la propia institución.

Tecnología de la información: Contempla las tecnologías, estrategias y actividades relacionados con los sistemas informáticos y trata además de las técnicas usadas en el tratamiento y la transmisión de la información como lo son la informática, Internet y las telecomunicaciones.

Tratamiento de riesgo: Está constituido por todas las actividades que permitan seleccionar e implementar las salvaguardas para controlar o mitigar el riesgo.

Vulnerabilidad: Es una falla, error, deficiencia u omisión asociado a un activo de información que puede ser aprovechado por una amenaza para causar daño.

-

RESUMEN

La seguridad de la información se ha visto en la imperiosa necesidad de contemplar el aspecto de la computación en la nube, la familia de normas ISO 27000 ha tenido que incrementarse con las normas ISO 27017, ISO 27018 para contemplar la seguridad en la nube, muchas organizaciones aún no consideran el uso de la computación en la nube por diversos motivos entre ellos por la falta de confianza en esta propuesta. El objetivo de este trabajo consiste en establecer una estrategia para que una universidad contemple la posibilidad de usar la computación en la nube; la propuesta se basa en el uso de las recomendaciones que hacen los estándares más usados en computación en la nube, como resultado se obtiene una serie de propuestas que incluye el análisis de la gestión de riesgos y la estrategia de migración de cierta información a la nube y otra no necesariamente y como trabajos futuros se propone analizar la optimización de la propuesta.

Palabras claves

Computación en la nube, ISO 27017, ISO 27018, Gestión de riesgos, Seguridad de la información

ABSTRACT

.

The security of information has been seen in the imperative need to contemplate the aspect of cloud computing, the family of ISO 27000 standards had gone through the ISO 27017, ISO 27018 standards to contemplate cloud security, many organizations They still do not consider the use of cloud computing for several reasons among them because of the lack of confidence in this proposal. The objective of this work is to establish a strategy for a university to consider the possibility of using cloud computing; the proposal is based on the use of the recommendations that make the most common standards in cloud computing, as a result we get a series of proposals that include the analysis of risk management and the migration strategy of information to the cloud and another unnecessary thing and as future work is compared with the optimization of the proposal.

Keywords

Cloud computing, ISO 27017, ISO 27018, Risk management, Information security

CAPITULO I: PLANTEAMIENTO DE LA INVESTIGACION

1.1 Identificación del problema

Actualmente la información se ha convertido en un elemento importante en las organizaciones, pero a pesar que los gerentes y la alta dirección tienen conocimiento de este hecho, no está internalizada aún, dentro de la cultura gerencial, la importancia de resguardarla. Es decir, no existe una *"cultura de la seguridad de la información"*. Es común observar que dentro de los presupuestos de las instituciones no están contemplados recursos para este rubro, evidenciando lo antes afirmado (Ambrust, 2010).

Por otro lado, los administradores que son conscientes de esta realidad, no tienen clara la estrategia para abordar el tema de manera sistemática y efectiva, suelen confundir la *"Seguridad de la información"* con *"Seguridad informática",* desvirtuando el concepto y abordando solo uno los aspectos que contempla un sistema de seguridad de la información.

La Información se caracteriza por tener propiedades que determinan su valor y están relacionados con la Confidencialidad, la Integridad y la Disponibilidad, son estos atributos los que se deben salvaguardar en todo Sistema de

Seguridad de Información. Alrededor de este enfoque se han diseñado diversos estándares tanto internacionales (la Norma ISO 27001) como nacionales (la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI) que establecen lo que debe contener todo Sistema de Seguridad de la Información a manera de marco general, sin especificar los detalles de su implementación, dejando a las organizaciones esta tarea (Ambrust, 2010).

En el Perú al respecto existe el marco legal que norma a través de la Resolución Ministerial Nº 187-2010-PCM de la Presidencia del Consejo de Ministros la obligatoriedad de implementar en cada institución pública un Sistema de Seguridad de la Información basado en la Norma Técnica Peruana antes mencionada. El alcance de esta resolución incluye naturalmente a las Universidades Nacionales como instituciones patrocinadas por el Estado Peruano.

Las universidades nacionales como particulares para su aspecto organizativo y funcional se rigen por la Ley Universitaria 30220 y son supervisadas por organizaciones como SUNEDU (Superintendencia Nacional de Educación Superior Universitaria) , la diferencia sustancial está en el patrocinador, mientras que las universidades nacionales son patrocinadas por el Ministerio de Educación, las universidades particulares son patrocinadas por promotores privados. Por tanto, desde el punto de vista organizativo y funcional, dos universidades públicas son más similares que dos universidades privadas o una privada y una nacional. Esta similitud permite pensar en un modelo similar para las universidades nacionales que permita ir desarrollando de

manera sistemática un sistema de gestión de la seguridad de la información.

Todo lo expuesto es para tener un sistema convencional de seguridad de la información, el problema se agudiza cuando se requiere tener el uso de la computación en la nube, pues el sistema convencional de seguridad de la información tendría que necesariamente adecuarse a las recomendaciones de los estándares de seguridad en la nube más usuales.

1.2 Formulación de problema

Identificado el problema anteriormente descrito, se planteó la necesidad de crear un modelo que permita implementar de manera concreta las buenas prácticas en seguridad de la información en la nube en una universidad nacional y de tal forma que se puedan desarrollar programas, proyectos y procedimientos que resguarden de manera segura la información. Para probar la validez del modelo se tomó como organización piloto la Universidad Nacional del Callao (UNAC).

De esta forma se remarca que el problema general y los problemas específicos se enuncian de la siguiente manera:

1.2.1 Problema general

¿Es posible crear una estrategia que permita la implementación exitosa de un sistema de gestión de seguridad de la información en la nube adecuado para una institución universitaria, basado en buenas prácticas informáticas?

1.2.2 Problemas específicos

1.2.2.1 Problema específico 1.

¿Cómo establecer los criterios para la migración adecuada de los procesos de gestión de una universidad a servicios prestados en la nube?.

1.2.2.2 Problema específico 2.

¿Cómo seleccionar el tipo de red y de servicio adecuado para la migración de procesos universitarios a la nube ?.

1.2.2.3 Problema específico 3.

¿Cómo implementar la arquitectura en la nube para soportar los procesos universitarios que se deciden migrar a la nube?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Crear un modelo para implementar y/o migrar a la nube un sistema de gestión de la seguridad de la Información para una universidad pública basándose en criterios propuestos por los estándares de seguridad de la información en la nube y contrastarlo en universidad Nacional del Callao.

1.3.2 Objetivos específicos

OE1. Establecer los criterios que se deben considerar para migrar los procesos universitarios a los servicios de computación en la nube.

OE2. Evaluar las propuestas de los modelos de redes en la nube así como los tipos de servicios ofrecidos por los proveedores de servicios en la nube.

OE3. Seleccionar propuestas para implementar la arquitectura en la nube que soporte la migración de procesos universitarios a redes y servicios en la nube.

1.4 Justificación

- Esta investigación es necesaria para contribuir con Modelos concretos a la implementación del Sistema de Seguridad de la Información en Universidades Públicas en la nube.
- Es necesario aumentar la cultura de la Seguridad de la Información y el uso de la nube en las organizaciones públicas y este trabajo contribuye a ello.
- La necesidad imperiosa de contar con un Sistema de Seguridad de Información implementado en la nube en la Universidad Nacional del Callao
- Contribuye a cumplir con la normatividad peruana respecto a la Seguridad de la Información y su implementación en la nube.

Este documento presenta el desarrollo del proyecto de tesis planteado y para su lectura adecuada se ha organizado en VIII capítulos y varios anexos

El capítulo I presenta a manera de introducción la identificación del problema que se ha estudiado, los objetivos de la investigación y la justificación de la misma., describe también el contenido del documento.

El Capítulo II contempla el marco teórico que sustenta la investigación, se comienza haciendo un estudio de los aspectos generales de la seguridad de la información, luego se ve la necesidad de resguardar la información frente a los desastres por pérdida de la

misma, se presenta las bases teóricas de la computación en la nube, estableciendo los tipos de servicios, los tipos de propiedad de las redes y los estándares de computación en la nube más usados

En el capítulo III se establece la estructura de la investigación, definiendo las variables de estudio, su operacionalización y la matriz de consistencia correspondiente se termina estableciendo las hipótesis de investigación

El capítulo IV aborda el tema de la metodología para llevar a cabo la investigación, se muestra las estrategias y secuencialidad de como se ha realizado la investigación

El Capítulo V, que es el más amplio, presenta los resultados de la investigación, se presenta en primer lugar el modelo de sistema de gestión de seguridad de la información en la nube para una universidad nacional (SGSI-UN-) como resultado de esta investigación y luego se presenta también el sistema SGSI-UNAC como prototipo de aplicación de este modelo.

En el Capítulo VI se presentan las discusiones de los resultados obtenidos a manera de crítica para avizorar futuras mejoras.

El Capítulo VII presenta las conclusiones que se logran formular después de haber realizado este trabajo de investigación.

El capítulo VIII se presenta las recomendaciones pertinentes para los lectores que puedan emprender futuras investigaciones en base a esta propuesta.

CAPÍTULO II. MARCO TEÓRICO

En este capítulo se presenta los fundamentos teóricos que sustentan la investigación, tales teorías son la seguridad de la información y la computación en la nube, se presenta también algunos antecedentes o estudios preliminares relacionados con la teoría

2.1 Antecedentes del estudio

Como un antecedente a nivel internacional se menciona por ejemplo el trabajo hecho por Rodas y Toscano (Rodas y Cruz, 2015) donde presenta un modelo referente en la gestión de servicios universitarios en la nube, haciendo un mapeo de procesos, subprocesos y actividades de una universidad, estableciéndose los sistemas de información que deberían ser automatizados y se estableció un portafolio con los servicios que prestan las universidades, los cuales se recomiendan deberían ser implantados en la nube. Tomando como base este documento generó un “Modelo para la adecuada gestión de los servicios relacionados con las tecnologías de información en la nube para las universidades de Ecuador.

Otro antecedente a nivel internacional es el atribuido a la empresa CISCO, (especialista redes de computadoras), la cual presenta un estudio donde se evidencia las ventajas que ofrece la

computación en la nube a las universidades, enfatizando el hecho de reducir costos en sus procesos, mediante la virtualización de su almacenamiento y procesamiento. Este estudio también muestra los posibles riesgos que acarrea la selección de servicios en una nube pública y recomienda considerar su implementación en nubes privadas y de esta manera conseguir un desarrollo rápido, escalable, a bajo costo y con el menor riesgo posible. CISCO vaticina una futura generalización del uso de la nube por parte de las instituciones universitarias, pero a su vez recomienda tener mesura al momento de seleccionar los procesos y servicios a migrar a la nube para tener riesgos mínimos.

No se registran antecedentes a nivel nacional sobre estrategias para migrar los procesos de una universidad a la nube desde el punto de vista de la seguridad de la información como una complementación de un Sistema de Gestión de Seguridad de la Información, según la búsqueda en los principales repositorios de CONCYTEC y de las principales universidades.

2.2 Seguridad de la información

La información constituye actualmente como uno de los activos más relevantes e imprescindibles en las empresas es por tal razón que se considera necesario establecer normas organizacionales, normas de tipo tecnológicas y aspectos legales o jurídicos para su protección (Chiregi y Navimipour, 2017), (Chowdhury, 2014).

La información en la universidad se encuentra en diversos formatos como por ejemplo en forma impresa, digital, transmitiéndose electrónicamente, en imágenes, en conversaciones o de otra manera no necesariamente física como puede ser la imagen institucional o la marca de la empresa. Esta

información es susceptible de ataques por parte de agentes internos como externos, pues existen múltiples amenazas asociadas a los activos y representan un obstáculo para la continuidad de la organización (Chiregi y Navimipour, 2017), (Chowdhury, 2014).

Toda información en propiedad o custodia de la universidad debe estar clasificada en términos de su valor, de sus requerimientos legales, de su grado de confidencialidad y criticidad para la organización.

Entiéndase por seguridad de la información un área del conocimiento que contempla la protección de los activos de información en las organizaciones, La protección es de las amenazas a las que están expuestas y de ser el caso se trata de minimizar el daño causado por los ataques. Trata los fundamentos y aspectos para la preservación de tres de los atributos de la información, a saber: la confidencialidad, la integridad y la disponibilidad que se pasará a estudiar en las siguientes líneas (Chiregi y Navimipour, 2017), (Chowdhury, 2014).

Confidencialidad: La información debe estar protegida de los accesos no autorizados independientemente del formato o almacenamiento que tenga. Los controles deben garantizar que la información podrá ser conocida y accedida únicamente previa autorización (Varghese y Buyya, 2017), (Vasuyadav y krishnareddy, 2017).

Integridad: La integridad consiste en garantizar que la información sea y permanezca confiable, completa y exacta, dado que la misma no ha sido alterada, borrada, o reorganizada. Su relevancia

radica en la necesidad de asegurar que la información refleja la realidad que la genera, ya que la tendencia hacia la automatización de los procesos conlleva a que en muchos procesos organizativos, la única evidencia de una transacción será la información que se haya generado de esta (Varghese y Buyya, 2017), (Vasuyadav y krishnareddy, 2017).

Disponibilidad: La disponibilidad abarca no solo a la información, sino a los procesos que sustenta su generación y uso; esto debe cumplir con las características de oportunidad, es decir, la recuperación de la información en el momento que se necesite, evitar la pérdida o bloqueo por algún acto inapropiado, no autorizado, mala operación accidental o causas fortuitas, para, de esta manera, garantizar su accesibilidad (Varghese y Buyya, 2017), (Vasuyadav y krishnareddy, 2017).

Seguridad Informática

La seguridad informática es el área de conocimiento que se encarga de establecer los procedimientos, herramientas y protocolos necesarios para garantizar el correcto, seguro y continuo funcionamiento de los diferentes elementos que componen un sistema o red informática. El campo de la seguridad informática se puede dividir en varias áreas diferenciadas: (Veeramachaneni, 2015), (View y Heng, 2014).

Seguridad de Sistemas Operativos: Se refiere a la seguridad intrínseca del propio sistema operativo empleado como Windows o linux.

Seguridad de Aplicaciones o Servicios: Se refieren a los programas empleados tanto para acceder a los servidores Web, gestores de correo electrónico, gestores de base de datos, etc.

Seguridad de Redes: Se refiere a la seguridad de los datos transmitidos de un computador a otro, así como de la seguridad de todos los dispositivos que conforman la red.

Seguridad de Datos: Comprende las normas necesarias para una adecuada protección de los datos de un sistema.

Seguridad de Física: Se refiere a los aspectos de seguridad de ambientes, relacionados con la seguridad informática.

Tratamiento de la confidencialidad

En el tratamiento de la confidencialidad se suele usar dos tipos de tratamientos, el tratamiento general y el tratamiento específico40 (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Tratamiento general de la confidencialidad:

Para el tratamiento general de la confidencialidad, la información se puede clasificar como información pública, información interna, información restringida, información confidencial, información secreta.

Información pública: La información se clasifica como pública cuando no requiere de protección especial y existe el deseo expreso de su publicación por parte de la universidad, también debido a la exigencia de su publicación por parte de la normativa legal vigente, la divulgación de esta información no implica ningún tipo de riesgo para la universidad. La información clasificada

pública será accesible por personal de la universidad o personas ajenas a la universidad como por ejemplo lo que se publica en el portal de transparencia institucional (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Información interna: Información necesaria para el correcto desempeño de las funciones del personal administrativo y docente de la universidad; cuya divulgación, intencionada o accidental, puede suponer problemas leves a la organización, no deteriorará significativamente la imagen institucional, ni atentará contra los derechos de las personas. La información clasificada interna será accesible por el personal de la universidad o personal ligado a esta, de manera contractual, esta información no deberá transmitirse ni comunicarse a nadie fuera de los mencionados en este párrafo, sin la autorización respectiva de las autoridades universitarias. Información de este tipo es por ejemplo el cronograma de pagos (Wei et al, 2014), (Yogamangalam y Shankar, 2013)..

Información restringida: Información de uso interno exclusivo de grupos de usuarios o áreas específicas que no debe transmitirse libremente dentro de la universidad. La información clasificada restringida será accesible únicamente por un grupo limitado de personas que necesita dicha información para el desempeño de sus actividades laborales. Son ejemplos de este tipo la configuración de servidores, el mapeo IP, teléfonos de docentes (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Información confidencial: Información cuya divulgación, alteración o pérdida puede suponer un problema grave para la organización, un deterioro significativo de su imagen pública, atentar directamente contra el derecho a la intimidad de las

personas o puede afectar significativamente a su posición en el mercado o el incumplimiento de la normativa vigente. No se transmitirá o divulgará a terceras personas, con excepción de que exista autorización explícita y por escrito de las autoridades universitarias por ejemplo citaciones judiciales (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Información secreta: Información que debe ser conocida únicamente por el propietario de la misma, tales como: contraseñas de usuario, claves criptográficas, etc. (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Tratamiento específico de información confidencial:

Datos Personales: Los datos personales del personal docente, administrativo y alumnos de la universidad, a los que se tenga acceso por motivos profesionales deberán ser tratados siempre de manera confidencial y siguiendo en todo caso los procedimientos establecidos para dicho tipo de datos según la legislación vigente; no se transmitirán o divulgarán a terceras partes si no nos consta que existe autorización de la universidad (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Datos secretos: Los datos que permitan accesos u operaciones en la Oficina de Informática y Estadística tales como las claves criptográficas ,claves criptográficas asociadas a aplicaciones, claves o contraseñas de acceso u operación, se consideran secretos . No se deben divulgar los propios ni solicitar los ajenos. Excepcionalmente, y bajo los procedimientos de seguridad y registro establecidos, el personal de soporte técnico puede establecer claves iníciales o de desbloqueo que

deberán ser cambiadas por el titular en el primer acceso (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Archivos temporales: Los usuarios que por motivos de trabajo y de acuerdo con los procedimientos establecidos, organizativamente, necesiten trabajar en archivos temporales con datos personales o sujetos a confidencialidad, deberán proceder al borrado de los mismos una vez finalizado el tratamiento de los mismos y consolidados los resultados finales obtenidos (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Tratamiento de la integridad

Clasificación general: La información se clasificará por sus requerimientos de mantenimiento de integridad en función del impacto que su modificación no autorizada pueda dañar a la universidad. Siguiendo criterios similares a los establecidos para riesgo operacional, los riesgos derivados de la no integridad pueden ser legales/regulatorios y de referencia a la buena imagen organizacional (Zaghloul et al, 2018) , (Zissis y Lekkas, 2012).

Se analizarán los posibles riesgos derivados de la manipulación o alteración de la información procesada por los sistemas de información atendiendo a las pérdidas directas, indirectas (debidas a los procesos de cuadre y conciliación), regulatorias y de imagen organizacional (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Información de operaciones del área de economía: La información sobre operaciones del área económica cuya alteración suponga una pérdida patrimonial cierta y no recuperable

mediante procesos posteriores de cuadre o conciliación deberá estar especialmente protegida.

Para las posibles pérdidas recuperables mediante procesos de conciliación se evaluará la conveniencia de establecer el mismo tipo de controles. La modificación de la información almacenada que soporte operaciones financieras se efectuará siempre a través de aplicaciones que garanticen que siempre existe la contrapartida correspondiente, cualquier otro tipo de acceso extraordinario para cuadres manuales deberá estar restringido y estrictamente auditado (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Las comunicaciones de información cuya modificación en tránsito estén sujetas al tipo de riesgo antedicho deberán estar protegidas mediante mecanismos de control de integridad (mediante claves de acceso). Si la comunicación es con terceros los mecanismos de integridad deberán incluir adicionalmente la posibilidad de no repudio (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Información para la elaboración de reportes económicos: La información para la elaboración y consolidación de los reportes económicos de la universidad, estará sometida a procesos rigurosos para el control de su integridad, a fin de dar adecuado cumplimiento a las regulaciones y al compromiso de la organización de ofrecer información veraz a los entes superiores en general que están registrados en su sistema de Gobierno (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Información expuesta a redes públicas: La información accesible directamente por terceros a través de la Internet (Web institucional) deberá estar especialmente protegida contra su

alteración no autorizada mediante la aplicación de las Normas de Seguridad perimetral, segmentación de redes, sistemas software de seguridad, sistemas operativos, controles de acceso, análisis periódico de vulnerabilidades, detección de intrusión y aquellas específicas de control de integridad de contenidos públicos (Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Credenciales y perfiles de acceso: Por su capacidad de dar o modificar privilegios de acceso, se protegerán especialmente la integridad de las credenciales (incluso en su almacenamiento cifrado) y de los perfiles asignados a los usuarios de los Sistemas de Información. El acceso a las bases de datos de autenticación y autorización de usuarios estará estrictamente limitado al personal de la Oficina de Informática y Estadística, los accesos a cualquier sistema de la universidad siempre serán auditados(Wei et al, 2014), (Yogamangalam y Shankar, 2013).

Tratamiento de la disponibilidad

La clasificación de los activos de información, de los procesos y sistemas que los soportan, en cuanto a su disponibilidad frente a contingencias y las correspondientes medidas a adoptar se desarrollarán, de acuerdo al nivel crítico asignado por las diferente área de la universidad a los mismos, en el marco de los planes de recuperación de sistemas (Muthakshi y Meyyappan, 2013), (Pallis, 2010) y (Radu, 2017).

Evaluación de Riesgos

La evaluación de riesgos identifica, cuantifica y documenta las amenazas a la seguridad de la institución, evalúa el nivel de

exposición en el que queda la universidad por cada riesgo asumido y determina el grado de importancia para la eliminación de cada uno de ellos. La evaluación del riesgo provee la base para desarrollar políticas de seguridad (Muthakshi y Meyyappan, 2013), (Pallis, 2010) y (Radu, 2017).

Es necesario realizar un análisis formal para identificar los riesgos específicos asociados con los activos críticos de información. El resultado más importante del proceso de evaluación de riesgo, es la información que se utiliza para desarrollar e implantar las políticas de seguridad.

Se debe identificar en cada unidad organizacional de la UNAC con una frecuencia anual para asegurar tanto la integridad como la disponibilidad y confidencialidad de la información.

Política de Seguridad

Las políticas de seguridad informática surgen como una herramienta organizacional para sensibilizar a la comunidad de la UNAC sobre la importancia de la información y servicios críticos que permiten a la universidad crecer y mantenerse competitiva (Muthakshi y Meyyappan, 2013), (Pallis, 2010) y (Radu, 2017).

Todo el personal de la universidad debe seguir las políticas y estándares de seguridad para controlar y proteger la Información, esto también alcanza a empleados no regulares tales como temporales, contratistas, vendedores y consultores. Este estándar se refiere a toda la información sin tomar en cuenta la forma ni formato.

Selección de Controles

Una vez identificados los requerimientos de seguridad, se debe implementar los controles para garantizar que los riesgos sean reducidos a un nivel aceptable Muthakshi y Meyyappan, 2013), (Pallis, 2010) y (Radu, 2017).

Los controles se seleccionarán sobre la base de este documento o según nuevos controles que se pueden diseñar para satisfacer necesidades específicas según corresponda.

Los controles serán seleccionados teniendo en cuenta el costo de implementación en relación con los riesgos a reducir y las pérdidas que podrían producirse de tener lugar una violación de la seguridad.

También se tendrá en cuenta los factores no monetarios, como el daño en la reputación institucional (Muthakshi y Meyyappan, 2013), (Pallis, 2010) y (Radu, 2017).

2.3 Computación en la nube

La Computación en la nube (*Cloud Computing*) se refiere a un paradigma que contempla un conjunto de tecnologías de computación que están configurando un nuevo orden mundial en las Tecnologías de la Información (TI). La idea principal de este paradigma consiste en que las TI se convierten en un servicio, de modo que, por ejemplo “las aplicaciones del software no tienen por qué existir en un lugar concreto, sino que pueden estar compuestos de múltiples piezas procedentes de múltiples sitios” (Joyanes, 2009), (Adamuthe et al, 2015) y (Anjali y Pandey, 2013).

Como afirma Joyanes (Joyanes, 2009), la idea clave es que los usuarios, las empresas, las grandes corporaciones acceden a los servicios de TI a través de una red de computadoras que se denomina “nube” (*cloud*, una red pública generalmente Internet o una red Intranet); los clientes pueden acceder bajo demanda –siguiendo el modelo “gratuito” o de “pago” por uso- a un gran número de recursos informáticos de modo dinámico, dotándose así de una enorme capacidad de procesamiento y almacenamiento sin necesidad de instalar máquinas localmente, lo que se traduce en considerables ahorros de tiempo e incluso de consumo energético.

Como se mencionó anteriormente, la nube está formada por computadoras virtualizadas e interconectadas que usan sistemas paralelos y distribuidos para dinámicamente provisionar recursos informáticos en función de algunos acuerdos de nivel de servicio que se establecen entre los clientes y el proveedor de servicios.
La Computación en la nube como toda tecnología emergente ofrece sus ventajas y desventajas, dentro de las ventajas se menciona a los grandes recursos de computación, el bajo costo, los controles de seguridad, elasticidad rápida, alta escalabilidad y servicios tolerantes a fallas con alto rendimiento (Joyanes, 2009), (Adamuthe et al, 2015) y (Anjali y Pandey, 2013).

Dentro de las desventajas de usar computación en la nube se tiene por ejemplo la seguridad con respecto a la privacidad, el cumplimiento, los asuntos legales, la seguridad en el host, red, niveles de datos, las vulnerabilidades de virtualización y accesibilidad, la administración de identidades y credenciales, la confidencialidad, la autenticación del dispositivo demandado y la

integridad (Joyanes, 2009), (Adamuthe et al, 2015) y (Anjali y Pandey, 2013).

A pesar de tener plena conciencia de la existencia de las ventajas y desventajas de esta tecnología, los proveedores de servicios en la nube cada vez se esfuerzan por mejorar sus procesos de seguridad y cumplimiento normativo, esto explica la madurez del mercado y el crecimiento constante (Joyanes, 2009), (Adamuthe et al, 2015) y (Anjali y Pandey, 2013).
Básicamente, la computación en la nube funciona gracias a la tecnología de virtualización, donde el host ejecuta una aplicación denominada hipervisor, la cual genera Máquinas Virtuales (VM) que simulan las computadoras físicas que son capaces de operar cualquier software desde el sistema operativo hasta la aplicación del usuario final. Respecto al
hardware utilizado, se dispone de discos duros, procesadores y dispositivos de red que se colocan en los centros de datos (Joyanes, 2009), (Adamuthe et al, 2015) y (Anjali y Pandey, 2013).

La gestión de los recursos que se usan en la computación en la nube se hace a través de capas, la capa virtualización, la capa de software y la capa de gestión. La capa de virtualización contempla la elasticidad, la acción rápida, agrupación de recursos y ubicación independiente. La capa de gestión se encarga de la seguridad y monitoreo en toda la nube (Joyanes, 2009), (Adamuthe et al, 2015) y (Anjali y Pandey, 2013).

2.4 Modelos de implementación en la nube

Existen cuatro modelos para poder implementar computación en la nube: nube pública, nube privada, nube comunitaria y nube híbrida. Estos modelos representan la forma como se usa la infraestructura informática ai brindar los servicios en la nube (Adriano y Lucrédio, 2012), (Cloud-customer-standars, 2017)

2.4.1 Nube pública

Este modelo de implementación sostiene que los recursos de computación en la nube son provistos por un proveedor externo a través de la Web. Los datos y las aplicaciones de los usuarios están ubicados en una misma infraestructura física asignada y administrada por el proveedor, pero con una asignación individual separada. Es decir, varios usuarios comparten la misma infraestructura de la nube (View,2014), (Jara, 2012), (Kalpana, 2015), (Saggi y Bhatia, 2015) y (Shawish y Salama, 2014).

2.4.2 Nube privada:

Participar de este modelo de implementación en la nube implica que los recursos para computación en la nube se proporcionan por un proveedor externo, pero se personalizan según los requisitos del usuario y son de su uso exclusivo. La infraestructura es administrada y mantenida por el proveedor que comprende a varios clientes (View,2014), (Jara, 2012), (Kalpana, 2015), (Saggi y Bhatia, 2015) y (Shawish y Salama, 2014).

Los costos de usar este modelo de implementación son significativamente más altos debido a que se requiere experiencia y capacitación para la administración del servidor, experiencia en virtualización y especialización

en redes, experiencia en el manejo de las aplicaciones virtuales y los recursos escalables proporcionados por el proveedor, los cuales se agrupan y están disponibles para que los clientes los usen (View,2014), (Jara, 2012), (Kalpana, 2015), (Saggi y Bhatia, 2015) y (Shawish y Salama, 2014).

En el modelo de nube privada las relaciones contractuales entre el proveedor y el cliente son más fáciles abordar porque la infraestructura opera y es propiedad de la misma organización y usa las capacidades del software de gestión de la nube a fin de garantizar un servicio de entrega confiable cuidando la integridad de los recursos externos (View,2014), (Jara, 2012), (Kalpana, 2015), (Saggi y Bhatia, 2015) y (Shawish y Salama, 2014).

2.4.3 Nube híbrida:

Este modelo de implementación en la nube combina las ventajas de la nube publica con las ventajas de la nube privada, existiendo por tanto una gran variedad de propuestas de este tipo (View,2014), (Jara, 2012), (Kalpana, 2015), (Saggi y Bhatia, 2015) y (Shawish y Salama, 2014).

La importancia de la nube híbrida radica en que generalmente el proveedor ofrece recursos adicionales según la demanda del cliente como por ejemplo poder migrar algunos trabajos de la nube privada a la pública. La nube híbrida se perfila como un modelo dominante

debido a que tiene la capacidad del ahorro de costos, la escalabilidad, la elasticidad, la flexibilidad del control de la nube publica cuando se necesita (View,2014), (Jara, 2012), (Kalpana, 2015), (Saggi y Bhatia, 2015) y (Shawish y Salama, 2014).

2.4.4 Nube comunitaria:

El modelo de nube comunitaria propone que la infraestructura de la nube es compartida y propiedad de diferentes organizaciones, como grupos de investigación, grupo de empresas y organizaciones gubernamentales, las cuales comparten entre sus clientes que tienen intereses o inquietudes similares (View,2014), (Jara, 2012), (Kalpana, 2015), (Saggi y Bhatia, 2015) y (Shawish y Salama, 2014).

2.5 Tipos de servicios en la nube

Los servicios que ofrecen por los proveedores en la nube tienen que ver con el acceso a los recursos informáticos que son resultan ser configurables, dinámicamente escalables, virtualizados y bajo demanda como, por ejemplo, aplicaciones, almacenamiento, servidores, redes, etc. Se detallan a continuación estos tipos de servicios (Hepsiba y Sathiaseelan, 2016), (Kalpana, 2015) y (Shojaiemehr, 2010).

2.5.1 Infraestructura como servicio (IaaS).

Este tipo de servicio en la nube se caracteriza porque el proveedor proporciona una infraestructura informática básica al cliente. Consiste en proveer hardware como servidores, almacenamiento, procesador, centro de datos, red y varios otros recursos de infraestructura para que el usuario puede ejecutar e implementar su software. IaaS proporciona servicios de almacenamiento, servicios en la web, alojamiento de servidor, máquina virtual, copia de seguridad, estrategia de recuperación. Sus recursos son escalables y proporcionados bajo demanda, se recomienda para cargas de trabajos experimentales, trabajos temporales o cambios inesperados de procesamiento (View,2014), (Devi y Ganesan, 2015), (Kalpana, 2015), (Shojaiemehr, 2010).

Este tipo de servicio permite minimizar los costos iniciales de adquirir hardware como dispositivos de red, servidores y a cambio posibilita mejorar la capacidad de procesamiento en las organizaciones permitiéndoles enfocarse en sus objetivos y competencias centrales en lugar de preocuparse por la administración y aprovisionamiento de la infraestructura informática o centros de datos propios (View,2014), (Devi y Ganesan, 2015), (Kalpana, 2015), (Shojaiemehr, 2010).

Otros servicios ofrecidos por IaaS lo conforman por ejemplo la virtualización del escritorio, el escalamiento dinámico, la automatización de tareas administrativas, los servicios basados en políticas, etc. (View,2014), (Devi y Ganesan, 2015), (Kalpana, 2015), (Shojaiemehr, 2010).

El cliente tiene control sobre las aplicaciones implementadas, sobre el almacenamiento, control del sistema operativo y la posibilidad de seleccionar componentes de red como el servidor de seguridad en lugar de controlar o administrar la infraestructura de la nube. (View,2014), (Devi y Ganesan, 2015), (Kalpana, 2015), (Shojaiemehr, 2010).

2.5.2 Plataforma como servicio (PaaS):

Este tipo de servicio se caracteriza porque el cliente solo tiene acceso para controlar las aplicaciones desplegadas por el proveedor y poder configurar posibles entornos de alojamiento en lugar de controlar los servidores, el almacenamiento, la red y el sistema operativo. Los servicios de infraestructura son de nivel más alto para el usuario permitiéndole configurar aplicaciones diferenciadas de acuerdo a sus requerimientos tanto en tiempo de ejecución como en un entorno de desarrollo integrado. (View,2014), (Devi y Ganesan, 2015), (Kalpana, 2015), (Shojaiemehr, 2010).

PaaS incluye gestores de bases de datos, servicios de directorio, inteligencia comercial, herramientas de pruebas y herramientas de desarrollo. La máquina virtual se emplea para actuar como catalizador y se requiere proteger contra los ataques de malware en la nube (View,2014), (Devi y Ganesan, 2015), (Kalpana, 2015), (Shojaiemehr, 2010).

La seguridad en este tipo de servicio puede verse comprometida durante el despliegue de la aplicación del usuario o durante el tiempo de ejecución de la aplicación y por tanto se requiere cuidar la seguridad de la infraestructura subyacente, cuidar el desarrollo del ciclo de vida y la relación con terceros, se hace necesario entonces incluir las autenticaciones durante la transferencia de datos a través de los canales de red en general con el objetivo de mantener la integridad de las aplicaciones (View,2014), (Devi y Ganesan, 2015), (Kalpana, 2015), (Shojaiemehr, 2010).

2.5.3 Software como servicio (SaaS):

En el tipo de servicio SaaS se dispone de una colección de aplicaciones alojadas de forma remota por el proveedor de servicios en la nube y que los pone a disposición de los clientes que lo soliciten. En consecuencia, los usuarios ahorran los costos de las licencias de hardware y software y el mantenimiento de la infraestructura. Incluye escritorio virtual, correo electrónico, automatización de oficinas, aplicaciones comerciales, gestión de documentos y contenido. SaaS ofrece software comercial a usuarios empresariales a costo bajo frente a la posibilidad de desarrollar software o aplicaciones propias (View,2014), (Devi y Ganesan, 2015), (Kalpana, 2015), (Shojaiemehr, 2010).

Algunas ventajas del servicio SaaS son, por ejemplo: administración más fácil, accesibilidad universal, fácil

colaboración, compatibilidad de software, administración de actualizaciones lo que permite a las empresas obtener servicios tal como si fuera con un software con licencia comercial, la principal desventaja es que los clientes no se sienten seguros debido a la deficiencia en la visibilidad con respecto a sus datos almacenados (View,2014), (Devi y Ganesan, 2015), (Kalpana, 2015), (Shojaiemehr, 2010).

2.6 Terminología de la computación en la nube

La computación en la nube se implementa con los componentes básicos de hardware y software y consisten en una amplia gama de equipos y de servicios que se pueden utilizar en Internet. En este estudio, algunos componentes servicios y terminología importantes se describen de la siguiente manera: (Devi y Ganesan, 2015), (Shojaiemehr, 2010).

2.6.1 Hipervisor

El hipervisor es el software que logra virtualizar el hardware de forma tal que permite ejecutar y crear múltiples máquinas virtuales en un único host de hardware, monitorea y administra los sistemas operativos como por ejemplo windows, linux y Mac OS que pueden compartir recursos virtualizados de hardware y que pueden ejecutarse en el único sistema físico (Munyaka et al, 2012), (Shojaiemehr, 2010), (Wei et al, 2014).

2.6.2 Virtualización

la virtualización es la tecnología que permite compartir los recursos físicos por varios clientes. Logra crear un recurso físico que resulte igual que los recursos virtuales múltiples para los clientes. Se usa para consolidar los recursos de red, almacenamiento, procesador y sistema operativo en un entorno virtual (Munyaka et al, 2012), (Shojaiemehr, 2010), (Wei et al, 2014).

2.6.3 Almacenamiento en la nube

Mediante el almacenamiento en la nube, los clientes realizan copias de seguridad que lo almacenan y gestionan de forma remota, el proveedor se preocupa de la autenticación y el cifrado de tal forma que los datos estén seguros y disponibles. El almacenamiento en la nube depende del modelo nube y tipo de servicio utilizado, el almacenamiento en la nube pública ofrece un entorno de almacenamiento multiusuario que es apropiado para los datos no estructurados, el servicio en la nube privada ofrece un entorno de almacenamiento dedicado que está protegido detrás del firewall de los clientes, en una nube híbrida proporciona más opciones de implementación de datos y flexibilidad comercial porque combina los servicios en la nube privada y pública (Comput et al, 2015), (Shojaiemehr, 2010), (Zaghloul et al, 2018).

2.6.4 Multitenancy

Esta tecnología se caracteriza porque una sola instancia de software de aplicación puede servir a múltiples usuarios o clientes, a los clientes solo se les permite compartir aplicaciones o recursos, pero no pueden observar o compartir datos entre ellos dentro del entorno de ejecución.

Cada cliente es considerado como un inquilino con ciertas atribuciones y restricciones puede por ejemplo personalizar la aplicación hasta cierto punto, pero está restringido de personalizar el código de las aplicaciones.

En el servicio SaaS el proveedor puede ejecutar una parte de la aplicación con la base de datos correspondiente y ofrecer acceso o servicio web a varios inquilinos, la misma base de datos almacena datos de varios clientes sin la posibilidad de fuga de datos entre ellos. Es obligación del proveedor garantizar la seguridad de los datos, garantizando la utilización óptima del almacenamiento de datos y el mecanismo de hardware (Mushtaq et al, 2017), (Shojaiemehr, 2010), (Zaghloul et al, 2018).

2.6.5 Red en la nube:

Para implementar la red en la nube se necesita una conexión a Internet a manera de red privada virtual que permite al cliente acceder de forma segura a los recursos como archivos, aplicaciones, impresoras, etc. La tecnología que se usa es la de redes definidas por software. La red en la nube se utiliza en el acceso a los recursos desde el proveedor de servicios, los recursos de

red se pueden compartir entre los clientes, es necesario contar con una infraestructura de red segura para poder administrar y construir eficientemente el almacenamiento en la nube (Munyaka et al, 2012), (Shojaiemehr, 2010), (Wei et al, 2014).

2.7 Seguridad en la nube

Constituida por un conjunto de políticas diseñadas para implementar la protección de aplicaciones, datos e infraestructura asociados con la nube, algunas vulnerabilidades son por ejemplo que los proveedores de la nube, los empleados y sus contratistas pueden revelar deliberadamente el almacén de datos en la nube, los datos basados en la nube pueden estar incorrectamente modificados y vulnerable a eliminar (perdido accidentalmente) por el proveedor del servicio, En la red pública, posiblemente se pueda acceder a los datos a través de API y protocolos inseguros (Furth y Escalante, 2010), (Zaghloul et al, 2018).

2.7.1 Seguridad de almacenamiento en la nube:

El almacenamiento en la nube contiene riesgos inherentes al usar aplicaciones de intercambio de archivos y almacenamiento en la nube. Los clientes almacenan sus datos en la nube y un tercero los transferirá, lo que significa que la configuración de privacidad de los datos está fuera del control del proveedor de servicios o de los clientes. Las principales preocupaciones de seguridad sobre el almacenamiento en la nube son la fuga de datos, el posible espionaje, las

gestiones de credenciales de la nube y la adecuada administración de claves (Malik et al, 2014), (Yogamangalam y Shankar, 2013).

2.7.2 Seguridad de la infraestructura en la nube

La seguridad en la nube requiere que se opere la infraestructura en la nube con total garantía y que permita la verificación de la implementación segura de los servicios, del almacenamiento de datos, de las comunicaciones y operación segura de la administración. Se recomienda organizar la seguridad de la infraestructura por capas según los niveles de aplicación, host y red (Malik et al, 2014), (Yogamangalam y Shankar, 2013).

2.7.3 Seguridad del software:

Es de entera responsabilidad del proveedor de servicios en la nube la protección de las aplicaciones o software que brinda tanto en los aspectos internos como externos durante todo el ciclo de vida del desarrollo del software. Es común implementar errores, fallas de diseño, desbordamiento de búfer, acuerdos de manejo de errores, para detectar las fallas del software (Malik et al, 2014), (Yogamangalam y Shankar, 2013).

2.7.4 Seguridad de red en la nube:

El control de la seguridad de la red en la nube es por parte del proveedor, solo debe permitir el tráfico de red válido y

bloquear todo el tráfico malicioso, no se comparten la infraestructura de red interna, como por ejemplo los enrutadores y los conmutadores de acceso que se usan para permitir conectar las máquinas virtuales de los clientes. La seguridad de la red en la nube presenta problemas de ataques internos y externos debido a que el atacante puede autorizar legalmente desde otra parte de la red y el ataque puede ocurrir ya sea en una red física como en una red virtual (Fernández, 2012), (Yogamangalam y Shankar, 2013).

2.8 Desafíos de seguridad en la computación en la nube

El principal desafío de la computación en la nube es la confianza en la tecnología, se refiere a que los clientes aseguran las capacidades del proveedor que les proporciona los servicios requeridos de manera confiable y precisa. Cuando se implementa una nube pública, la confianza recae en el proveedor de la infraestructura. Cuando la nube es privada la confianza se mantiene dentro de la organización (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

La seguridad en la nube implica identificar las amenazas que deben abordarse para implementar las contramedidas adecuadas, se hace necesario la evaluación del riesgo en áreas tales como integridad, confidencialidad, privacidad, auditoría, confiabilidad y disponibilidad (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

Otro aspecto importante es la criptografía que se debe utilizar para garantizar la autenticidad, la confidencialidad y la integridad

de los datos al tratar de abordar las vulnerabilidades de seguridad específicas (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

2.8.1 Integridad en la nube

El atributo de integridad de la información en la nube se refiere a que se debe preservar los datos que se almacenan en el servidor para verificar que los datos no se modifiquen o pierdan al emplear los servicios de la nube (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

Generalmente la integridad de la información involucra al proveedor, al propietario de los datos y a un auditor que garantice la integridad de los datos, el auditor puede ser el propietario de los datos o puede asignar la responsabilidad a un tercero (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

Una forma de garantizar la integridad de los datos es hacer un pre procesamiento que genere metadatos adicionales para que después que se externalizan los datos y metadatos se pueda usar para verificar la integridad. Esto permitirá la identificación oportuna de cualquier eliminación o corrupción de datos y permitirá la toma las medidas necesarias para la recuperación de datos (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

Se debe cuidar no degradar la eficiencia de cálculo debido al uso de metadatos, evitando sobrecarga cuando se trata de grandes volúmenes de datos, de igual manera cuidar la eficiencia de la comunicación, el uso adecuado de los discos (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

Según los tipos de servicio en la nube IaaS, PaaS y SaaS, es fundamental las políticas para mantener la integridad de los datos. El almacenamiento de datos en la nube requiere de discos de estado sólido debido a que aumentan su capacidad pero se puede tener como consecuencia la alta posibilidad de corrupción de datos, pérdida de datos, falla del disco o falla del nodo y además puede no ser mucho más rápida en términos de acceso a datos (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

2.8.2 Confidencialidad en la nube

La confidencialidad se refiere a mantener los datos del cliente en secreto en el sistema de computación en la nube y solo los clientes o sistemas autorizados pueden acceder a los datos (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

Por lo tanto, es el requisito fundamental para mantener los datos del cliente en secreto cada vez más el número de aplicaciones, clientes y dispositivos involucrados (Mushtaq

et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

Los proveedores de computación en la nube han adoptado ampliamente los dos enfoques básicos, como la criptografía y el aislamiento físico para lograr la confidencialidad (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

La computación en la nube proporciona servicios y datos que se transmiten a través de la red pública y no puede lograr el aislamiento físico. Si bien la LAN virtual y la red de cajas intermedias, como filtros de paquetes y firewall, deben implementarse para lograr el aislamiento físico virtual (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

La confidencialidad también se mejora mediante la encriptación de los datos antes de la transferencia al almacenamiento en la nube

1) Alquiler múltiple (Multitenancy) Hace referencia a las características de los recursos en la nube que se comparten, incluidos los datos, la memoria, las redes y los programas. La computación en la nube es como el modelo comercial en el que los múltiples clientes pueden acceder a los mismos recursos compartidos a nivel de aplicación, nivel de host y nivel de red. Multitenancy es similar a la multitarea que comparte algunos recursos de procesamiento comunes como la CPU y presenta varias amenazas de confidencialidad y privacidad (Mushtaq et al,

2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

2) Remanencia de datos: los datos se representan en residuales que pueden eliminarse o borrarse involuntariamente debido a la falta de separación de hardware entre diferentes clientes y la separación virtual de las unidades lógicas en una sola infraestructura de nube, puede llevar a revelar involuntariamente los datos privados (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

3) Seguridad y privacidad de la aplicación: la confidencialidad de los datos está asociada a la autenticación del usuario. Proteger la cuenta del cliente de los piratas informáticos es un gran problema para controlar el acceso de los objetos, incluidos el software, los dispositivos y la memoria (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

2.8.3 Disponibilidad en la nube

El atributo de la disponibilidad de la información en la nube está relacionado con garantizar que los clientes autorizados puedan acceder a las aplicaciones y a la infraestructura de los servicios en la nube en cualquier momento bajo demanda (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

La mayoría de proveedores en la nube brindan redundancia geográfica en su nube para permitir una alta disponibilidad, incluso en las posibilidades de violaciones de seguridad (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

2.8.4 Servicios de tercero confiable

Para garantizar la seguridad de la información en la nube se suele contratar a una tercera empresa que brinde el servicio de verificar una correcta prestación de servicios desde el punto de vista de la seguridad, usa generalmente un sistema de criptografía para revisar todas las operaciones cruciales entre el proveedor y el usuario. Es una organización imparcial que ofrece la confianza de las empresas mediante funciones de seguridad técnica y comercial a las transacciones electrónicas, con el fin de proporcionar una confianza web se establece el concepto de infraestructura de clave pública (PKI) (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

La clave pública es un medio legalmente aceptable y técnicamente sólido que permite implementar la integridad, la confidencialidad de los datos, la autorización, la autenticación y el no repudio en la nube (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

El tercero confiable verifica las entidades o sistemas que participan en la interacción en la nube, como son la certificación de servidores virtuales, dispositivos de red, usuarios y servidores de infraestructura física. PKI desarrolla las credenciales sólidas y necesarias para las entidades virtuales o físicas que están involucradas en la nube (Mushtaq et al, 2017), (Rot, 2017), (Varghese y Buyya, 2017), (Veeramachaneni, 2015).

2.9 Estándares para la seguridad en Computación en la nube

Al entender la forma en que está construida la tecnología de la computación en la nube, se ha encontrado que se existe mucha información sobre la arquitectura del Software, pero la información sobre los protocolos de comunicación utilizados es muy escasa o nula, la Computación en la Nube se ha ido desarrollando por diferentes fabricantes de software, pero hasta el momento no se tienen unos criterios de estandarización ni para la arquitectura del software, ni para los esquemas de comunicación que se utilizan. La falta de normas es el mayor problema para la nube (Mushtaq et al, 2017), (Veeramachaneni, 2015).

No existen aún marcos ampliamente aceptados para ayudar a la integración de los servicios en la nube en las arquitecturas empresariales, para apoyar la transferencia de información entre diferentes nubes o para permitir rápida adquisición y negociación de contratos (Mushtaq et al, 2017), (Veeramachaneni, 2015).

Respecto a los tipos de servicios de computación en la nube, IaaS, PaaS y SaaS su implementación se basa en los protocolos de comunicaciones TCP/IP, servicios Web, protocolos y formatos de datos Web con estándares bien establecidos, el intercambio de paquetes está regido por protocolos de comunicaciones típicos en un ambiente de computación distribuido tales como TCP, IP, SMTP y HTTP (Mushtaq et al, 2017), (Veeramachaneni, 2015).

Los estándares para los servicios de computación en la nube, en prescriptivos y evaluativos, dentro de los prescriptivos están los estándares de comunicaciones, tales como los protocolos TCP, IP, SNMP, HTTP, etc. Dentro de los evaluativos se consideran a los estándares de calidad de los sistemas de cloud computing, como la familia de estándares ISO 9000, y para seguridad de la información la familia ISO 27000 (Mushtaq et al, 2017), (Veeramachaneni, 2015).

La institución Unión Internacional de Telecomunicaciones o por sus siglas en ingles UIT ha realizado preclaros esfuerzos de estandarización de la computación en la nube, mediante su Grupo Focal (FG) y sus grupos de trabajo SG13 que dirigirá la normalización de cloud computing, y el grupo SG17 quien cubrirá la seguridad en la nube. Algunas de sus recomendaciones son: (Mushtaq et al, 2017), (Veeramachaneni, 2015).

2.9.1 UIT-T Y.3501

Es un marco de referencia para la computación en nube que identifica los requisitos de alto nivel para los tipos de servicios y la interconexión en la nube desde el extremo del proveedor al cliente. (Mushtaq et al, 2017), (Rao y Selvamani , 2015), (Subashini y Kavitha, 2011).

2.9.2 UIT-T Y.3510

Este trabajo presenta una visión general de la infraestructura de la nube, establece los requisitos para una arquitectura de cloud computing, contempla los requisitos para los recursos informáticos, los requisitos de recursos de la red, los requisitos de recursos de almacenamiento, y los requisitos para la abstracción y control de recursos (Mushtaq et al, 2017), (Rao y Selvamani , 2015), (Subashini y Kavitha, 2011).

2.9.3 UIT-T Y.3520

Se encarga de describir la plataforma de computación en la nube que se necesita para realizar la gestión de recursos de los usuarios, establece un marco para la gestión de extremo a extremo de los recursos. Se incluyen los conceptos generales de extremo a extremo en la gestión de recursos, se incluye también una visión para la gestión de recursos en un entorno apoyado en el uso intensivo de telecomunicaciones, contempla también la gestión de extremo a extremo de los recursos y servicios de la nube a través de múltiples plataformas (Mushtaq et al, 2017), (Rao y Selvamani , 2015), (Subashini y Kavitha, 2011).

2.9.4 UIT-T Y.3511

Es un marco de recomendaciones para la comunicación inter-redes y la infraestructura en la nube. Esta recomendación describe el marco para las interacciones de múltiples proveedores de servicios de computación en la nube, toma en cuenta los diferentes tipos de modelos que se conoce como inter-Cloud Computing. Sobre la base de los casos de uso que implican varios CSP y la consideración de los diferentes tipos de servicios y modelos en la nube y recomienda la posible relación entre varios proveedores, las interacciones, y los requisitos funcionales pertinentes (Mushtaq et al, 2017), (Rao y Selvamani , 2015), (Subashini y Kavitha, 2011).

2.9.5 UIT-T X.1600

En esta recomendación se proporciona una metodología marco para determinar las capacidades de seguridad para mitigar las amenazas, se establece una especificación para mejorar la mitigación de las amenazas de seguridad y hacer frente a los desafíos de seguridad de la computación en nube (Mushtaq et al, 2017), (Rao y Selvamani , 2015), (Subashini y Kavitha, 2011).

2.9.6 UIT-T Y.ccdef | ISO / IEC 17788

Este documento contiene Información general y el vocabulario de Cloud Computing, proporciona una visión general de la computación en nube, establece un conjunto de términos, definiciones y conceptos y es aplicable a todo

tipo de organizaciones (Mushtaq et al, 2017), (Rao y Selvamani , 2015), (Subashini y Kavitha, 2011).

2.9.7 UIT-T Y.ccra | ISO / IEC 17789

En esta recomendación se especifica la arquitectura de referencia de cloud computing, así como aspectos de calidad del servicio en cloud computing tales como en sus aspectos básicos y su terminología de Nivel de Servicio (SLA- Service Level Agreement), se describe una visión general de los SLA y los términos y las métricas de uso común en los SLA de servicios en la nube (Mushtaq et al, 2017), (Rao y Selvamani , 2015), (Subashini y Kavitha, 2011).

Otras organizaciones que han tomado un papel importante en la estandarización de los sistemas de Cloud Computing son:

2.9.8 Open Grid Forum (OGF):

Es una comunidad abierta comprometida con la evolución y la adopción de computación distribuida aplicada, tiene como objetivo la creación de una solución práctica para interconectarse con nubes tipo Infraestructuras como servicio (IaaS). Esta comunidad complementa su trabajo con foros abiertos, explora tendencias, comparte buenas prácticas y consolida estas prácticas en estándares (Mushtaq et al, 2017), (Rao y Selvamani , 2015), (Subashini y Kavitha, 2011).

2.9.9 Cloud Computing Interoperability Forum (CCIF)

Fue conformado para dinamizar el uso de computación en la nube y conseguir que las empresas trabajen de manera conjunta para la adopción amplia de la tecnología de Cloud Computing y servicios relacionados. Enfatiza su trabajo en la creación de una estructura común que permita intercambiar información entre dos plataformas de Cloud Computing de manera unificada (Pallis, 2010), (Radu, 2017).

2.9.10 DMTF

Se ocupa de establecer los estándares para la virtualización para que se simplifiquen la interoperabilidad, seguridad y gestión de las máquinas virtuales, utilizando un formato extensible, abierto, seguro, portable y eficiente para el empaquetado y distribución de las aplicaciones virtuales, permitiendo a los desarrolladores de Software lanzar soluciones pre-configuradas y listas para implementar, logrando así que los usuarios finales distribuir aplicaciones en sus ambientes con mínimo esfuerzo, la virtualización es parte de la infraestructura de la nube (Pallis, 2010), (Radu, 2017).

2.9.11 Open Cloud Consortium (OCC)

Es una organización sin fines de lucro patrocinada por la Universidad de Illinois en Chicago, investiga la creación de interfaces entre nubes con el objetivo de desarrollar estándares de compatibilidad y permitir las transiciones

suaves de un servicio en la nube a otro (Pallis, 2010), (Radu, 2017).

2.9.12 Cloud Security Alliance

Es una organización sin ánimo de lucro formada para promover el uso de mejores prácticas en el aseguramiento de la seguridad dentro de sistemas de computación en la nube, se ocupa también en proveer educación en el uso de cloud computing para ayudar a asegurar otras formas de computación (Pallis, 2010), (Radu, 2017).

2.10 Estado actual de la estandarización de seguridad en la computación en la nube

Para la seguridad de computación en la nube se han establecido algunos estándares que si llegar a ser de uso común en la comunidad de proveedores y desarrolladores de sistemas basados en la computación en la nube de alguna manera establecen buenas practicas que guían la tecnología de seguridad en la nube (Erl et al, 2013), (Saggi y Bhatia, 2015), (Sun et al, 2011), (Vasuyadav y krishnareddy, 2017).

2.11 La norma ISO 27017

Se utiliza con la familia de normas ISO 27001, la norma ISO/IEC 27017 proporciona controles para proveedores y clientes de servicios en la nube, aclara las funciones y responsabilidades de ambas partes a fin de que los servicios

en la nube sean tan seguros como el resto de los datos incluidos en un sistema de gestión de la información certificado. La norma proporciona una guía con 37 controles en la nube basados en ISO/IEC 27002, pero adjunta aspectos relacionados las responsabilidades entre el proveedor y el cliente, la disolución de contratos, protección virtual del cliente, configuración de la máquina virtual, procedimientos administrativos, seguimiento de las actividades y alineación del entorno de red (Sun et al, 2011), (Vasuyadav y krishnareddy, 2017).

2.12 La norma ISO 27018

Esta norma es un conjunto de buenas prácticas para garantizar la seguridad de la computación en la nube, se caracteriza porque crea un conjunto de normas, procedimientos y controles para que los proveedores de servicios de cómputo en la nube puedan garantizar el cumplimiento de las obligaciones legales en materia de tratamiento de los datos personales y proporciona a los clientes de la nube una herramienta comparativa para verificar y auditar a los niveles de cumplimiento de las regulaciones establecidas por el proveedor (Sun et al, 2011), (Vasuyadav y krishnareddy, 2017).

Esta norma contempla que el proveedor tendrá que proporcionar las herramientas adecuadas para permitir y facilitar al cliente, de los derechos de acceso, rectificación y cancelación en relación con el tratamiento de los datos y debe velar por el cumplimiento del tratamiento a los únicos usos descritos al cliente en el momento de la contratación del servicio, en particular garantizando que los datos no serán utilizados para fines distintos de los especificados por el cliente, ni para el propósito de marketing directo o publicitario, a menos que haya consentimiento explícito o salvo que exista una prohibición establecida por la ley, la solicitud de divulgación de los datos personales por parte de las autoridades administrativas o judiciales (Sun et al, 2011), (Vasuyadav y krishnareddy, 2017).

En cuanto al tema de la subcontratación, la norma establece, el derecho que tiene del cliente de conocer toda la cadena de los subcontratistas, los países en los que se establecen, la ubicación de los Data Centers utilizados por ellos y sus obligaciones en relación con el tratamiento de los datos. También se reconoce el derecho del cliente a oponerse a los cambios en la cadena de los subcontratistas y a poder rescindir el contrato cuando este en desacuerdo. En relación con las medidas de seguridad de la información, contempla que

todo el personal del proveedor y de los subcontratistas deben firmar un acuerdo de confidencialidad (Sun et al, 2011), (Vasuyadav y krishnareddy, 2017).

Dentro de otras ventajas de las norma ISO 27018 se puede mencionar que por ejemplo que el proveedor sea transparente en los términos y condiciones de sus servicios, y en las prácticas de negocio que lleva a cabo; y demuestre compromiso con el cliente para ayudarle a cumplir con las leyes y regulaciones sobre protección de datos personales o privacidad, y seguridad. Respecto al cliente, hace posible que controle el tratamiento de los datos personales que ha encomendado al proveedor (Sun et al, 2011), (Vasuyadav y krishnareddy, 2017).

2.13 CSA Cloud Controls Matrix (CSA CCM)

Es una matriz creada para proporcionar principios de seguridad fundamentales y para orientar a los proveedores de la nube, así como para posibilitar a los clientes de la nube a evaluar el riesgo de seguridad de un proveedor de la nube. Proporciona un marco de control que permite una comprensión detallada de los conceptos y principios de seguridad que están alineados con la propuesta de Cloud Security Alliance y se basan en su relación personalizada con otros estándares de seguridad como ISO 27001/27002, ISACA COBIT, PCI, NIST, etc. (EINISA, 2012), (ISACA, 2009), (Singh et al, 2017).

2.14 Ventajas empresariales de la computación en la nube

La creación de aplicaciones en la nube presenta ciertas ventajas empresariales. A continuación, mencionamos algunas de ellas:

Inversión inicial en infraestructura casi nula

En el supuesto que se tenga que implementar un sistema a gran escala los costos a considerar serian altos al invertir en un edificio, en seguridad física, en hardware, gestión del hardware (gestión energética, refrigeración) y en personal de operaciones. Por el nivel de costes iniciales, se necesitaría varias reuniones con la alta dirección para ponerlo en marcha, pero con la computación en la nube, no existe ningún tipo de coste fijo ni de coste de puesta en marcha (EINISA, 2012), (ISACA, 2009), (Singh et al, 2017).

Infraestructura justo a tiempo

Mediante la implementación de servicios en la nube, se logra el aprovisionamiento automático justo a tiempo sin tener la preocupación de procurar la capacidad previa para sistemas a gran escala, se aumenta la agilidad, se reduce los riesgos y disminuye los costes operativos, ya que tendrá que ampliar únicamente cuando se crezca y solo se pagará estrictamente por lo que use (EINISA, 2012), (ISACA, 2009), (Singh et al, 2017).

Utilización de recursos más eficiente

La computación en la nube resuelve el problema de los administradores de sistemas referente a la preocupación de conseguir hardware cuando se quedan sin capacidad o tienen capacidad ociosa pues con la nube pueden gestionar los recursos con mayor eficacia y eficiencia en un entorno en el que las aplicaciones solicitan y ceden los recursos bajo demanda (EINISA, 2012), (ISACA, 2009), (Singh et al, 2017).

Costes según el uso

En la nube se establece el sistema de fijación de precios similar a los servicios públicos, únicamente se le cobrará por los servicios que se haya utilizado, no se tendrá que pagar por infraestructura asignada pero no utilizada. Se puede reducir los costos si se implementa una revisión de los reales servicios que se están presentando (EINISA, 2012), (ISACA, 2009), (Singh et al, 2017).

Reducción del tiempo de comercialización

El uso de la computación en paralelo reduce el tiempo de procesamiento Tener disponible una infraestructura elástica ofrece a la aplicación la posibilidad de aprovechar la paralización de una forma rentable, reduciendo el tiempo de comercialización (EINISA, 2012), (ISACA, 2009), (Singh et al, 2017).

2.15 Ventajas técnicas de la computación en la nube

Entre algunas de las ventajas técnicas de la informática de nube se incluyen las siguientes:

Automatización.

Se podrá crear secuencias de comandos podrá crear sistemas de creación e implementación que podrán repetirse aprovechando la infraestructura programable gestionada mediante API (EINISA, 2012), (Singh et al, 2017).

Autoescaling

Se podrá ampliar y reducir sus aplicaciones para adaptarlas a demandas inesperadas sin ningún tipo de intervención humana. La función Autoescaling promueve la utilización y hace que el sistema funcione de una forma más eficiente (EINISA, 2012), (Singh et al, 2017).

Escalado proactivo

Permite ampliar y reducir su aplicación para cumplir con demandas previstas, con una planificación adecuada y el conocimiento correcto de sus patrones de tráfico con el objeto que los costes no sean elevados a la hora de escalar (EINISA, 2012), (Singh et al, 2017).

Ciclo de vida del desarrollo más eficiente

Los sistemas de producción podrán clonarse con facilidad para utilizarlos como entornos de desarrollo y prueba. Los entornos de ensayo podrán trasladarse fácilmente a entornos de producción (EINISA, 2012), (Singh et al, 2017).

Funciones de prueba mejoradas

Se podrá instaurar un laboratorio de pruebas instantáneo con entornos reconfigurados que estará vigente únicamente durante el periodo de la fase de pruebas (EINISA, 2012), (Singh et al, 2017).

Recuperación de desastres y continuidad empresarial

La nube proporciona una opción de menor coste para mantener servidores y almacenamiento de recuperación de desastres, se puede aprovechar sacar la distribución geográfica y replicar el

entorno en otros lugares en tan solo unos minutos (EINISA, 2012), (Singh et al, 2017).

“Desbordar” el tráfico hacia la nube:

Mediante procesos sencillos se podrá hacer el equilibrado de carga, logrando crear una aplicación totalmente a prueba de desbordamiento, mediante el enrutado del exceso de tráfico hacia la nube (EINISA, 2012), (Singh et al, 2017).

2.16 Proveedores de computación en la nube

2.16.1 Amazon Web Services (AWS)

Es uno de los proveedores de los servicios tipo IaaS más importante en el mercado informático, permite crear una imagen de máquina virtual de Amazon con el sistema operativo Windows o Linux en donde el usuario instala sus aplicaciones, librerías y datos, se asigna características físicas de acuerdo al contrato suscrito con el usuario, se accede a esta máquina de manera remota como si accediera a un servidor físico tradicional, se puede escalar sus servicios y monitorear el estado de su máquina virtual. Los servicios más destacables de Amazon son los siguientes: (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Amazon Elastic Compute Cloud (EC2):

Es un servicio web que proporciona capacidad modificable y está diseñado para facilitar a los

desarrolladores en la nube escalable basada en web (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Identity and Access Management (IAM).

Controla de forma segura el acceso a servicios y recursos de AWS, se puede crear y gestionar usuarios y grupos de AWS, así como utilizar permisos para permitir o denegar el acceso de estos a los recursos (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Amazon Simple Storage Service (S3).

Incorpora una sencilla interfaz de servicios web para almacenar y recuperar datos desde cualquier ubicación de la web, se ofrece varios tipos de almacenamiento diseñados para distintos casos de tipo de nube (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Amazon RDS.

Para configurar, gestionar y escalar una base de datos relacional en la nube, permite gestionar las tareas de administración de la base de datos, se puede elegir entre seis motores de bases de datos conocidos: Amazon Aurora, Oracle, Microsoft SQL Server, PostgreSQL, MySQL y MariaDB (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Amazon Route 53.

Establece un sistema de nombres de dominio (DNS) escalable y de alta disponibilidad. Está diseñado para ofrecer a los desarrolladores y las empresas una forma altamente fiable y rentable de direccionar los usuarios a las aplicaciones en Internet (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Amazon Cloud Watch.

Permite la supervisión de los recursos de la nube de AWS y de las aplicaciones que se ejecutan en AWS. Puede utilizarse para recabar métricas y hacer un seguimiento de las mismas, recopilar y supervisar archivos de registro y establecer alarmas (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

2.16.2 Windows Azure

Es una plataforma de nube que permite implementar y administrar aplicaciones en una red global de centros de datos administrados por Microsoft. Se puede compilar aplicaciones en cualquier lenguaje, herramienta o marco (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Los servicios más destacables que ofrece Windows Azure son:

Aplicaciones web de Azure.

Permite implementar y escalar fácilmente aplicaciones web escritas en varios lenguajes como .NET, Java, PHP y Python. La función de escalado automático integrada permite escalar o reducir verticalmente una aplicación web en función del tráfico real de clientes (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Máquinas virtuales de Azure.

Se ofrece Máquina virtual y Red virtual, una aplicación se puede implementar en una máquina con distintos sistemas operativos como Windows, Linux, etc. Una máquina virtual se puede escalar verticalmente desde una con pocas capacidades hasta otra con capacidades a demanda con memoria suficiente y procesadores, la máquina virtual incluye un servidor web, un servidor de base de datos y entornos de desarrollo y prueba (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Informática de alto rendimiento.

Con Azure, se puede escalar los recursos horizontalmente o reducirlos verticalmente de forma fácil, mientras se aprovecha la avanzada infraestructura de redes y procesos que se ha configurado específicamente para ejecutarse incluso en las aplicaciones HPC más exigentes. La combinación de flexibilidad y rendimiento da como resultado pagar solo por el tiempo que se usa los

recursos (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Soporte para Sistemas operativos Linux.

Azure hace sencillo crear una máquina virtual en Linux por medio de la galería de imágenes (blueprints) utilizando el Portal de administración. También es posible acceder a las instancias de estas máquinas virtuales Linux para personalizarlas a gusto por medio de un usuario con privilegios de administrador. También se pueden implementar máquinas virtuales ya disponibles que corren sistemas operativos Linux, por ejemplo, con instancias de máquinas virtuales VMWare (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

SQL Server en máquinas virtuales.

Si se requiere funcionalidades de SQL Server en Máquinas virtuales se pueden encontrar ofertas de imágenes de SQL Server 2012 y SQL Server 2008 R2 en sus ediciones Standard, Web y Enterprise. Si tiene una licencia de SQL Server con Software Assurance, como ventaja adicional puede trasladar la licencia existente a Windows Azure y pagar solo por proceso y almacenamiento (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

2.16.3 Google App Engine

Permite crear y alojar aplicaciones web en los mismos sistemas escalables con los que funcionan las aplicaciones de Google. Además, ofrece procesos de desarrollo y de implementación rápida y una administración sencilla, sin necesidad de preocuparse por el hardware, las revisiones o las copias de seguridad y una ampliación sin esfuerzos (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Las aplicaciones Google App Engine son fáciles de crear, fáciles de mantener y fáciles de escalar a medida que el tráfico y las necesidades de almacenamiento de datos crecen. Con App Engine no es necesario mantener ningún servidor. Basta con cargar su aplicación y está ya se encontrará lista para servir a los usuarios (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Como servicios más destacados ofrece los siguientes:

Google Compute Engine.

Proporciona máquinas virtuales que se ejecutan en Google de los centros de datos innovadores y red de fibra. Las herramientas y flujo de trabajo de apoyo permiten escalar de casos individuales a lo global, la computación en nube con equilibrio de carga. Compute Engine provee el arranque máquinas virtuales de forma rápida, vienen con almacenamiento

en disco persistente, ofrecen un rendimiento consistente y están disponibles en muchas configuraciones incluyendo tamaños predefinidos o la opción de crear Tipos de máquina personalizada optimizados para sus necesidades específicas (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Google App Engine.

Es una plataforma para la creación de aplicaciones web escalables y backends móviles. Proporciona servicios y APIs integrados tales como almacenes de datos NoSQL, memcache, y una API de autenticación de usuario, comunes a la mayoría de las aplicaciones. Ademas permite escalar automáticamente en respuesta a la cantidad de tráfico que recibe por lo que sólo paga por los recursos que utiliza. Sólo tienes que subir su código y Google se encargará de la disponibilidad de su aplicación. No es necesario disponer o mantener servidores (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Google Cloud SQL.

Es un servicio de base de datos gestionada totalmente lo que hace que sea fácil de configurar, mantener, gestionar y administrar las bases de datos MySQL relacionales en la nube. Ademas ofrece un mejor

rendimiento, escalabilidad y conveniencia. Alojado en Google Cloud Platform, Nube SQL proporciona una infraestructura de base de datos para aplicaciones que se ejecutan en cualquier lugar (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

2.16.4 Dropbox

Dropbox es un programa que une todos los ordenadores que se quiera a través de una única carpeta, permitiendo hacer copias de seguridad y sincronizar archivos entre ordenadores. Dentro de esa carpeta podemos crear tantas subcarpetas e incluir tantos archivos como queramos, en principio hasta una capacidad de 2 GB, que nos ofrecen gratuitamente, aunque pagando podemos aumentarla hasta a 100 GB (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Aunque no contemos en un momento determinado con nuestro ordenador (por ejemplo, si estamos de viaje o en el colegio) podremos acceder a nuestros archivos en esa carpeta (y subcarpetas) a través de Internet visitando el sitio web de Dropbox, pudiendo además compartir aquellas carpetas que queramos con otras personas (por ejemplo, con nuestros alumnos). Puede utilizarse también con dispositivos

móviles (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

2.16.5 Google Drive

Google Drive es un servicio web que le permite almacenar, modificar, compartir y acceder a sus archivos y documentos independientemente de dónde se encuentre a través de internet. Puede subir al servicio más de 30 tipos de archivos entre los que se incluyen vídeos en alta definición, PSD de Photoshop® o AI de Adobe Ilustrator®. El servicio dispone de almacenamiento ilimitado gratuito (beneficio UFM). Dispone de versiones móviles tanto para Android como para IOS para poder acceder a través de nuestro dispositivo a nuestros datos, editar documentos etc. (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

2.16.6 OneDrive

Es un servicio de almacenamiento online, similar a un disco duro adicional disponible para cualquier dispositivo, y que proporciona las siguientes características:

Un solo lugar de trabajo para todos tus archivos de trabajo u ocio permitiendo su almacenamiento, sincronización y compartición de forma segura.

Trabajar e interaccionar más fácilmente con otros usuarios porque permite la colaboración en tiempo real.

Cumplimiento con los principales estándares de seguridad con el propósito de mantener protegidos los datos (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

2.16.7 Pydio

Pydio es una alternativa de código abierto a Dropbox y ownCloud, es decir es una plataforma para el intercambio de archivos, y aunque está enfocada en el usuario, esta plataforma está dirigida a empresas y organizaciones. Pydio se centra principalmente en montar un servidor de almacenamiento privado con software libre y carente de funciones y configuraciones adicionales por defecto, aunque si se pueden instalar mediante el uso de plugins. Esta plataforma resulta ideal para aquellos que buscan un servidor de almacenamiento sencillo y potente (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

2.16.8 Next Cloud

Nextcloud proporciona acceso universal a sus archivos a través de la web, su computadora o sus dispositivos móviles dondequiera que se encuentre. También proporciona una plataforma para ver y sincronizar fácilmente sus contactos, calendarios y

marcadores en todos sus dispositivos y permite la edición básica directamente en la web (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

2.16.9 OwnCloud

Owncloud es un software open source bajo licencia AGPL que permite crear un servidor en la nube. Lejos de lo que pueda parecer, crear y administrar nuestro propio servidor y disponer de él en la nube es muy sencillo. A estas alturas a todos nos suenan términos como “cloud computing” y “servidor en la nube” y la mayoría de nosotros utilizamos los servicios de alguno de ellos como p.ej. UbuntuOne, DropBox, SpiderOak, Sugar Sync, Google Drive, etc. Basta con crear una cuenta en uno de estos servicios y ya disponemos de un espacio en el que almacenar nuestros archivos; En cualquier momento podemos acceder a ellos desde un ordenador que disponga de conexión a internet. No obstante, el espacio disponible, aunque gratuito es muy limitado y si trabajamos en serio nos resulta insuficiente. Cierto es que podemos contratar espacio adicional, pero esto ya nos supone un coste económico. Además, la confidencialidad de nuestros datos y de nuestros archivos está supeditada a la “honestidad” de las empresas que ofrecen este tipo de servicios. Owncloud nos permite crear un servidor y conectarlo a internet, de una manera sencilla. Además, seremos

nosotros quienes lo administraremos controlando el acceso a la información almacenada (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

Podemos contratar un hosting e instalar owncloud, pero también podemos instalarlo en un ordenador propio. De esta forma eliminamos las limitaciones en cuanto a capacidad ya que dispondremos de todo el espacio libre que tengamos en el disco duro. Owncloud trae activado por defecto soporte para WebDAV con el que podemos conectarnos a nuestra nube desde un explorador de archivos y desde un navegador web; también dispone de CalDAV para sincronizar el calendario, CardDAVpara gestionar nuestra agenda de contactos y Ampache con el que podremos hacer streaming de audio y vídeo (Muthakshi y Meyyappan, 2013), (Singh et al, 2017), (View y Heng, 2014), (Zissis y Lekkas, 2012).

CAPITULO III: VARIABLES E HIPOTESIS

3.1 Definición de las variables

Se define a continuación las variables que se han utilizado en la investigación, clasificándolas y estableciendo la manera de como se ha llevado a cabo su estudio, es decir su operacionalización.

3.1.1 Variable dependiente.

Sistema de gestión de seguridad de la información en la nube para una universidad.

Constituido por un conjunto de controles organizados según políticas de seguridad de la información para lograr el resguardo de los activos de información que son migrados a los servicios de computación en la nube.

3.1.2 Variable independiente.

Normatividad de Seguridad de la información en la nube.

Está formada por las buenas prácticas de seguridad en la nube que son acopiadas en los expertos en el tema y plasmadas en las diferentes normas que son patrocinadas por organismos reguladores internacionales.

3.2 Operacionalización de las variables

El estudio de las variables se hace mediante la descripción e implementación de sus respectivos componentes, estableciendo la definición conceptual de cada una de las variables sus respectivas dimensiones y sus indicadores.

Variable dependiente: Sistema de gestión de seguridad de la información en la nube para una universidad.

Dimensiones de la variable:

Políticas de seguridad de la información.

Responsables de la seguridad de la información.

Controles establecidos para el resguardo de activos.

Organización para la seguridad de la información.

Planes de contingencia.

Relaciones contractuales con los proveedores de servicios en la nube.

Roles y responsabilidades asumidas por la organización y compartidas con el proveedor de servicios.

Indicadores de medición de la variable:

Numero de políticas sobre seguridad de la información establecidas.

Número de reuniones del comité de seguridad de información de la institución.

Veces de actualizaciones del organigrama de la organización para considerar la seguridad de la información.

Porcentaje del riesgo asumido

Porcentaje del riesgo residual

Numero de planes de contingencia

Reportes de incidencias de violaciones a la seguridad de la información en la nube.

Numero de revisiones de los aspectos contractuales con los proveedores de servicios.

Variable independiente: Normatividad de Seguridad de la información en la nube.

Dimensiones de la variable:

Activos de información de la institución.

Vulnerabilidades que presentan los sistemas.

Amenazas a las que están expuestos los activos de información.

Riesgo de que las amenazas se cristalicen a través de las vulnerabilidades y afecten los activos de información.

Impacto del riesgo.

Indicadores de medición de la variable:

Número de veces de actualización del inventario de activos de información.

Número de veces de actualización de la identificación de amenazas a los activos de información.

Actualizaciones de las vulnerabilidades

Matriz de riesgo que relacione las amenazas, su probabilidad de ocurrencia y el impacto

3.3 Hipótesis general e hipótesis específicas

3.3.1 Hipótesis general

La implantación adecuada de controles para seguridad de la información en la nube basada en estándares internacionales garantiza la implementación de un adecuado sistema de gestión seguridad de información en la nube para una institución universitaria.

3.3.2 Hipótesis específicas

3.3.2.1 Hipótesis específica 1.

Los aspectos legales y las políticas de seguridad de la institución universitaria permiten definir que procesos de gestión se pueden migrar a la nube y cuales no deben ser implementados para no trasgredir la normatividad.

3.3.2.2 Hipótesis específica 2.

Basado en las buenas prácticas de los estándares internacionales que hacen referencia a los modelos de nubes y los tipos de servicios ofrecidos por los diversos proveedores se puede seleccionar el modelo de red y tipo de servicio para garantizar la preservación de la seguridad de la información en la nube.

3.3.2.3 Hipótesis específica 3.

Una adecuada evaluación de proveedores de servicio en la nube y tomando como referencia el modelo de red elegido y el tipo de servicio elegido mediante acuerdos contractuales se puede construir la arquitectura que soporte los procesos elegidos para migrar a la nube.

CAPITULO IV: METODOLOGIA

4.1 Tipo de investigación

Esta investigación por su naturaleza es considerada dentro de la clasificación como investigación aplicada puesto que se pone en práctica las bases teóricas para obtener un producto tangible como lo es un sistema de seguridad de la información en la nube para una universidad.

4.2 Diseño de la investigación

El diseño de la investigación está ligado a la metodología que se utilizó para lograr los objetivos específicos. La investigación se hará por etapas adecuando los procesos de gestión de los activos de información a las buenas prácticas establecidas en los estándares internacionales sobre seguridad de la información en la nube.

4.2.1 Etapas de la investigación

La presente investigación se hará en base a las siguientes etapas:

Seleccionar las bases de datos para realizar una Revisión Sistemática para obtener los estándares más usados por la comunidad de usuarios de seguridad de la información en la nube.

Realizar la Revisión Sistemática en las principales bases de datos bibliográficas relacionadas con el tema.

Seleccionados los principales estándares de seguridad de la información en la nube, se procede a establecer las mejores prácticas comunes de los estándares a fin de establecer las bases de la estrategia a formular.

Basado en las buenas practicas obtenidas, se estableció la estrategia a recomendar.

Para validar la estrategia formulada se procedió a recomendar como hacer la implementación en la Universidad Nacional del callao en base a sus procesos académicos y administrativos de las principales áreas funcionales.

Se hizo el análisis del parque tecnológico in formatico de la Universidad para en base a los resultados recomendar la implementación de la infraestructura tecnológica a usar en la nube.

4.2.2 Estrategias de pruebas de hipótesis

Para probar la hipótesis establecida, se presenta una metodología para la implementación de controles de seguridad en la nube, esta metodología se fundamenta en una serie de etapas siguiendo las recomendaciones de los estándares internacionales sobre seguridad de la información en la nube

implementados en un ciclo de mejora continua según la propuesta de Deming y consiguiendo la mejora de los controles a través de una propuesta de madurez.

Materiales:

Los materiales utilizados para esta investigación son fundamentalmente los estándares internacionales sobre seguridad de la información en la nube
Como materiales de apoyo se ha contado con:
2 computadoras con conexión a internet.
2 USB de 32 Gb.
1 impresora múltiple.
10 millares de papel bond A4.
Útiles de escritorio.

Lugar de desarrollo:

La tesis en mención se desarrolló en la Facultad de Ingeniería Industrial y de sistemas en la Escuela Académica Profesional de Ingeniería de Sistemas de la Universidad Nacional del Callao.

Lugar de aplicación:

Para la parte experimental se tomó en cuenta las diferentes áreas funcionales de la Universidad Nacional Callao y la validación con los procesos de esta institución.

4.3 Población y muestra.

Población.

Para esta investigación la población de estudio está constituida por todos los estándares sobre seguridad de la información en la nube, publicados hasta la fecha.

Muestra.

Se seleccionan como muestra los estándares que tienen mayor aceptación entre la comunidad de usuarios de seguridad de la información en la nube y que tienen aceptación y reconocimiento internacional.

4.4 Técnicas e instrumentos de recolección de datos.

Para la recolección de datos se utilizó los motores de búsqueda de las bases de datos bibliográficas como SCOPUS, IEEE DIGITAL EXPLORER, ACM, ELSEIVER, como técnica se utilizó la Revisión Sistemática y como instrumento de recolección de datos un listado consultas estructuras en base a las preguntas de investigación establecidas al inicio de la Revisión Sistemática.

4.5 Procedimiento de recolección de datos.

Se siguió las recomendaciones establecidas en protocolo de una revisión sistemática que consiste en:

Establecer las preguntas de investigación

Seleccionar las palabras claves

Establecer las consultas

Realizar las consultas

Acopiar los artículos de investigación

4.6 Procesamiento estadístico y análisis de datos.

Se hizo el proceso estadístico de Meta análisis en base a los artículos científicos obtenidos y el análisis de datos se basó en la lectura de los resúmenes de los artículos y en la parte conceptual y metodológica de los mismos para obtener el nivel de importancia que tiene el estándar en el trabajo de investigación, seleccionado en base a evidencias los estándares sobre seguridad de la información más conocidos y utilizados en el mundo.

CAPITULO V: RESULTADOS

5.1 Modelo SGSI-UN-CN

Como resultado se presenta un modelo denominado SGSI-UN-CN para crear o actualizar un Sistema de Gestión de Seguridad de la Información de una universidad pública a fin de establecer una hoja de ruta a seguir para aprovechar de manera adecuada y legal los servicios ofrecidos en la nube por diferentes proveedores de estos servicios.

La validación de este modelo es obvio pues proviene de seleccionar buenas prácticas recomendadas por expertos en el mundo y plasmados en los diferentes estándares respecto a lo que se debe tener en cuenta para construir un Sistema de Seguridad de la Información en la nube.

La propuesta formulada se fundamenta en los siguientes aspectos:

- Los estándares de la familia ISO 27000 para formular un sistema de gestión de seguridad de la información(SGSI) básicamente las normas ISO 27001, ISO 27002, ISO 27005 y 27006 que permiten crear un SGSI de forma estructurada basado en la gestión de riesgos.

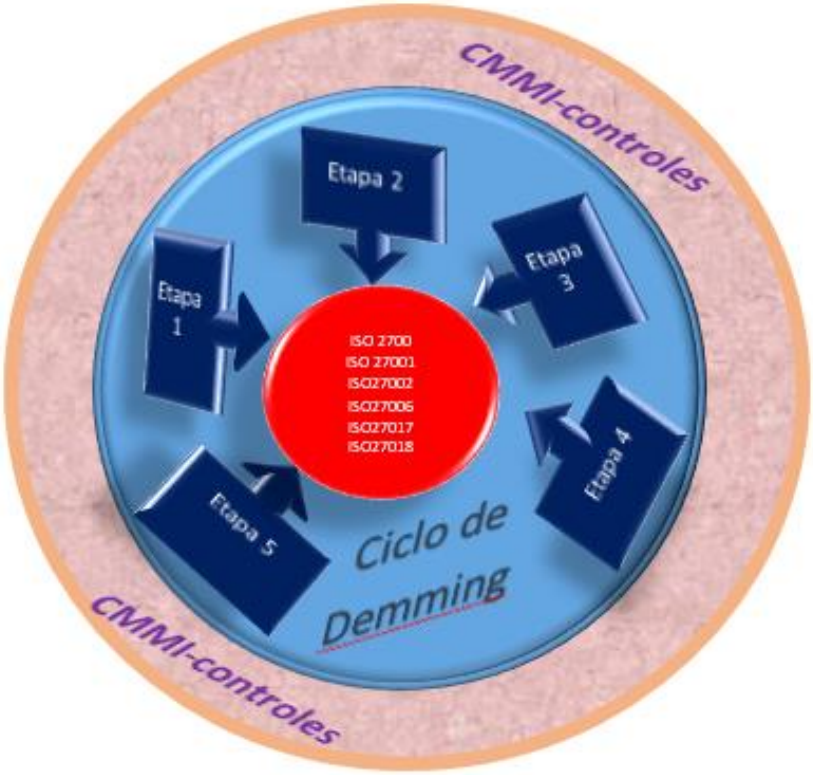
- Las normas ISO 27017, ISO 27018 que contemplan aspectos para seguridad de la información en la nube incluyendo la seguridad de datos personales.
- Los modelos contractuales para la negociación de la prestación de servicios en la nube entre el proveedor y el cliente.
- El ciclo de mejora continua de Deming que permite implementar la calidad en una organización y sostenerlo de manera permanente.

- El modelo de madurez de organizaciones CMMI para la mejora de la capacidad de los procesos y de esta forma lograr la madurez de los controles para la seguridad en la nube.

5.2 Etapas del Modelo SGSI-UN-CN

El modelo SGSI-UN-CN propone que se debe implementar un Sistema de Gestión de ´la Seguridad de la Información en la Nube por etapas, proponiendo cinco etapas, las cuales se implementan de manera progresiva y se da mantenimiento de forma permanente dentro de un ciclo de mejora continua de Demming y atendiendo a la mejora de los controles dentro de un marco de mejora de capacidades y madurez de los mismos, en la Figura 5.1 muestra el modelo planteado, Observe que cada etapa recoge las buenas prácticas de los estándares correspondientes. El circulo de Deming permite la implementación gradual en las etapas y circulo de madurez CMMI obliga a mejorar los procesos para que los controles alcances sus niveles de madurez adecuados.

Figura 5.1
MODELO SGSI-UN-CN



Se describen detalladamente las etapas propuestas

5.2.1 Etapa 1. Creación del SGSI

Esta etapa tiene por finalidad crear el SGSI pero es opcional en el caso que ya se cuente con un SGSI implementado, para esta etapa se siguen las recomendaciones de las normas ISO 27001, ISO 27002, ISO 27005 y 27006 y consta de las siguientes tareas.

a) Formación del comité directivo del SGSI
b) Definición de las políticas de seguridad de la información

c) Identificación de los activos de información y los responsables de resguardarlos.
d) Identificación de las amenazas
e) Identificación de las vulnerabilidades
f) Construcción de la matriz de riesgos
g) Evaluación del impacto de los riesgos
h) Formulación de los controles.

5.2.2 Etapa 2. Preparación para migración a la nube.

Establecido ya el SGSI, esta etapa tiene por objetivo migrar a la nube parte de los procesos de la universidad, teniendo en cuenta las recomendaciones que hacen los estándares para seguridad en la nube.

De acuerdo a la metodología establecida en primer lugar se determinará qué información o aplicación se va a migrar y la importancia que esta tiene dentro de la universidad, teniendo en cuenta los atributos de la seguridad de la información (confidencialidad, integridad y disponibilidad), deben considerarse las siguientes tareas:

- Identificación de los procesos
- Evaluación de las restricciones
- Evaluación del parque tecnológico
- Selección del modelo de servicios
- Selección de proveedores
- Socialización del cambio.

a) Identificación de los procesos

Primero se identifica los procesos que se realizan en la institución. Los procesos una universidad pública y en particular en la UNAC se clasifican en dos tipos, a saber:

Los procesos administrativos y los procesos académicos, ambos tipos pueden ser implementados total o parcialmente en la nube siguiendo una estrategia adecuada que garantice la seguridad de la información.

Los procesos académicos se dan fundamentalmente en las facultades y en las dependencias asociadas al Vicerrectorado Académico y al Vicerrectorado de investigación, los procesos administrativos por el contrario de dan en las dependencias asociadas al Rectorado, ver organigrama en el Anexo B para identificar las dependencias de las universidades.

Antes de migrar los procesos a la nube, lo aconsejable es comenzar con procesos del negocio que no impacten en la productividad de la institución y no afecten la prestación de servicios de la institución. Lo recomendable es una migración paso a paso.

En el cuadro 5.1, se presenta una propuesta para hacer un inventario de los procesos académicos de una Facultad de la UNAC y el nivel de impacto en la productividad.

El nivel de impacto en la productividad es un indicador que se obtiene en base a la asignación de un valor entre 0 y 100 y representa el porcentaje de importancia que tiene el proceso

en la prestación de un buen servicio a la comunidad universitaria.

Cuadro 5.1.
PROCESOS ACADÉMICOS EN UNA FACULTAD E IMPACTO EN EL NIVEL DE PRODUCTIVIDAD

Proceso	Decanato	Dirección de escuela	Jefatura de departamento	Unidad de investigación	% de impacto
Matrícula	x	x	x		80
Registro de notas	x	x			80
Programación académica	x	x	x		90
Registro de notas	x	x			70
Planes curriculares	x	x			50
Convalidaciones		x			30
Reservas de matriculas		x			30
Certificaciones	x	x			30
Resoluciones.	x	x		x	50
Rectificación de matrícula		x			30
Matrícula especial		x			30
Adecuación curricular		x			30
Constancia para egresar	x				20
Traslados internos	x	x			50
Traslados externos	x	x			50
Control de prácticas pre profesionales	x	x			30
Carga horaria		x	x		80
Cartas de presentación	x				20
Control de asistencia		x	x		80
Control de avance silábico		x			80
Actas de notas	x	x			70
Rectificación de notas	x	x			50
Cursos dirigidos		x			20
Cursos paralelos		x			20
Ampliación de créditos		x			40
Asignación de docentes			x		80
Control de carga lectiva	x	x	x		80
Control de carga no lectiva	x	x	x		80
Control de documentos de docentes	x		x		80
Planes de trabajo individual	x	x			80
Proyectos de investigación				x	50
Informes trimestrales de investigación				x	50
Informes finales de investigación				x	50

De igual forma en los cuadros 5.2 y 5.3 se presentan los procesos académicos asociados a las responsabilidades del Vicerrectorado Académico, y al Vicerrectorado de Investigación respectivamente especificando el impacto en la productividad de la universidad.

Cuadro 5.2.
PROCESOS ACADÉMICOS EN EL VICERRECTORADO ACADÉMICO Y NIVEL DE PRODUCTIVIDAD

Procesos de:	% de impacto
Planificación del año académico	80
Planificación de los ciclos académicos	80
Gestión de las currículos	90
Registros académicos y archivos académicos	70
Procesos de educación a distancia	50
Reglamento de docentes	30
Reglamento de estudiantes	30
Convenios nacionales	30
Convenios internacionales	50
Centro Pre-Universitario	30
Unidad de Archivo General	30
Oficina de Bienestar Universitario	30
Oficina de Servicios Académicos	20
Oficina de Educación a Distancia	50
Oficina de Desarrollo Docente e Innovación	50
Centro de Idiomas	30

Cuadro 5.3.
PROCESOS ACADÉMICOS EN EL VICERRECTORADO DE INVESTIGACIÓN Y NIVEL DE PRODUCTIVIDAD

Procesos de:	% de impacto
Dirección de Evaluación, Transferencia Tecnológica y Patentes - DETTP	80
Oficina de Gestión de la Investigación	80
Editorial Universitaria	90
Instituto Central de Investigación de Ciencia y Tecnología	70
Instituto de Investigación de Especialización en Agroindustria	50
Oficina de Capacitación VRI	30

En el Cuadro 5.4 se presentan los principales procesos de la Dirección General de Administración de la universidad (DIGA).

En el Cuadro 5.4 de igual forma se presentan los principales procesos a cargo del Rectorado, especificando el nivel de impacto correspondiente.

Cuadro 5.4.
PROCESOS ADMINISTRATIVOS EN EL RECTORADO Y NIVEL DE PRODUCTIVIDAD

Procesos de:	% de impacto
DIGA	
Oficina de Recursos Humanos	90
Oficina de Tesorería	70
Oficina de Contabilidad y Presupuesto	50
Oficina de Abastecimientos y Servicios Auxiliares	30
Oficina de Infraestructura y Mantenimiento	30
Oficina de Gestión Patrimonial	30
RECTOR	
Resoluciones	50
Oficina de Secretaría General	30
Oficina Asesoría Jurídica	80
Oficina de Tecnología de Información y Comunicación	20
Dirección Universitaria de Gestión y Aseguramiento de la Calidad	80
Oficina de Planificación y Presupuesto	80
Dirección Universitaria de Extensión y Responsabilidad Social (DUERS)	70
Oficina General de Admisión	50
Oficina de Relaciones Públicas e Imagen Institucional	20
Oficina de Cooperación Técnica Internacional	20

b) Evaluación de las restricciones

Corresponde luego evaluar si existen restricciones regulatorias, políticas o normas internas en la institución que limiten la migración de información o aplicaciones a la

nube, debido al alto impacto que la prestación de estos servicios brinda a la organización.

Tener presentes las características regulatorias políticas o normatividades que impidan la migración a la nube Si hay procesos que trabajan en un sector regulado, es importante que la migración no infrinja una normatividad nacional o internacional, del mismo modo si los procesos están certificados bajo algún criterio de certificación, es necesario tomar en cuenta que deberán apegarse a las recomendaciones.

En el Cuadro 5.5. se presentas los procesos y se mencionan los aspectos regulatorios para tomar en cuenta al momento de decidir que procesos se deben implementar primero en la nube.

Cuadro 5.5.
PROCESOS Y ASPECTOS REGULATORIOS

Proceso	Facultades	VRA	VRI	DIGA	Rector	Regulado
Matrícula	x					no
Registro de notas	x					si
Programación académica	x					no
Planes curriculares	x					no
Convalidaciones	x					no
Reservas de matriculas	x					no
Certificaciones	x					no
Resoluciones.	x					no
Rectificación de matrícula	x					no
Matrícula especial	x					no
Adecuación curricular	x					no
Constancia para egresar	x					no
Traslados internos	x					no
Traslados externos	x					no
Control de prácticas pre profesionales	x					no
Carga horaria	x					no
Cartas de presentación	x					no
Control de asistencia	x					no
Control de avance silábico	x					no
Actas de notas	x					si
Rectificación de notas	x					no
Cursos dirigidos	x					no
Cursos paralelos	x					no
Ampliación de créditos	x					no

Proceso	Facultades	VRA	VRI	DIGA	Rector	Regulado
Asignación de docentes	x					no
Control de carga lectiva	x					no
Control de carga no lectiva	x					no
Control de documentos de docentes	x					no
Planes de trabajo individual	x					no
Proyectos de investigación	x					no
Informes trimestrales de investigación	x					no
Informes finales de investigación	x					no
Planificación del año académico		x				no
Planificación de los ciclos académicos		x				no
Gestión de las currículos		x				no
Registros académicos y archivos académicos		x				no
Procesos de educación a distancia		x				no
Reglamento de docentes		x				no
Reglamento de estudiantes		x				no
Convenios nacionales		x				no
Convenios internacionales		x				no
Centro Pre-Universitario		x				no
Unidad de Archivo General		x				si
Oficina de Bienestar Universitario		x				si
Oficina de Servicios Académicos		x				no
Oficina de Educación a Distancia		x				si
Oficina de Desarrollo Docente e Innovación		x				si
Centro de Idiomas		x				no
Dirección de Evaluación, Transferencia Tecnológica y Patentes - DETTP			x			no
Oficina de Gestión de la Investigación			x			si
Editorial Universitaria			x			no
Instituto Central de Investigación de Ciencia y Tecnología			x			si
Instituto de Investigación de Especialización en Agroindustria			x			no
Oficina de Capacitación VRI			x			no
Oficina de Recursos Humanos				x		si
Oficina de Tesorería				x		no
Oficina de Contabilidad y Presupuesto				x		si
Oficina de Abastecimientos y Servicios Auxiliares				x		si
Oficina de Infraestructura y Mantenimiento				x		no
Oficina de Gestión Patrimonial				x		no
Resoluciones					x	no
Oficina de Secretaría General					x	si
Oficina Asesoría Jurídica					x	si
Oficina de Tecnología de Información y Comunicación					x	si
Dirección Universitaria de Gestión y Aseguramiento de la Calidad					x	no
Oficina de Planificación y Presupuesto					x	si
Dirección Universitaria de Extensión y Responsabilidad Social (DUERS)					x	no
Oficina General de Admisión					x	si
Oficina de Relaciones Públicas e Imagen Institucional					x	no
Oficina de Cooperación Técnica Internacional					x	si

c) Evaluación del parque tecnológico en TI.

Se debe analizar el estado actual de la tecnología existente en la universidad, teniendo en cuenta que los desarrollos de aplicaciones de terceros junto con los propios pueden conllevar a la utilización de equipos que no sean compatible

o quizá ni siquiera continúan en operación y por consiguiente no se puedan integrar a las necesidades de la nube, asimismo es posible que muchos equipos no estén en condiciones de coexistir con la alta disponibilidad que ofrece la nube.

En el Cuadro 5.6 se hace un análisis del parque tecnológico actual de la UNAC.

Cuadro 5.6.
EVALUACIÓN DEL PARQUE TECNOLÓGICO DE LA UNAC

Tecnología	Descripción	Características	Compatibilidades con la nube
REDES			
Redunac	Red de la Oficina de Tecnología de la Información y Comunicaciones (OTIC)	Red de fibra óptica que cubre como backbone toda la ciudad universitaria de la UNAC	Compatible
Redes de las facultades	Red local en cada facultad	Red LAN con cableado alámbrico o con Wireless	Compatible
Red de la oficina de Registros y Archivos Académicos (ORA)	Red Local que soporta las actividades propias de ORA	Red LAN con cableado alámbrico o con Wireless	Compatible
Red del rectorado	Red Local que soporta las actividades propias de ORA	Red LAN con cableado alámbrico o con Wireless	Compatible
SOFTWARE			
Sistema operativo de la red OTIC	Software básico para el soporte de aplicaciones que utiliza OTIC	Linux	Compatible
Sistema operativo de ORA	Software básico para el soporte de aplicaciones que utiliza ORA	Linux	Compatible
Sistema operativo de las facultades	Software básico para el soporte de aplicaciones que utilizan las facultades	Linux y Windows	Compatible
Sistema de Gestión Académica	Software básico para la gestión académica	Open bravo software libre	Compatible
Sistema SIAF	Software básico para la gestión de logística con el estado	Sistema integrado de gestión financiera	No compatible
Sistema SIGA	Software básico para la gestión con el ministerio de economía y finanzas del gobierno	Sistema integrado de gestión administrativa	No compatible

d) Identificar qué modelo de servicio se ajusta a las necesidades.

Es crucial la elección del modelo de servicio a contratar cuidando que este alineado a los procesos; recordar que hay tres modelos que se pueden elegir: Software as a Service (SaaS), Infrastructure as a service (IaaS) o Platform as a Service (PaaS),

Más allá de la tecnología, la migración a la nube es una estrategia integral que contempla aspectos económicos, legales y tecnológicos con la finalidad de lograr productividad y competitividad de las organizaciones, para tener una capacidad de respuesta ágil frente las necesidades de los mercados actuales y futuros, teniendo en cuenta estos aspectos se debe hacer una adecuada elección del modelo de servicio a elegir.

Una vez comprendida la importancia de la información o aplicación que se desea migrar a la nube, corresponde evaluar las diferentes opciones de almacenamiento brindadas por la computación en la nube, teniendo presente las opciones de redundancia y capacidades de recuperación ofrecidas y asegurando que las mismas están alineadas con los requerimientos de la aplicación.

Luego, se debe evaluar el tipo de implementación que satisfaga sus necesidades, seleccionando entre nube pública, privada o híbrida.

En el Cuadro 5.7 se hace como ejemplo un análisis de la selección del servicio

Cuadro 5.7.
ANÁLISIS DE LA SELECCIÓN DEL SERVICIO

Proceso	IaaS	PaaS	SaaS
Matrícula	x	x	x
Registro de notas	x	x	
Programación académica	x	x	x
Registro de notas	x	x	x
Planes curriculares	x	x	x
Convalidaciones		x	x
Reservas de matriculas		x	x
Certificaciones	x	x	x
Resoluciones.	x	x	
Rectificación de matrícula		x	x
Matrícula especial		x	
Adecuación curricular		x	
Constancia para egresar	x		
Traslados internos	x	x	
Traslados externos	x	x	
Control de prácticas pre profesionales	x	x	x
Carga horaria		x	x
Cartas de presentación	x		
Control de asistencia		x	x
Control de avance silábico		x	x

Elegido el tipo de implementación se debe evaluar el modelo de servicio de nube a utilizar, seleccionando entre IaaS, PaaS o SaaS. Con base en las selecciones anteriores, la empresa podrá establecer cuáles roles y responsabilidades quedarán de su lado, cuáles del lado del proveedor y cuáles serán compartidas entre ambos, siempre desde el punto de vista de cumplimiento de controles de seguridad de la información.

En el Cuadro 5.8 se hace una selección de asignación de rol de responsabilidades según los procesos tanto al proveedor como al cliente.

Cuadro 5.8.
ASIGNACIÓN DE ROLES Y RESPONSABILIDADES DEL PROVEEDOR Y DEL CLIENTE

Proceso	Rol del Proveedor	Rol del Cliente
Matrícula	x	x
Registro de notas	x	x
Programación académica		x
Registro de notas	x	x
Planes curriculares		x
Convalidaciones		x
Reservas de matriculas		x
Certificaciones	x	x
Resoluciones.	x	x
Rectificación de matrícula		x
Matrícula especial		x
Adecuación curricular		x
Constancia para egresar	x	x
Traslados internos	x	x
Traslados externos	x	x
Control de prácticas pre profesionales	x	x
Carga horaria		x
Cartas de presentación	x	x
Control de asistencia		x
Control de avance silábico		x
Actas de notas	x	x
Rectificación de notas	x	x
Cursos dirigidos		x
Cursos paralelos		x
Ampliación de créditos		x
Asignación de docentes		x
Control de carga lectiva	x	x
Control de carga no lectiva	x	x
Control de documentos de docentes	x	
Planes de trabajo individual	x	x
Proyectos de investigación		x
Informes trimestrales de investigación		x
Informes finales de investigación		x
Control de inventarios	x	x
Compras	x	x
Resoluciones	x	x

e) Selección de proveedores

Determinado con precisión los tipos de servicios a contratar, la adopción de servicios en la nube precisa elegir bien a los proveedores, dentro de la gama posible de empresas que ofertan estos servicios. Las ofertas se diferencian no solo en costos, ver con cuidado los niveles de servicios y desempeño. Así, la decisión adecuada de la elección va a depender básicamente de estos factores, en

concordancia con la infraestructura física de la empresa, además de tener en cuenta la naturaleza de los aplicativos con los que cuenta la organización.

En el Cuadro 5.9 se hace un análisis para poder seleccionar los proveedores actuales que prestan servicios de computación en la nube

Cuadro 5.9.
ANÁLISIS DE LA SELECCIÓN DE PROVEEDORES PARA SELECCIONARLOS

Proveedor	Costo	Nivel de servicio	Desempeño
Amazon Web Services	Alto	A	Bueno
AT&T	Alto	A	Bueno
Google Cloud Storage	Alto	A	Bueno
HP	Alto	A	Bueno
IBM	Alto	A	Bueno
Internap	Medio	A	Regular
Microsoft	Medio	A	Regular
Nirvanix	Medio	A	Regular
Rackspace	Medio	B	Regular
Softlayer	Bajo	B	Regular
Drive	Bajo	B	Regular
Droboox	Bajo	B	Regular

f) Socializar el cambio.

Es importante preparar y capacitar a la fuerza laboral frente a la migración a esta nueva tecnología, es posible tener resistencia al cambio, lo cual es natural en las personas y muchas veces es debido al desconocimiento. Por tanto, resulta necesario comunicar a todas las áreas de la organización sobre las nuevas decisiones y además acompañar un calendario de actualización en la tecnología, haciendo talleres e incluso promover la certificación.

5.2.3 Etapa 3. Implementación en la nube.

Una vez abordadas todas las necesidades de la institución e identificados los requerimientos necesarios, es importante diseñar una estrategia técnica para implementar en la nube, esto debe considerarse como una vista de alto nivel, la cual puede ser luego materializada mediante una prueba de funcionalidad que permita verificar la funcionalidad más crítica de la solución en el nuevo ambiente, se recomienda seguir los siguientes pasos:

5.2.3.1 Creación de una máquina virtual

Coordinar con el proveedor la creación de una máquina virtual, esta creación se hace en coordinación con el proveedor del servicio, existen diversas máquinas virtuales en el mercado informático para elegir, se puede elegir por ejemplo la herramienta Oracle VM VirtualBox que es multiplataforma, compatible con Windows, macOS, Linux y Solaris, tiene herramientas para compartir archivos entre máquinas, permite crear instantáneas para restaurar el estado anterior de una VM fácilmente, cuenta con una herramienta de captura de vídeo y de pantalla y es compatible con el sistema operativo Ubuntu Server.

5.2.3.2 Instalación del sistema operativo

Para la instalación del sistema operativo se debe tener en cuenta ciertos criterios de performance que definen su elección, entre los criterios más

relevantes tenemos la estabilidad, la seguridad, el manejo de aplicaciones, flexibilidad, costos, comunidad, criterios que se describen a continuación.

Estabilidad: Una instalación típica puede correr durante años sin presentar fallas. puede manejar grandes cantidades de procesos no requiere reiniciar ante los cambios de configuración o luego de actualizaciones del sistema.

Seguridad: Capacidad de responder muy rápido ante los fallos y de preferencia contar con el código fuente disponible, de tal forma que cualquiera con los conocimientos necesarios puede corregir un fallo y ponerlo a disposición de los usuarios de inmediato.

Manejo de aplicaciones: Usa repositorios oficiales para sus aplicaciones, centralizando todo lo que podamos necesitar en un solo lugar.

Flexibilidad: Una instalación puede ajustarse tanto como sea necesario, instalando solo lo necesario.

Costos: El sistema operativo por el lado del cliente y la mayoría del software asociado que se usa debe ser de preferencia gratuito.

Comunidad: Es importante considerar que el sistema operativo cuente con una comunidad ya establecida que siempre está escuchando que

dicen y que necesitan sus usuarios.

Se puede elegir por ejemplo con estas características el sistema operativo Ubuntu Server.

5.2.3.3 Instalación de la aplicación de almacenamiento en la nube

Para facilitar la instalación de la aplicación de almacenamiento en la nube se debe usar un cliente adecuado por ejemplo se recomienda usar SSH PuTTY con el que podremos conectarnos remotamente al servidor Ubuntu. Además, se debe contar una aplicación de almacenamiento en la nube que cuente con almacenamiento de archivos con estructura de directorios convencionales, administración de usuarios y grupos, contar con el intercambio de contenidos a través de grupos o direcciones URL públicas, tener un editor de texto en línea con resaltado de sintaxis y plegado de códigos. Se recomienda por ejemplo ownCloud.

5.2.3.4 Despliegue de la aplicación de almacenamiento en la nube

En coordinación con el proveedor de servicios contratado por la modalidad de SaaS, se despliegan y luego se configuran las aplicaciones que soportan los procesos seleccionados para implementar en la nube, se procede luego a la carga real de la data de la universidad para probar el correcto funcionamiento de

las aplicaciones, solo después de haber hecho las pruebas suficientes se debe poner en producción las aplicaciones que darán soporte a los procesos migrados a la nube.

5.2.4 Etapa 4. Implementación de los controles.

La seguridad de información en la nube tiene que implementarse en todas las capas de la arquitectura de la aplicación de nube. La seguridad física corresponde gestionarla a su proveedor de servicios, la seguridad a nivel de red y de aplicaciones es responsabilidad de la universidad y se debe implementar según las políticas de seguridad establecidas.

Se recomienda lo siguiente:

a) Hacer la protección de los datos que van a estar en tránsito entre un navegador y un servidor WEB configurando un SSL en el servidor, usar un certificado externo que tenga una clave pública que autentique el servidor en el navegador y cifrar los datos en ambas direcciones.

b) Proteger los datos que no están en tránsito cifrando los datos y minimice el riesgo que supone no contar con las claves pues los datos pueden perderse para siempre.

c) Además de proteger sus datos de accesos no autorizados, se debe proteger los datos de los

desastres. Hacer pruebas periódicas de resistencia y disponibilidad.

d) Proteger las credenciales de seguridad como claves de acceso y certificados de seguridad.

e) Se deben proteger las aplicaciones con conjuntos de reglas con nombre que especifican qué tráfico de red de entrada debe trasladarse a su instancia. Podrá especificar puertos TCP y UDP, tipos y códigos ICMP y direcciones de origen.

f) Realizar secuencias de comandos de prueba, para poder ejecutar comprobaciones de seguridad de forma periódica y automatizar el proceso de ser posible.

g) Verificar que el software de otros fabricantes esté configurado con la configuración más segura.

h) Por ningún motivo ejecute los procesos usando el inicio de sesión root o administrador, salvo el caso que sea estrictamente necesario.

Después, se recomienda realizar un análisis de riesgos, donde se evalúan los diferentes escenarios ofrecidos por la nube.

En el Cuadro 5.10 se presenta una matriz donde se hace el análisis de riesgos asociados a los activos de información implementados en la nube.

Cuadro 5.10.
ANÁLISIS DE RIESGOS

Activo de in formación implementado en la nube	Amenaza	Vulnerabilidad	Posibilidad del riesgo	Niel de Impacto
Matrícula	Alta	Alta	Alta	Alta
Registro de notas	Alta	Alta	Alta	Alta
Programación académica	Baja	Alta	Alta	Alta
Planes curriculares	Baja	Alta	Alta	Media
Convalidaciones	Alta	Media	Media	Media
Reservas de matriculas	Baja	Media	Media	Media
Certificaciones	Media	Media	Media	Media
Resoluciones.	Media	Media	Media	Alta
Rectificación de matrícula	Media	Baja	Alta	Alta
Matrícula especial	Alta	Media	Alta	Alta
Adecuación curricular	Media	Media	Alta	Media
Constancia para egresar	Media	Alta	Media	Media
Traslados internos	Media	Alta	Baja	Media
Traslados externos	Media	Alta	Baja	Baja
Control de prácticas pre profesionales	Baja	Baja	Media	Baja
Carga horaria	Media	Media	Media	Media
Cartas de presentación	Baja	Media	Media	Media
Control de asistencia	Media	Media	Media	Media
Control de avance silábico	Media	Baja	Media	Media
Actas de notas	Alta	Baja	Media	Baja
Rectificación de notas	Alta	Baja	Media	Baja
Cursos dirigidos	Media	Baja	Media	Media
Cursos paralelos	Media	Media	Media	Media
Ampliación de créditos	Alta	Alta	Media	Media
Asignación de docentes	Media	Alta	Alta	Alta
Control de carga lectiva	Media	Alta	Alta	Alta
Control de carga no lectiva	Media	Alta	Alta	Alta
Control de documentos de docentes	Media	Media	Alta	Alta
Planes de trabajo individual	Media	Media	Media	Baja
Proyectos de investigación	Alta	Media	Media	Alta
Informes trimestrales de investigación	Media	Media	Media	Alta
Informes finales de investigación	Media	Media	Alta	Alta
Control de inventarios	Alta	Alta	Alta	Alta
Compras	Alta	Alta	Alta	Alta
Resoluciones	Alta	Alta	Alta	Alta

5.2.5 Etapa 5. Evaluación de los controles establecidos

Posteriormente se deben determinar las opciones de seguridad ofrecidas por el proveedor del servicio. Debido a las múltiples posibilidades entre modelos de implementación y modelos de servicios en la nube, la lista de controles de seguridad aplicables a cada uno de ellos es extensa. Quedará en manos de la universidad elegir cuáles son los controles de seguridad requeridos por la aplicación para su publicación en la nube. Entre algunos

de los requerimientos de seguridad que se deben evaluar con el proveedor, se encuentran el manejo de identidad y acceso, ciberamenazas, privacidad, regulaciones, disponibilidad, monitoreo, ciclo de desarrollo del *software* y capacitación del personal que dará mantenimiento a los servicios en la nube.

Como si se tratara de cualquier otra adquisición, al optar por un servicio en la nube, se debe verificar que los requerimientos tanto de la institución como de seguridad de la aplicación están cubiertos por Acuerdos de Nivel Servicios (Services Level Agree, SLA, por sus siglas en inglés).

Por lo general, los proveedores de servicios en la nube están en capacidad de realizar mayores inversiones en temas de seguridad, sobre las que podría realizar un cliente individualmente, ofreciendo un servicio de calidad. Así, por ejemplo, se mejora la disponibilidad de la información, distribuyendo la información en diferentes localidades geográficas, aumentando la redundancia de datos, brindando diferentes niveles de recuperación de desastres, por eso resulta sumamente necesario las coordinaciones y acuerdos con los proveedores para establecer un adecuado sistema de controles de seguridad de la información.

5.3 Niveles de madurez de los controles

Los controles que se implementan para prevenir los ataques a los activos de información en el proceso de mejora continua

dentro del circulo virtuoso de la calidad de Demming deben experimentar revisiones periódicas mejorando sus definiciones y estructuraciones de forma sistemática para lograr cada vez mejores performances en el objetivo de resguardar mejor los activos de información que corresponden a los procesos implementados en la nube. En la Figura 5.2, se muestra los diferentes niveles de madurez que deben alcanzar los controles de manera secuencial y su progreso sistemático se obtiene a medida que se implementan ciertas características adicionales en cada ciclo de mejora.

Figura 5.2.
MADUREZ DE LOS CONTROLES

1.- **inicial.** Los controles están establecidos atendiendo básicamente a las necesidades iniciales de resguardo de los activos de información

2. **Definido.** Están perfectamente establecidos todos los elementos del control y definidos los detalles de cada componente

3. **Formalizado**. Existen modelos que describen con precisión el funcionamiento de los controles y que permiten su simulación

4. **Sistematizado.** La implementación y gestión del control se visualiza como un sistema de gestión con actividades sistemáticamente establecidas.

5. **Automatizado.** Existen programas o software que permiten medir los indicadores de gestión de los controles

CAPITULO VI. DISCUSION DE RESULTADOS

2.1. Contrastación de hipótesis con los resultados

A la luz de los resultados obtenidos se afirma que se contrasta la hipótesis general planteada y las tres hipótesis específicas formuladas, la fundamentación se basa en lo siguiente:

- Efectivamente existe suficientes propuestas de buenas prácticas registradas en los normas y estándares internacionales para establecer controles que permitan resguardar adecuadamente los activos de información de los procesos implementados en la nube.

- Existen también normas para establecer aspectos contractuales que permiten definir los roles que deben desempeñar los proveedores de servicios en la nube y los clientes, estos criterios son nuevos dentro del diseño y desarrollo de sistemas y se justifica debido a la naturaleza propia del tema que se está estudiando.

- El diseño del sistema de gestión de seguridad de la información en la nube resulta implementado gracias a las recomendaciones obtenidas de los estándares de tanto para el diseño e implementación del sistema, así como de la seguridad

en la nube, logrando establecer con precisión cada una de las etapas del modelo de sistema propuesto.

- El modelo de mejora continua de Demming se consolida como una adecuada propuesta para la implementación gradual del sistema de gestión de seguridad en la nube. En cada ciclo de mejora se agregan nuevas funcionalidades del sistema o se da valor agregado a los subsistemas implementados.

- La propuesta de mejorar los controles en cada ciclo de mejora se ve acotada por el modelo de madurez que permite evaluar de manera concreta el estado del logro del objetivo de resguardar la información en la nube, permitiendo perfeccionar de manera sistemática las características que deben tener los controles a fin de lograr una mejor performance es decir un tipo de madurez de la salvaguarda establecida.

- Los proveedores de servicios de computación en la nube procuran seguir las recomendaciones de los estándares sobre computación en la nube y prestan sus servicios siguiendo estas propuestas.

- Los tipos de servicios de computación en la nube IaaS, PaaS, SaaS y la forma de desplegar la red ya sea pública, privada, hibrida permiten configurar adecuadamente el sistema de gestión de seguridad en la nube.

- El modelo propuesto para migrar los servicios a la nube de la universidad corrobora el uso de buenas prácticas de forma gradual y sistemática y permite la toma de decisiones para el

uso seguro y progresivo de los servicios brindados en la nube, tecnología que constantemente se consolida y madura para que las instituciones como las universitarias puedan disponer de estos servicios y lograr ahorros significativos en el uso tecnologías de información.

2.2. Contrastación de resultados con otros estudios similares.

Nos es posible contrastar los resultados obtenidos por otros estudios similares puesto que los estudios similares expuestos en los antecedentes tienen propósitos poco similares al presente estudio y por tanto resulta no adecuado la contratación de los resultados, resultado ser esta propuesta una innovación desde la perspectiva planteada.

CAPITULO VII. CONCLUSIONES

El sistema de gestión de la seguridad de la información se puede reconfigurar adecuadamente para abordar el problema de computación en la nube, mediante una adecuada estrategia de políticas y controles.

Las buenas practicas establecidas en los estándares tanto para la infraestructura de computación en la nube como para la seguridad en la nube permiten formular una serie de controles para resguardar la integridad, confidencialidad y disponibilidad de la información en la nube.

El análisis de los modelos de servicios de computación y de los tipos de servicios ofrecidos por los proveedores de computación en la nube sirven de base para formular un modelo de sistema de seguridad de la información en la nube.

Teniendo en cuenta el estado de la infraestructura y el sistema de gestión de la seguridad de la información de la Universidad Nacional del Callao, pudo corroborar el modelo de migración propuesto en el presente trabajo de investigación.

CAPITULO VIII. RECOMENDACIONES

Se propone realizar futuras investigaciones que puedan analizar más a fondo en la calidad y la disponibilidad de los servicios en la nube para lograr la atracción de los clientes hacia la implementación de la computación en la nube y desarrollan una mayor confianza del cliente.

Además, el desarrollo de un marco de seguridad completo y un sistema de gestión de la evaluación de la confianza es parte de los servicios de computación en la nube que satisfacen las demandas de seguridad es tarea de futuros trabajos.

Es de crucial importancia motivar a las instituciones universitarias y en especial a las entidades supervisoras que consideren el uso de la computación en la nube para lograr los beneficios que esta tecnología ofrece y permitir el ahorro de costos en tecnologías de información.

El uso del servicio de Software como Servicio SaaS, debe ser pensado como una alternativa para resolver la falta de laboratorios de cómputo para las especialidades de ingeniería que usen software de desarrollo o comercial con la ingeniería de sistemas o las escuelas de negocio.

REFERENCIAS BIBLIOGRAFICAS

1. Adamuthe, A. C., Salunkhe, V. D., Patil, S. H., & Thampi, G. (2015). Cloud Computing – A market Perspective and Research Directions. *Information Technology and Computer Science*, *10*(September), 42–53. https://doi.org/10.5815/ijitcs.2015.10.06
2. Adriano, E., & Lucrédio, D. (2012). Software Engineering for the Cloud : a Research Roadmap.
3. Angadi, A. B., Angadi, A. B., & Gull, K. C. (2013). Security Issues with Possible Solutions in Cloud Computing-A Survey. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *2*(2).
4. Anjali, J., & Pandey, U. (2013). Role of cloud computing in higher education. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(7), 966–972.
5. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Stoica, I. (2010). A view of Cloud Computing. *Comunications of the ACM*, *53*(4).
6. Chiregi, M., & Navimipour, N. J. (2017). Cloud computing and trust evaluation : A systematic literature review of the state-of-the-art mechanisms. *Journal of Electrical Systems and Information Technology*. https://doi.org/10.1016/j.jesit.2017.09.001
7. Chowdhury, R. R. (2014). Security in Cloud Computing. *International Journal of Computer Applications*, *96*(15), 24–30.

8. Cloud -Customer- Standards, C. (2017). Practical Guide to Cloud Computing. *Cloud Standars Customer Council*.
9. Cloud Security Alliance. (2010). Top Threats to Cloud Computing v1.0, (March), 1–14.
10. Comput, J. P. D., Assunção, M. D., Calheiros, R. N., Bianchi, S., Netto, M. A. S., & Buyya, R. (2015). Big Data computing and clouds : Trends and future directions. *J. Parallel Distrib. Comput.*, *79–80*, 3–15. https://doi.org/10.1016/j.jpdc.2014.08.003
11. Devi, T., & Ganesan, R. (2015). Platform-as-a-Service (PaaS): Model and Security Issues. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, *15*(1), 151–161. https://doi.org/10.11591/telkomnika.v15i1.8073
12. ENISA. (2012). *Cloud Computing Benefits , risks and recommendations for information security*.
13. Erl, T., Mahmood, Z., & Puttini, R. (2013). *Cloud Computing*.
14. Fernández Aller, C. (2012). Algunos retos de protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en la nube (CLOUD COMPUTING). *Revista de Derecho UNED*, *10*, 125–146.
15. Furht, B., & Escalante, A. (2010). *Handbook of Cloud Computing*.
16. Gholami, A., & Laure, E. (2015). Security and privacy of sensitive data in cloud computing : a survey of recent developments. *CSEIT,SPM*, 131–150.
17. Hepsiba, C. L., & Sathiaseelan, J. G. R. (2016). Security Issues in Service Models of Cloud Computing. *International Journal of Computer Science and Mobile Computing*, *5*(3), 610–615.
18. ISACA. (2009). *Cloud Computing : Business Benefits With Security , Governance and Assurance Perspectives*.

19. Jara Collahuazo, J. A. (2012). *Guía para el análisis de factibilidad en la implantación de tecnologías de cloud computing en empresas del Ecuador*.
20. Joyanes Aguilar, L. (2009). La Computación en Nube (Cloud Computing) : El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento. *Icade, Revista Cuatrimestral de La Facultad de Derecho Y Ciencias Económicas Y Empresariales*, *76*, 95–112.
21. Kalpana, G., Kumar, P. V, & Krishnaiah, R. V. (2015). A brief Survey on Security Issues in Cloud and its service models. *International Journal of Advanced Research in Computer and Communication Engineering*, *4*(6), 457–463. https://doi.org/10.17148/IJARCCE.2015.4698
22. Kwame, P., Addae, E., & Boateng, R. (2018). Cloud computing research : A review of research themes , frameworks , methods and future research directions. *International Journal of Information Management*, *38*(1), 128–139. https://doi.org/10.1016/j.ijinfomgt.2017.07.007
23. Malik, V., Gupta, S., & Kaushik, J. (2014). Network Security : Security in Cloud Computing. *International Journal of Engineering and Computer Science*, *3*(1), 3643–3651.
24. Martinez, P. (1961). Cloud Computing.
25. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *800-145*.
26. Mell, P., Grance, T., & Grance, T. (2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*.
27. Munyaka, D., Yenchik, A., & Durham, S. (2012). Cloud Computing Security. *Research Paper for Telecomunications Management*.

28. Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud Computing Environment and Security Challenges : A Review. *(IJACSA) International Journal of Advanced Computer Science and Applications*, *8*(10), 183–195.
29. Muthakshi, S., & Meyyappan, T. (2013). A Survey on Security Services In Cloud Computing. *International Journal of Engineering Tends and Technology (IJETT)*, *4*(July), 2785–2788.
30. Pallis, G. (2010). Cloud Computing: The New Frontier of Internet Computing. *IEEE Internet Computing*.
31. Radu, L. (2017). Green Cloud Computing : A Literature Survey. *SS Symmetry*, *9*, 295. https://doi.org/10.3390/sym9120295
32. Rao, R. V., & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015)*, *48*(Iccc), 204–209. https://doi.org/10.1016/j.procs.2015.04.171
33. Rodas Orellana, F. J., Cruz, T., & Elizabet, D. (2015). *Propuesta de un Modelo de Gestión de Servicios de Tecnologías de Información y Comunicación en la Nube (Cloud Computing) para Universidades* (Master's thesis, Quito, 2015.).
34. Rot, A. (2017). Selected Issues of IT Risk Management in the Cloud Computing Model . Theory and Practice. In *Proceedings of The 8th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2017)* (pp. 89–94).
35. Saggi, M. K., & Bhatia, A. S. (2015). A Review on Mobile Cloud Computing : Issues , Challenges and Solutions.

International Journal of Advanced Research in Computer and Comunications Engineering, *4*(6), 29–34. https://doi.org/10.17148/IJARCCE.2015.4608

36. Shawish, A., & Salama, M. (2014). Cloud Computing : Paradigms and Technologies. *Studies in Computacional Intelligence*, 39–68. https://doi.org/10.1007/978-3-642-35016-0
37. Shojaiemehr, B., Masoud, A., & Nasih, N. (2018). Cloud computing service negotiation : A systematic review. *Computer Standards & Interfaces*, *55*(February 2017), 196–206. https://doi.org/10.1016/j.csi.2017.08.006
38. Singh, M., Sheng, Q. Z., & Casati, F. (2017). A Service Computing Manifesto : The Next 10 Years. *Comunications of the ACM*, *60*(4), 72.
39. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006
40. Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and Analyzing Security , Privacy and Trust Issues in Cloud Computing Environments. *Advanced in Control Engineering and Information Science*, *15*, 2852–2856. https://doi.org/10.1016/j.proeng.2011.08.537
41. Varghese, B., & Buyya, R. (2017). Next generation cloud computing : New trends and research directions. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.09.020
42. Vasuyadav1, D., & KrishnaReddy, V. (2017). A survey of issues in cloud computing. *International Journal of Pure and Applied Mathematics*, *115*(8), 253–258.

43. Veeramachaneni, V. K. (2015). Security Issues and Countermeasures in Cloud Computing Environment. *International Journal of Engineering Science and Innovative Technology (IJESIT)*, *4*(5), 82–93.
44. View, G., & Heng, S. (2014). Cloud Computing : Clear Skies Ahead. *E-Conomics Cloud Computing*, (June), 0–20.
45. Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences*, *258*, 371–386. https://doi.org/10.1016/j.ins.2013.04.028
46. Yogamangalam, R., & Shankar, S. (2013). A review on Security Issues in Cloud Computing.
47. Zaghloul, E., Zhou, K., Ren, J., & Jan, C. R. (2018). P-MOD : Secure Privilege-Based Multilevel Organizational Data-Sharing in Cloud Computing.
48. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

ANEXOS

ANEXO A: MATRIZ DE CONSISTENCIA

Problema	Objetivos	Hipótesis	Variables	Dimensiones	Indicadores
Problema general ¿Es posible crear una estrategia que permita la implementación exitosa de un sistema de gestión de seguridad de la información en la nube adecuado para una institución universitaria, basado en buenas prácticas informáticas? **Problemas específicos** **Problema específico 1**. ¿Cómo establecer los criterios para la migración adecuada de los procesos de gestión de una universidad a servicios prestados en la nube? **Problema específico 2.** ¿Cómo seleccionar el tipo de red y de servicio adecuado para la migración de procesos universitarios a la nube?	**Objetivo general** Crear un modelo para implementar y/o migrar a la nube un sistema de gestión de la seguridad de la Información para una universidad pública basándose en criterios propuestos por los estándares de seguridad de la información en la nube y contrastarlo en universidad Nacional del Callao. **Objetivos específicos** **OE1**. Establecer los criterios que se deben considerar para migrar los procesos universitarios a los servicios de computación en la nube. **OE2**. Evaluar las propuestas de los modelos de redes en la nube, así como los tipos de servicios ofrecidos por los	**Hipótesis general** La implantación adecuada de controles para seguridad de la información en la nube basada en estándares internacionales garantiza la implementación de un adecuado sistema de gestión seguridad de información en la nube para una institución universitaria. **Hipótesis específicas** **Hipótesis específica 1**. Los aspectos legales y las políticas de seguridad de la institución universitaria permiten definir que procesos de gestión se pueden migrar a la nube y cuales no deben ser implementados para no trasgredir la normatividad. **Hipótesis específica 2.** Basado en las buenas prácticas de los estándares internacionales que hacen referencia a los modelos de	**Variable dependiente.** *Sistema de gestión de seguridad de la información en la nube para una universidad.* Constituido por un conjunto de controles organizados según políticas de seguridad de la información para lograr el resguardo de los activos de información que son migrados a los servicios de computación en la nube.	**P**olíticas de seguridad de la información. Responsables de la seguridad de la información. **C**ontroles establecidos para el resguardo de activos. **O**rganización para la seguridad de la información. **P**lanes de contingencia. **R**elaciones contractuales con los proveedores de servicios en la nube. **R**oles y responsabilidades asumidas por la organización y compartidas con el proveedor de servicios.	**N**umero de políticas sobre seguridad de la información establecidas. **N**úmero de reuniones del comité de seguridad de información de la institución. **V**eces de actualizaciones del organigrama de la organización para considerar la seguridad de la información. **P**orcentaje del riesgo asumido **P**orcentaje del riesgo residual **N**umero de planes de contingencia **R**eportes de incidencias de violaciones a la seguridad de la información en la nube. **N**umero de revisiones de los aspectos contractuales con los proveedores de servicios.

Problema	Objetivos	Hipótesis	Variables	Dimensiones	Indicadores
Problema específico 3. ¿Cómo implementar la arquitectura en la nube para soportar los procesos universitarios que se deciden migrar a la nube?	proveedores de servicios en la nube. **OE3.** Seleccionar propuestas para implementar la arquitectura en la nube que soporte la migración de procesos universitarios a redes y servicios en la nube.	nubes y los tipos de servicios ofrecidos por los diversos proveedores se puede seleccionar el modelo de red y tipo de servicio para garantizar la preservación de la seguridad de la información en la nube. **Hipótesis específica 3**. Una adecuada evaluación de proveedores de servicio en la nube y tomando como referencia el modelo de red elegido y el tipo de servicio elegido mediante acuerdos contractuales se puede construir la arquitectura que soporte los procesos elegidos para migrar a la nube.	**Variable independiente.** *Normatividad de Seguridad de la información en la nube.* Está formada por las buenas prácticas de seguridad en la nube que son acopiadas en los expertos en el tema y plasmadas en las diferentes normas que son patrocinadas por organismos reguladores internacionales. Variable independiente: Normatividad de Seguridad de la información en la nube	**A**ctivos de información de la institución. **V**ulnerabilidades que presentan los sistemas. **A**menazas a las que están expuestos los activos de información. **R**iesgo de que las amenazas se cristalicen a través de las vulnerabilidades y afecten los activos de información. **I**mpacto del riesgo	**N**úmero de veces de actualización del inventario de activos de información. **N**úmero de veces de actualización de la identificación de amenazas a los activos de información. **A**ctualizaciones de las vulnerabilidades **M**atriz de riesgo que relacione las amenazas, su probabilidad de ocurrencia y el impacto

ANEXO B: ORGANIGRAMA DE LA UNAC