UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Científica
http://revistas.udistrital.edu.co/ojs/index.php/revcie/index

CIDC

Arquitectura de seguridad de un entorno computacional para eCiencia en la nube

Security architecture of a computing environment for eScience

Arquitetura de segurança de um ambiente de computação em nuvem para eCiência

José Nelson Pérez [1]
Fabrizio Bolaño López[2]
Nubia Rincón Mosquera[3]

Resumen

La computación en nube es un paradigma donde los recursos tecnológicos se distribuyen globalmente y la información se almacena internet, permitiendo un acceso hasta hace poco impensable a servicios por medio del pago por consumo. Este nuevo paradigma ha fortalecido nuevas tendencias tales como la E-ciencia. El mayor desafío en estas tendencias de E-ciencia sobre plataformas privadas de computación en la nube son los problemas de seguridad y privacidad causados por su naturaleza multi-usuario y procesos de virtualización. En este trabajo colaborativo se pueden presentar intrusiones, daños irreparables o accesos ilegales a datos críticos y confidenciales de los usuarios del ecosistema académico e investigativo. El presente trabajo, aplicado para el CECAD de la UDFJC de Bogotá, propone la especificación de un modelo arquitectural de seguridad que permita a las organizaciones que deseen abordar proyectos de nube privada, fortalecer la seguridad y minimizar los riesgos de exposición que estas debilidades conllevan.

Palabras Clave:
Cloud Computing, Seguridad, Arquitectura, Modelo, E-Ciencia.

Abstract

Cloud computing is a paradigm where technological resources are distributed globally and internet information is stored, allowing access until recently unthinkable services by paying for consumption. This new paradigm has strengthened new trends such as E-science. The biggest challenge in these trends E-science platforms on private cloud computing are security and privacy problems caused by its multi-tenant nature and processes of virtualization. In this collaborative work may occur intrusions, irreparable damage or illegal access to sensitive and critical users of academic and research ecosystem data. This work, applied for CECAD of UDFJC Bogotá, proposes specifying an architectural security

[1] Universidad Distrital Francisco José de Caldas, Bogotá-Colombia. Contacto: jnperezc@correo.udistrital.edu.co
[2] Universidad Distrital Francisco José de Caldas, Bogotá-Colombia. Contacto: fabriziobolano@gmail.com
[3] Universidad Distrital Francisco José de Caldas, Bogotá-Colombia. Contacto: nubiabioing@yahoo.com

model that allows organizations wishing to undertake projects of private cloud, strengthen security and minimize risk exposure that these weaknesses involved.
Keywords:
Cloud Computing, Security, Architecture, Model, E-Science.

Resumo
A computação em nuvem é um paradigma onde os recursos tecnológicos são distribuídos globalmente e informações de internet são armazenados, permitindo o acesso até que os serviços recentemente impensáveis, pagando para consumo. Este novo paradigma tem fortalecido as novas tendências, tais como E-ciência. O maior desafio nessas plataformas tendências e-Ciência sobre computação em nuvem privada são problemas de segurança e privacidade causados por sua natureza multi-utilizador e processos de virtualização. Neste trabalho colaborativo podem ocorrer intrusões, danos irreparáveis ou acesso ilegal a usuários sensíveis e críticas de dados sobre o ecossistema acadêmicas e de pesquisa. Este trabalho, aplicada para CECAD de UDFJC Bogotá, propõe a especificação de um modelo de segurança de arquitetura que permite que as organizações que desejam realizar projetos de nuvem privada, reforçar a segurança e minimizar a exposição ao risco que estas deficiências envolvidos.
Palavras-chave:
Cloud Computing, Segurança, Arquitectura, Modelo, E-Science.

INTRODUCCIÓN

La computación en nube es una tendencia actual y una de las mejores soluciones del gasto del presupuesto excesivo para muchas organizaciones de configuración de TI. Con Cloud Computing las organizaciones entiendan la manera de maximizar los beneficios y minimizar riesgos llevar sus procesos(Balu & Mary).

La nube privada es un modelo o arquitectura (Smoot & Tan, 2012) y, a menudo presentada como la solución para todos sus problemas informáticos en el sector de las empresas. Es muy cercano al modelo más tradicional de las redes de acceso individuales locales (LAN) que se utilizaron en el pasado por la empresa, pero que tienen ventajas adicionales tales como la virtualización, aplicaciones como servicios, alta disponibilidad, etc.

Aunque la nube introduce el concepto innovador y rentable de la demanda en el servicio, a pagar a medida que avanza, y la asignación de recursos, la seguridad es a menudo el área de preocupación en cuanto a su adopción. Las soluciones basadas en la seguridad existentes para plataformas basada en la nube se soportan ya sea en hardware a prueba de manipulaciones simple o encriptación. La solución basada en hardware carece de capacidad de ampliación, mientras que los cifrados para cocientes son una teoría difícil de implementar. Por otra parte, la tradicional defensa en mecanismo de seguridad no se puede implementar directamente en la plataforma basada en la nube debido a la naturaleza variable de su servicio y modelo de implementación (Gallego, 2014).

Particularmente para la Universidad Distrital Francisco Jose de Caldas y su Centro de Computación de Alto Desempeño (CECAD) cuyo objetivo y destinación principal es el apoyo al fortalecimiento de las actividades académicas, investigativas y colaborativas de E-Ciencia, se tiene las siguientes preocupaciones y/o consideraciones de seguridad, así:

1. Seguridad en el acceso y protección de identidad.
2. Confidencialidad de los datos e información de los docentes e investigadores que usan la plataforma.
3. Protección de la información contra ataques externos e internos.
4. Alta disponibilidad de la información con esquemas seguros.

El objetivo principal del presente documento, es proporcionar un Modelo Arquitectural que permita establecer un esquema de seguridad a la nube privada del CECAD de la Universidad Distrital Francisco Jose de Caldas destinada a actividades de E-Ciencia.

MARCO TEÓRICO

Los principales objetivos de una nube privada son:

- Utilización de servicios ajustada a los requerimientos del negocio.
- Provisión de auto-servicio que permite el acceso a la información y aplicaciones en cualquier momento (24 horas en un día / 7 días a la semana) y desde cualquier lugar (a nivel mundial).
- De acuerdo con el negocio y la demanda del sistema, los servicios serán automatizados, con aprovisionamiento elástico. Esto puede ser también llamado como "la agrupación de recursos". Esto significa que el servicio estará disponible a los diferentes usuarios mediante un modelo multi-usuarios.

Particularmente para el CECAD de la Universidad Distrital Francisco José de Caldas, actualmente se cuenta con una demanda considerable de docentes de pregrado y postgrado, así como investigadores asociados a los diferentes grupos de la universidad, quienes puedan estar en diferentes partes del país o en locaciones internacionales. Esta pluralidad de usuarios exige cada vez más que se implementen procedimientos, programas y proyectos con el fin de fortalecer la seguridad del ecosistema de E-Ciencia (Camargo et al, 2015).

Arquitectura Cloud Privada para E-Ciencia – CECAD - UDFJC

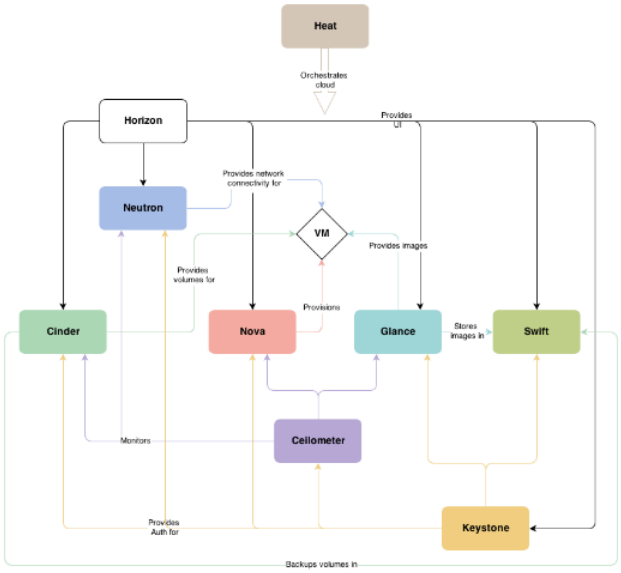
La actual nube privada del CECAD – UDFJC está diseñada sobre OpenStack. OpenStack es un proyecto de computación en la nube para proporcionar una infraestructura como servicio (IaaS)(Rosado & Bernardino, 2014). Es un software libre y de código abierto distribuido bajo los términos de la licencia Apache, desarrollados originalmente por la NASA y Rackspace, habiendo ganado hasta ahora tales robustez y fiabilidad tanto para las infraestructuras cloud públicas y privadas (del Castillo, Mallichan, & Al-Hazmi, 2013).

Su arquitectura modular y altamente configurable permite a esta solución adaptar los recursos de hardware disponibles para dar respuesta a cada caso en particular.

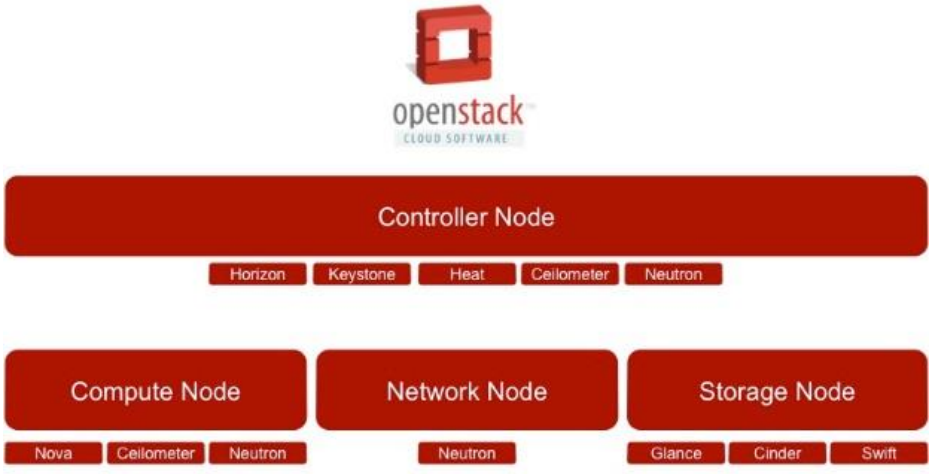
Esto permite a las empresas elegir entre una variedad de servicios complementarios con el fin de satisfacer las diferentes necesidades en cuanto a la computación, redes y almacenamiento.

La siguiente figura representa la arquitectura conceptual Openstack con todos los componentes de software nativas.

Fuente: https://www.openstack.org/



Fuente: https://www.openstack.org/



Componentes de Seguridad de OpenStack

OpenStack combina diferentes componentes para fortalecer la seguridad, tal es el caso de Keystone. Keystone proporciona un único punto de integración de la identidad de OpenStack, ficha, catálogo y Servicios de política para los diferentes proyectos que se implementen sobre ella.

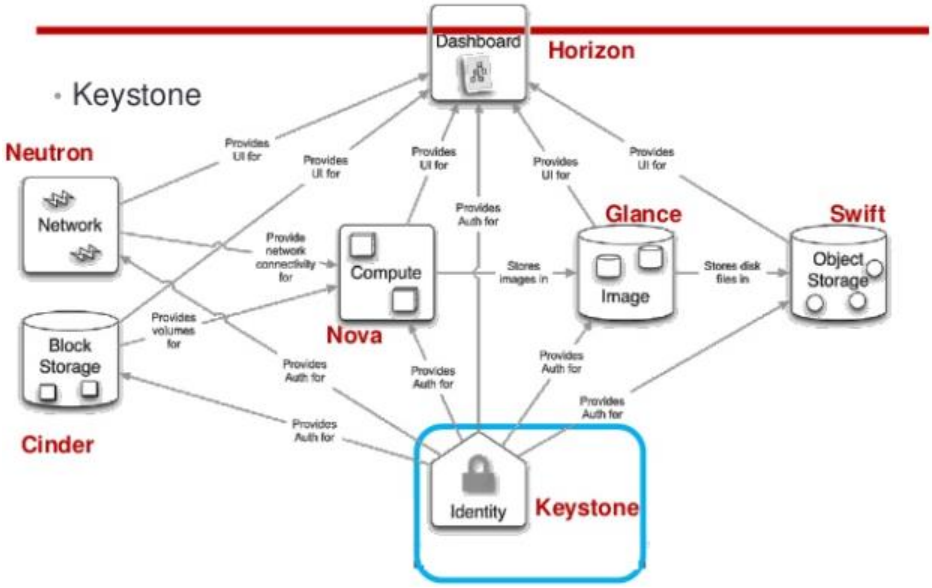
Keystone tiene muchos componentes que ayudan a modelar la arquitectura segura para construir una nube privada.

Hay dos funciones principales que se pueden conseguir mediante el uso de KeyStone:

- Gestión de usuarios - pistas de usuario y su ámbito de seguridad en el que se les permite hacerlo.
- Catálogo de Servicios - ofrece un catálogo de qué servicios pueden estar disponibles para el usuario.

En la siguiente gráfica se muestra el componente KeyStone asociado a OpenStack:

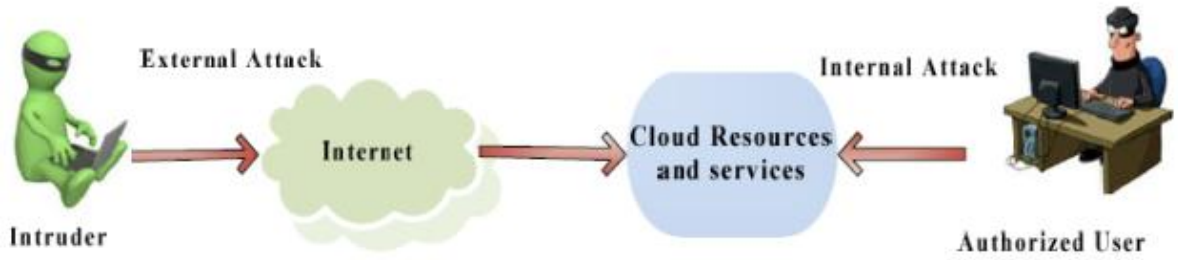
Fuente: http://docs.openstack.org/developer/keystone/



Principales problemas de seguridad en los modelos de servicios en Cloud Computing

Garantizar la seguridad de los datos corporativos en la "nube" es muy difícil, ya que ofrecen diferentes servicios como SaaS, PaaS, IaaS y cada servicio tiene sus propios problemas de seguridad (Bhadauria & Sanyal, 2012).

Los diferentes actores de la nube se enfrentan a dos tipos de amenazas a la seguridad a través de; ataques externos e internos.



Fuente:(Munir & Palaniappan, 2013)

Los ataques externos en la nube están aumentando a un ritmo notable. Usuarios maliciosos que se encuentran por fuera de la nube realizan a menudo ataques de Denegación de Servicio (DoS) con el fin de afectar a la disponibilidad de servicios y recursos de la nube. Escaneo de puertos, IP spoofing, envenenamiento de DNS y phishing también se ejecutan para ganar acceso a los recursos de la nube. Un usuario malintencionado puede capturar y analizar los datos de los paquetes enviados a través de esta red mediante técnicas de sniffing (Munir & Palaniappan, 2013).

IP spoofing ocurre cuando un usuario malicioso se hace pasar por una dirección IP de los usuarios legítimos donde pudieran acceder a información que no habrían sido capaces de acceder de otra manera. La disponibilidad es una característica muy importante y para un usuario final, el no tener acceso a los servicios cuando sea necesario puede ser un desastre, especialmente en el caso de denegación de servicio. Esta denegación puede ocurrir cuando el sobreprocesamiento de los servidores hace que las solicitudes de los consumidores legítimos sean negadas. Esto puede costarle a una empresa grandes pérdidas de dinero y tiempo si los servicios de los que dependen para operar no están disponibles.

METODOLOGÍA

Modelo Arquitectural de Seguridad para la plataforma integrada del proyecto de nube privada (CECAD) con fines de E-Ciencia de la UDFJC

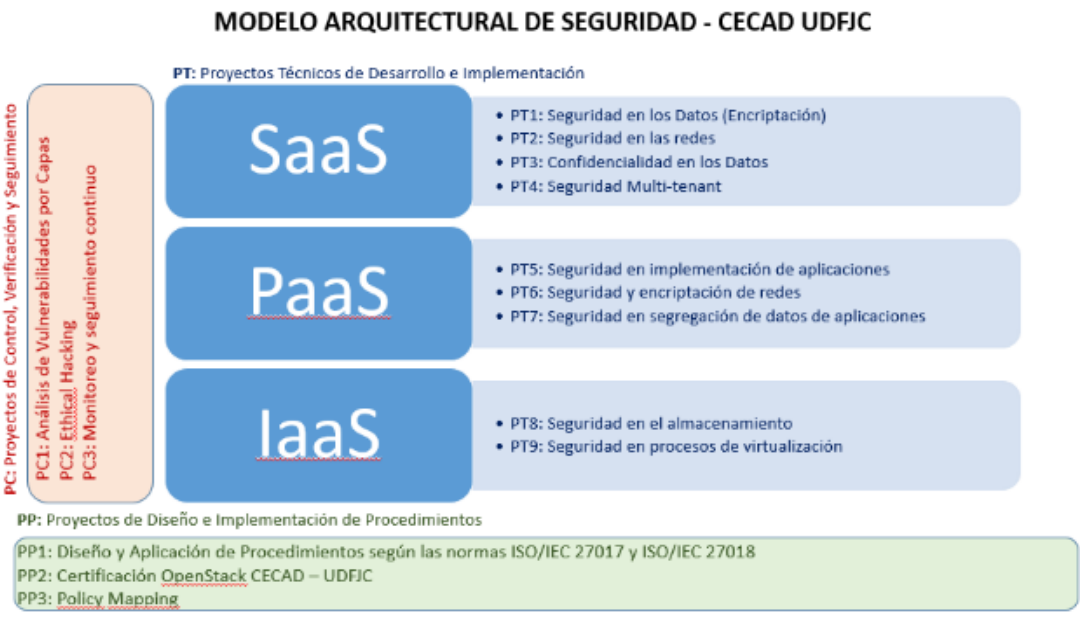
Una vez realizado el análisis de los elementos de riesgos y vulnerabilidades de seguridad del CECAD y el estado actual de la plataforma de nube privada bajo OpenStack, se procedió a generar y describir un Modelo Arquitectural de Seguridad que permita fortalecer la seguridad en los entornos de nube privada y así minimizar los riesgos de exposición que estas debilidades conllevan, en especial las derivadas de la interacción de los procesos académicos, investigativos, y colaborativos del CECAD.

El Modelo Arquitectural Propuesto, fue acompañado de un portafolio de programas y proyectos que se deben implementar en un corto plazo con el fin de materializar los elementos de seguridad y así minimizar los riesgos y cerrar las posibles brecas de vulnerabilidades a que se enfrenta la plataforma (Camargo et al, 2015).

RESULTADOS

La siguiente figura muestra el Modelo Arquitectural de Seguridad propuesto para implementar en el Centro de Computación de Alto Desempeño (CECAD) de la Universidad Distrital Francisco Jose de Caldas.

Fuente: Los Autores



Descripción del Modelo:

Proyectos de Implementación de Procedimientos y Buenas Prácticas - PP:

Dentro de este tópico, se estructurarán todas las estrategias y proyectos relacionados con la implementación y/o adopción de políticas, estándares, normas y buenas prácticas relacionadas las temáticas de seguridad para proyectos de nube privada y desarrollos de entornos de E-Ciencia.

En este tópico también se diseñarán y ejecutarán planes de capacitación tanto para actores internos como externos, así como para el personal técnico que administra el proyecto, asegurando así la sostenibilidad a través del tiempo (Millán y Pérez, 2014).

Su principal objetivo es consolidar procedimientos de buenas prácticas y estándares internacionales para adoptar controles de seguridad de alta calidad que respondan a los desafíos actuales a los que se enfrentan los entornos de nube privada como los que hoy se llevan en el CECAD.

Los proyectos modelados para esta estrategia son:

- PP1: Diseño y Aplicación de Procedimientos según las normas ISO/IEC 27017 y ISO/IEC 27018
- PP2: Certificación OpenStack CECAD – UDFJC
- Políticas de Mapeo

Proyectos de Control Verificación y Seguimiento - PC:

Dentro de este tópico, se estructurarán todas las estrategias relacionadas con la implementación transversal de proyectos que permitan realizar un continuo control y seguimiento de las diferentes actividades del proyecto de nube privada (Pérez et al, 2015).

En este tópico también se diseñarán planes de mejora continua a través de la aplicación y realimentación de indicadores y de elementos claves de éxito.

Su principal objetivo es identificar y estructurar herramientas y componentes para realizar seguimiento, control y seguimiento de los procesos de E-Ciencia, así como de los procesos administrativos de la plataforma de nube privada (Tolosa y González, 2015) .

Los proyectos modelados para esta estrategia son:

- PC1: Análisis de Vulnerabilidades por Capas
- PC2: Hackeo Ético
- PC3: Monitoreo y seguimiento continuo

Proyectos Técnicos de Desarrollo e Implementación – PT:

Dentro de este tópico, se estructurarán todas las estrategias relacionadas con la implementación transversal de proyectos de índole técnico que permitirán acortar las posibles brechas de seguridad en los diferentes niveles de la plataforma, así como minimizar los posibles riesgos que por su naturaleza enfrenta una plataforma de nube privada con fines de E-Ciencia.

En este tópico también se diseñarán planes de revisión de tecnologías y/o tendencias actuales con el fin de evaluar la decisión de comprar o desarrollar los diferentes componentes a utilizar.

Los proyectos modelados para esta estrategia son:

- PT1: Seguridad en los Datos (Encriptación)
- PT2: Seguridad en las redes
- PT3: Confidencialidad en los Datos
- PT4: Seguridad Multi-usuarios
- PT5: Seguridad en implementación de aplicaciones
- PT6: Seguridad y encriptación de redes
- PT7: Seguridad en segregación de datos de aplicaciones
- PT8: Seguridad en el almacenamiento
- PT9: Seguridad en procesos de virtualización

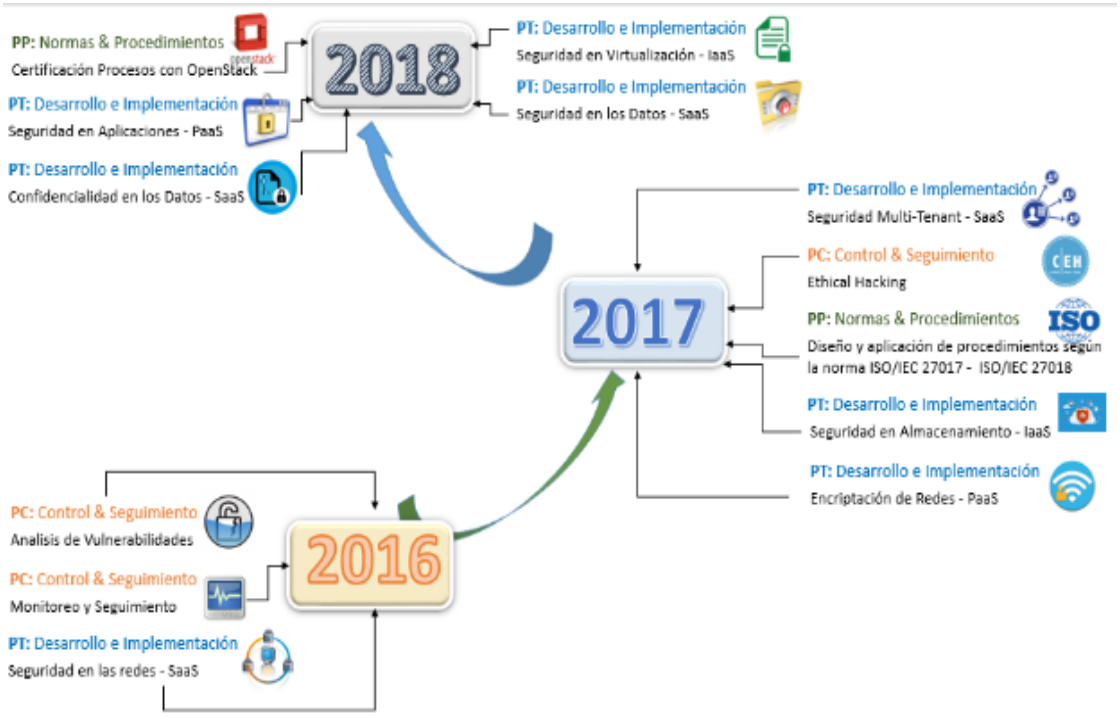
Con la implementación de estos proyectos se busca responder y minimizar los siguientes tipos de amenazas:

- Las fallas de inyección como SQL, OS y la inyección LDAP
- Secuencias de órdenes en sitios cruzados
- Autentificación y Gestión de Sesiones
- Inseguras referencias a objetos directos
- Falsificación de solicitudes
- Mala configuración de seguridad
- Almacenamiento criptográfico inseguro

Mapa de Ruta de Implementación:

La siguiente gráfica muestra el mapa de ruta sugerido para la implementación de portafolio de programa y proyectos del Modelo Arquitectural de Seguridad de la plataforma de nube privada con fines de E-ciencia de la UDFJC.

Fuente: Los Autores



CONCLUSIONES

El portafolio de programas y proyectos descritos anteriormente en el Modelo Arquitectural de Seguridad de la Plataforma de Nube Privada, responde a las exigencias de seguridad que demanda una nube privada con fines de E-Ciencia.

Los proyectos técnicos seleccionados para implementar están directamente alineados para contrarrestar las principales amenazas y brechas de seguridad.

La adopción de buenas prácticas y estándares internacionales responde a las debilidades detectadas en el CECAD, tanto técnicas como administrativas.

REFERENCIAS BIBLIOGRÁFICAS

Balu, V., & Mary, L. J. A Model of Security Architecture on Private Cloud Using OpenStack.

Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques. https://doi.org/10.5120/7292-0578

Camargo Vega, J. , Camargo Ortega, J., & Joyanes Aguilar, L. . (2015). Arquitectura Tecnológica Para Big Data. *Revista Científica*, *21*, 7-18. https://doi.org/10.14483/udistrital.jour.RC.2015.21.a1

Camargo-Vega, J. J., Camargo-Ortega, J. F., & Joyanes-Aguilar, L. (2015). Arquitectura Tecnológica Para Big Data-Technological Architecture For Big Data. Revista científica, 1(21), 7-18. https://doi.org/10.14483/udistrital.jour.RC.2015.21.a1

del Castillo, J. A. L., Mallichan, K., & Al-Hazmi, Y. (2013). Openstack federation in experimentation multi-cloud testbeds. Paper presented at the Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on. https://doi.org/10.1109/CloudCom.2013.103

Gallego-Torres, A. P. (2014). Relaciones ciencia, ingeniería, sociedad y ambiente-Science, Engineering, Society and Environment Relations. Revista científica, 2(19), 6-7. https://doi.org/10.14483/23448350.6488

Millán-Rojas, E. E., & Pérez-Castillo, J. N. (2014). Servicio Amazon Web Services de clasificación primaria de imágenes de fuentes hídricas del piedemonte amazónico que usan redes neuronales. *Revista Científica*, 2(19), 104-117. https://doi.org/10.14483/23448350.6498

Munir, K., & Palaniappan, S. (2013). Secure cloud architecture. Advanced Computing, 4(1), 9. https://doi.org/10.5121/acij.2013.4102

Pérez-Castillo, J. N., Díaz-Hernández, M. F., & Rincón-Mosquera, N. (2015). Web semántica y su aporte a la estrategia de datos abiertos del Estado Colombiano. Revista científica, 3(23), 124-132. https://doi.org/10.14483/23448350.9796

Rosado, T., & Bernardino, J. (2014). An overview of openstack architecture. Paper presented at the Proceedings of the 18th International Database Engineering & Applications Symposium. https://doi.org/10.1145/2628194.2628195

Smoot, S. R., & Tan, N.-K. (2012). Private cloud computing: consolidation, virtualization, and service-oriented infrastructure: Elsevier.

Tolosa-Cuadrado, C. L., & González-Sanabria, J. S. (2014). Amazon Web Services: alternativa para el almacenamiento de información. *Revista Científica*, 2(19), 134-147. https://doi.org/10.14483/23448350.6500