UNIVERSIDAD AMAZÓNICA DE PANDO

ÁREA DE CIENCIAS Y TECNOLOGÍA

CARRERA DE INGENIERÍA DE SISTEMAS

PROYECTO DE GRADO

"SISTEMA DE SEGURIDAD COMO MODELO EN EL GESTOR DE BASE DE DATOS SIRINGUERO DE LA UNIVERSIDAD AMAZÓNICA DE PANDO"

PROYECTO DE GRADO PRESENTADO PARA OBTENER EL TÍTULO ACADÉMICO DE LICENCIADO EN INGENIERÍA DE SISTEMAS

POSTULANTE: Univ. Yessenia Velasco Amasifuen

TUTOR: MSc. Ing. Freddy Morales Blanco

ASESOR: Ing. Abel Huaygua Chalco

Cobija - Pando – Bolivia

2016

AGRADECIMIENTO

En primer lugar agradecer a Dios por darme la vida y las fuerzas para seguir adelante a pesar de todas las adversidades, quien me protege y cuida en todo momento e ilumina mi vida.

Agradezco de todo corazón a mi madre Amalia Amasifuen Mamio, por la educación, paciencia, concejos y sobre todo por el amor que siempre me brinda, para poder tener fuerzas y valor para seguir adelante.

A mis hermanas Vania y Camila Yusara, quienes me han apoyado en todo momento de mi vida, por la paciencia y el cariño, especialmente a mi sobrinita Cristel Scarly ya que Dios envió para llenar de felicidad a mi familia, también a mi cuñado Grobert quien siempre estuvo presto para apoyarme en todo.

A mi tutor Ing. Freddy Morales, por su valioso tiempo brindado, quien con dedicación y paciencia supo darme una guía adecuada y el impulso para el desarrollo del presente proyecto.

A mi asesor Ing. Abel Huaygua, por las observaciones y concejos para poder llegar a culminar este proyecto.

A mis compañeros de trabajo Yosel, Marco Antonio, Álvaro y Rogelia, quienes me han apoyado siempre.

A mis compañeras Camila, Anaiz y Rosa Angélica, por ser buenas amigas y apoyarme constantemente y sobre todo por brindarme su amistad.

A mis docentes quienes con dedicación aportaron y compartieron sus conocimientos para así poder formarme profesionalmente.

DEDICATORIA

A mi Madre Amalia Amasifuen Mamio, quien ha dedicado su vida entera para apoyarme y motivarme en todo momento, A mis hermanas Vania y Camila, quienes me han dado fuerzas para seguir adelante y poder lograr este objetivo, a mi sobrinita Cristel Scarly que con su ternura alegra mi vida.

Yessenia Velasco Amasifuen

RESUMEN

El presente proyecto de grado trata sobre la implementación de un Sistema de Seguridad como Modelo en el Gestor de la Base de Datos Siringuero, en la Unidad de Sistemas Académicos dependiente de la Dirección de Información Académica de la Universidad Amazónica de Pando, la cual el problema principal es que el gestor de base de datos del Sistema Siringuero es vulnerable al no contar con sistema de seguridad la cual expone a daños colaterales los datos almacenados de los estudiantes y docentes de la Universidad Amazónica de Pando", en tal sentido es de interés implementar un Sistema de Seguridad como Modelo en el gestor de Base de Datos Siringuero, a través de ello se tiene como objetivos específicos , identificar requerimientos de seguridad de acuerdo a la evaluación de riesgos, realizar el mantenimiento de la base de datos actual e implementar medidas de seguridad, para realizar la implementación del sistema y alcanzar los objetivos, se hizo uso de las metodologías MABDEX II y la Metodología Gestión de Riesgo en SGBD, la implementación del sistema de seguridad en el Gestor de Base de datos se ha fundamentado de acuerdo a las teorías científicas de seguridad, seguridad de información, seguridad informática y seguridad en Sistema Gestores de Base de Datos, como herramienta de implementación se ha utilizado el motor de base de datos PostgreSql 9.6, Sistema Operativo Ubuntu 16.04 y firewall UWF. A partir de la fundamentación teórica se ha realizado el marco aplicativo del presente proyecto de grado, considerando el análisis de riesgo del entorno del Sistema Gestor de Base de Datos, migración del Gestor de Base de Datos de PostgreSql 8.1 a 9.6, mantenimiento de la Base de Datos y sus componentes, implementación de medidas de seguridad en el gestor de base de datos Siringuero, tal cual se ha planificado en el presente proyecto de grado.

Palabras Claves: SGBD **(**Sistema Gestor de Base de Datos) Sprint Frame Work, Postgresql**,** Siringuero**,** Seguridad**,** Base de Datos.

ABSTRACT

This draft degree deals with the implementation of a Security System as a Model in the Manager of the Siringuero Database, in the Unit of Academic Systems dependent on the Directorate of Academic Information of the Universidad Amazónica de Pando, which the problem Main is that the database manager of the Sringuero System is vulnerable to not having a security system which exposes to collateral damage the stored data of the students and teachers of the Amazon University of Pando ", in this sense it is of interest to implement A Security System as a Model in the Syringuero Database manager, through which it has as specific objectives, to identify security requirements according to the risk assessment, perform the maintenance of the current database and implement measures of In order to implement the system and achieve the objectives, the MABDEX II methodologies and the Risk Management Methodology in DBMS were used, the implementation of the security system in the Database Manager was based on the Theories of security, information security, computer security and security in System Database Managers, as a tool for implementation has been used the database engine PostgreSql 9.6, Operating System Ubuntu 16.04 and firewall UWF. Based on the theoretical basis, the application framework of the present degree project has been realized, considering the risk analysis of the Database Management System environment, migration from the PostgreSQL Database Manager 8.1 to 9.6, Base maintenance Of data and its components, implementation of security measures in the database manager Siringuero, as it has been planned in the present project of degree.

Key words: DBMS (Database Management System) Sprint Frame Work, Postgresql, Syringe, Security, Database.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I
MARCO INTRODUCTORIO

1.1. ANTECEDENTES

Las instituciones públicas y privadas a nivel nacional e internacional, pretenden dar mecanismos de seguridad a los sistemas de información en todos los ámbitos con finalidades de preservar y conservar la integridad y fiabilidad que administran los gestores de bases de datos, en tal sentido bajo esta perspectiva, al revisar la bibliografía y los trabajos de grado relacionados al presente proyecto de grado, se han encontrado trabajos de investigación que se describen a continuación.

En el año 2003 el Vice Ministerio de Educación Superior Ciencia y Tecnología firman un convenio con la Universidad Amazónica de Pando, con la finalidad de realizar la transferencia tecnológica entre ambas instituciones, dicha transferencia refiere a la implementación de sistema de información académica que en su momento se denominaría Siga-Coimata, esta es la era del inicio de la existencia de un sistema gestor de base de datos en la U.A.P.

En la Universidad Tecnológica Nacional de Argentina según el autor *(Borghello C.F., 2005)* ha desarrollado el trabajo de grado con el título, Seguridad Informática, sus Implicancias e Implementación, ha obtenido las siguientes conclusiones, Aislamiento Vs globalización, diseño seguro requerido, legislación, tecnologías y riesgos mínimos. Todo Este trabajo relacionado a la seguridad informática.

El trabajo realizado por Borghello muestra claramente que una vez establecidos los controles de acceso que se tiene al sistema, es necesario realizar una buena administración del sistema de seguridad a implementar, ya que se debe tomar muy en cuenta lo que es la seguridad tanto lógica como física, de la misma manera la seguridad de red de datos.

En la Universidad Amazónica de Pando según *(Díaz Y., 2006)*, ha desarrollado un Trabajo Dirigido, en la cual ha obtenido el siguiente objetivo, Mejorar la Administración de la Base de Datos del Siga-Coimata mediante documentación de la estructura de la Base de Datos y procedimientos técnicos, este trabajo ha mejorado básicamente la funcionalidad de la base de datos de dicho sistema.

Durante la gestión 2006 el sistema Siga-Coimata fue reemplazado por un sistema nuevo denominado Sistema Modelo Informacional, desarrollado por la Fundación AUTAPO, el gestor

de base de datos del nuevo sistema fue implementado con la estructura de tablas visiblemente mejoradas respecto a la versión anterior.

El trabajo realizado por Díaz, se toma como referencia para el presente proyecto de grado, porque demuestra la importancia de mejorar la estructura de las tablas del Gestor de Base de Datos del sistema Siga-Coimata, esta base de datos es una versión anterior al Siringuero, además permitirá analizar y estructurar las tablas de acuerdo a las prioridades de almacenamiento de datos.

En la escuela Superior de ingeniería, mecánica y eléctrica de México el autor *(Cuacuas A, 2008),* ha desarrollado una tesina denominada Seguridad de Base de Datos en Informix, y ha obtenido el siguiente objetivo, Proteger y mejorar la seguridad de las bases de datos de Informix con niveles de seguridad, reglas para acceder a las bases de datos y mecanismos de almacenamiento de información, para disminuir fallas en las aplicaciones. Implementación de bitácoras, reglas de acceso, perfiles de usuario (Roles/Usuarios) y mecanismos de almacenamiento persistentes para protección de la información en el centro nacional de control de energía. Se debe considerar que el trabajo mencionado fue desarrollado para el gestor de bases de datos en Informix.

El trabajo realizado por Cuacuas, se toma como referencia para el presente proyecto de grado, porque a través de ello se puede ver los mecanismos de seguridad en los Gestores de la Base de Datos, estos mecanismos de seguridad serán una base fundamental para establecer la implementación de sistema de seguridad en el gestor de base de datos PostgreSql del Sistema Siringuero.

En el transcurso de estos últimos años a partir del 2010 se ha realizado algunas configuraciones de seguridad, no a gran escala sin embargo cubría de manera preliminar los ataques que podría ser utilizado hacia la base de datos del Sistema Siringuero, estos aspectos de seguridad estaban relacionados con el cambio de usuario y la contraseña permanentemente del motor de base de datos, cierre de puerto de PostgreSql hacia los usuarios externos, instalación y configuración de firewall en la plataforma del sistema operativo. Sin embargo, estas medidas de seguridad superficiales no son suficientes para garantizar la integridad y la fiabilidad frente a los atacantes que permanentemente están pretendiendo acceder a la base de datos para las posteriores alteraciones de la estructura y de los datos que contiene la base de datos de dicho sistema.

La base de datos del Sistema Siringuero ha llegado almacenar gran cantidad de datos en estos últimos años, tanto así superan a un millón los registros en algunas tablas importantes de la base de datos. Esto se debe a que ha crecido considerablemente la cantidad de estudiantes y docentes que cursan la Universidad Amazónica de Pando, por esta razón nos permitimos hablar cerca de diez mil entre estudiantes y docentes de pre grado y postgrado respectivamente, frente a esta situación el Sistema Siringuero ha tenido percances en el funcionamiento principalmente en los últimos periodos académicos de la Universidad Amazónica de Pando.

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. Descripción del Problema

La Universidad Amazónica de Pando ha enfrentado grandes cambios transcendentales, cambios estructurales en lo académico y en lo administrativo, durante los últimos años la cantidad de estudiantes y docentes ha incrementado considerablemente y seguirá incrementando con el pasar de los años, a medida que la población está creciendo a pasos agigantados, como demuestran los resultados del último censo a nivel nacional.

Frente al gran crecimiento vegetativo de estudiantes y docentes el sistema académico implementado en la institución, está cayendo cada vez más en la obsolescencia, respecto a las tecnologías actuales.

La Base de Datos del Sistema Siringuero está funcionando desde la gestión 2006 con la tecnología que en su momento estaban disponibles, sin embargo, sin tomar en cuenta la obsolescencia de las aplicaciones, el Sistema Gestor de Base de Datos carece de un sistema de seguridad, que deberían estar implementados para la integridad y el resguardo de los datos que almacena la misma, las copias de seguridad y otros archivos importantes.

Al no contar con medidas de seguridad, el Sistema Gestor de Base de Datos se encuentra vulnerable, frente a cualquier tipo de ataque de agentes interno y/o externo de la institución con fines de acceso, alteraciones u otros fines que puedan tener estos agentes, lo cual pueda causar grandes impactos en las pérdidas y/o daños que administra el Gestor de Base de Datos.

El presente proyecto de grado pretende implementar un modelo de sistema de seguridad que pueda establecer aspectos y niveles de seguridad específicos para el Gestor de Base de Datos postgresql.

1.2.2. Formulación del Problema

Para el presente proyecto de grado se ha redactado el problema principal de la siguiente manera:

"El Gestor de Base de Datos del Sistema Siringuero es vulnerable al no contar con sistema de seguridad la cual expone a daños colaterales los datos almacenados de los estudiantes y docentes de la Universidad Amazónica de Pando".

1.3. OBJETIVOS

1.3.1. Objetivo General

Implementar un Sistema de Seguridad como Modelo en el Gestor de Base de Datos del Sistema Siringuero, aplicando las metodologías Administración de Bases de Datos-MABDEX-II y Gestión de Riesgo en SGBD, que permita establecer la confiabilidad de los datos de Estudiantes y Docentes de la Universidad Amazónica de Pando.

1.3.2. Objetivos Específicos

- Identificar Requerimientos de seguridad de acuerdo a la evaluación de riesgos, para establecer catálogo de requisitos de seguridad del gestor de base de datos del Sistema Siringuero.

- Realizar el mantenimiento de la Base de Datos actual, incorporando la versión más resiente del gestor de base de datos, para una mejor administración.

- Instalar y configurar medidas de seguridad para garantizar que las vulnerabilidades sean reducidas a un nivel aceptable.

1.4. JUSTIFICACIÓN

El presente proyecto de grado surge a raíz de la problemática que atraviesa el gestor de la base de datos del Sistema Siringuero, dicha problemática está basada en las vulnerabilidades del gestor de base de datos, la obsolescencia de las aplicaciones y los riesgos de seguridad, estos factores han dado lugar a realizar el trabajo de investigación científica y tecnológica, con la cual la unidad y la institución podrá resolver las problemáticas que se atraviesan actualmente.

El presente proyecto de grado a desarrollar permitirá resguardar de manera segura lo que es la autenticidad e integridad de los datos almacenados en la base de datos del Sistema Siringuero.

Es de interés la elaboración del proyecto de grado ya que se abordará los conocimientos tecnológicos que incorpora el Sistema Siringuero, analizando la envergadura de la base de datos, la cantidad de los módulos existentes en dicho sistema, las aplicaciones que permiten dar funcionalidad al sistema académico.

1.5. ALCANCES

El presente proyecto de grado pretende realizar la implementación de un Sistema de seguridad como modelo en el gestor de base de datos del Sistema Siringuero, la cual va a considerar aspectos de seguridad relacionados a postgresql.

Los procesos necesarios al implementar el sistema de seguridad como modelo en el gestor de base de datos del Sistema Siringuero, están en base a las metodologías mencionadas en el acápite anterior los cuales son los siguientes:

- **Requerimiento de Seguridad. -** Este aspecto refiere a qué componentes del Sistema Gestor de Base de Datos se deba dar seguridad y cuáles serán las medidas de seguridad, que se deba implementar en cada aspecto de los requerimientos establecidos.

- **Mantenimiento de la Base de Datos. -** Se realizará el mantenimiento de la base de datos mediante la migración del gestor de base de datos postgresql 8.1 hacia la versión 9.6, versión más reciente y estable que permiten instalar los servidores del sistema operativo Ubuntu, esta

innovación tecnológica permitirá establecer la integridad, confiabilidad y la disponibilidad de los datos que administra dicho gestor.

- **Implementación de Medidas de Seguridad. -** Una vez establecidos los requisitos de seguridad, la prioridad de la información y los riesgos que fueron analizados y evaluados, se instalará y configurará el sistema de seguridad como modelo en el Gestor de Base de Datos del Sistema Siringuero.

El presente proyecto de grado dedicará la implementación de Sistema de Seguridad como modelo en el Gestor de Base de datos del Sistema Siringuero, y no considerará la implementación de sistema de seguridad en el nivel de la aplicación del sistema, (lenguajes de programación, controles y vistas).

Se toma como referencia la norma ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información, al ser una norma para la implementación de seguridad en gestión de la información, no se aplica para la implementación de sistema de seguridad en gestor de base de datos del presente proyecto de grado.

1.6. METODOLOGÍA

Para el proceso de la implementación del presente proyecto de grado, ha aplicado dos metodologías las cuales son:

1.6.1. Metodología Administración de Base de Datos MABDEX-II

La presente metodología abarca sobre la administración de Gestores de Base de Datos orientado para los Administradores de Base de Datos (DBA), la cual tiene las siguientes fases:

- **Mantenimiento de la Base de Datos**

Para el mantenimiento de los componentes de la base de datos, la metodología recomienda realizar un estudio previo de la institución, para así verificar el funcionamiento de estos componentes y para determinar si existe sobresaturación de la información, esto con el fin de

tener una idea más clara de lo que puede hacerse sobre la base de datos para que esta esté optimizada.

❖ **Seguridad de la Base de Datos**

La seguridad de las bases de datos es importante, para evitar la fuga de información de la empresa, además de lograr una razonable estabilidad de la información y prevenir futuros accesos no autorizados que interrumpan el flujo normal de la empresa.

1.6.2. Metodología para Gestión de Riesgo en SGBD

La presente metodología refiere a la gestión de riesgos en Sistema Gestor de Base de Datos, la cual dispone de las siguientes fases:

❖ **Requerimiento de Seguridad**

La gerencia de TIC, debe identificar sus requerimientos de seguridad para ello cuenta con los siguientes insumos:

- Evaluación de riesgo
- Requisitos para el procesamiento de la Información

❖ **Seguridad de la Información**

La información es un recurso que, como el resto de los demás activos comerciales, tiene valor por una organización y por consiguiente debe ser debidamente protegida.

❖ **Evaluación de Riesgos**

Proceso en que se identifican las amenazas, a los activos se evalúan las vulnerabilidades y probabilidades de ocurrencia, y además se estigma el impacto potencial de una falla de seguridad.

- **Selección e Implantación de Controles**

Una vez identificado los requerimientos de seguridad y los factores de riesgo, se deben seleccionar e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable.

1.6.3. Herramientas Utilizadas

Las herramientas que se utiliza para realizar el presente proyecto de grado son: PostgreSql, Servidor Toncam, Linux, J2EE, Servidor Ubuntu, JSP

1.7. ORGANIZACIÓN DEL DOCUMENTO

- **Capítulo I:** Es la parte introductoria del documento en el cual se identifica el problema principal como la vulnerabilidad de la base de datos del Sistema Siringuero, el objetivo es dar solución implementando un sistema de seguridad como modelo, como alcance se describe el marco de la implementación del Sistema en el Gestor y no así en el Servidor de Aplicación, y la metodología que permitirá implementar dicho sistema.
- **Capítulo II:** Describe el marco teórico, el cual contempla las bases teóricas científicas, que sustente el presente proyecto.
- **Capítulo III:** Describe las metodologías que se utilizará para la elaboración del presente proyecto de grado
- **Capítulo IV:** Describe lo que es el marco institucional, el cual narra los datos de la intuición en donde se realizará el proyecto.
- **Capítulo V:** Describe la realización del análisis de riesgo, el mantenimiento en el gestor de la base de datos, y la implementación de medidas de seguridad en el Gestor de Base de Datos del Sistema Siringuero.
- **Capítulo VI:** Se describe como conclusiones los resultados que se han alcanzado de acuerdo a los objetivos general y los específicos, considerando los alcances que se ha planificado, las recomendaciones para que los funcionarios puedan ejecutar el instructivo, toda vez que el Gestor de Base de Datos Postgresql lance una nueva versión estable.

CAPÍTULO II
MARCO TEÓRICO

2.1. FUNDAMENTO TEÓRICO GENERAL

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

2.2. SEGURIDAD

Existen distintas concepciones sobre seguridad, que autores como Keymer Ávila (2006) siguiendo a Alessandri Baratta, resumen de las siguientes:

> *Por un lado, el Modelo del derecho a la seguridad define a la seguridad como un derecho, una necesidad humana y una función del sistema jurídico. Hace énfasis en los delitos contra la propiedad: robo y hurto. Está íntimamente relacionado con la construcción social del miedo. (Keymer Ávila ,2006)*
>
> *Por otro lado, el Modelo de la seguridad de los derechos concibe a la seguridad como una necesidad y un derecho de carácter secundario, respecto a todas las otras necesidades básicas o reales, que pueden definirse como primarias (alimento, vestimenta y abrigo). Esta política abarca un campo extremamente más amplio que la restringida prospectiva de la "lucha" contra la criminalidad. (Alessandri Baratta)*
>
> *La Seguridad, en el sentido más amplio del término, hace referencia a la ausencia de riesgos o amenazas, tanto en el campo de los asuntos internacionales como en el ámbito individual de las personas físicas. Así pues, la seguridad concierne a Estados, gobiernos e individuos. Es un término que ha sufrido transformaciones y ha tenido distintas concepciones a lo largo de la historia, debido a los cambios políticos, económicos y sociales a nivel global.*
> *(Pérez, 2013)*

Seguridad Como un concepto controvertido, ya que no existe un consenso generalizado sobre su significado. En función de las personas, sus ideas, cultura y percepciones de la realidad el término seguridad adquiere un valor distinto. Este hecho se ve corroborado por el importante número de definiciones de seguridad que han aparecido, sobre todo a partir del final de la Guerra Fría. Seguridad Nacional, Seguridad Común, Seguridad Colectiva, Seguridad Compartida, Seguridad Humana o Seguridad Cooperativa efectúan una descripción de lo que sus ideólogos consideran que debe ser entendido por seguridad y, lo que es quizás más importante, como conseguirla. En los últimos años, a los términos ya citados se les han ido uniendo Seguridad Sostenible, así como conceptos híbridos tales como "poder duro - poder blando" o "poder inteligente" (Buzan, 2011)

FIGURA 1: *Seguridad y Privacidad*
Fuente: Elaboración Propia

2.3. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos, que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

> *Se podría definir como seguridad de la información a un estado específico de la misma sin importar su formato, que nos indica un nivel o un determinado grado de seguridad de información, por ejemplo, que está libre de peligro, daño o riesgo, o por el contrario que es vulnerable y puede ser objeto de materialización de una amenaza. Las vulnerabilidades, el peligro o el daño de la misma es todo aquello que pueda afectar su funcionamiento directo y la esencia en sí de la información, o en su defecto los resultados que se obtienen de la consulta, administración o procesamiento de ella (Ávila, 2012).*

> *Garantizar un nivel de protección total es virtualmente imposible, la seguridad de la información en la práctica a un nivel total o de completitud no es alcanzable porque no existe un sistema seguro al ciento por ciento. "La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en cualquier tipo de conversación". Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene (Ruiz, 2008)*

> *La seguridad de la información protege a una organización que la adopte como parte de su visión y misión de un amplio rango de amenazas, para asegurar la continuidad del negocio, minimizar los posibles daños y maximizar el retorno de las inversiones y las oportunidades. La información digital o en papel y los procesos que la apoyan, los sistemas y redes son importantes activos de la organización (Ruiz, 2008)*

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños

como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

De acuerdo a los autores Ávila y Ruiz, la seguridad de la información refiere a la protección del estado de la misma, estas informaciones pueden estar en diversos formatos, las cuales permiten el funcionamiento adecuado de una institución u organización, los resguardos de éstas permiten maximizar la disponibilidad, minimizar los posibles daños y las vulnerabilidades en la administración de la información.

2.4. SEGURIDAD INFORMÁTICA

La seguridad informática o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta y especialmente la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose en información privilegiada.

> *Seguridad es un estado de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. (Rodea, 1994).*

Según el autor Rodea, un sistema informático es utópico, porque no es preciso brindar la seguridad al 100%, sin embargo, los riesgos y las vulnerabilidades se disminuyen al implementar un sistema de seguridad en los niveles que la institución vea conveniente.

Sin embargo, para Beekman la seguridad informática lo ve desde el punto de vista de la importancia y define de la siguiente manera.

> *La seguridad es un tema muy importante para cualquier* empresa, *este o no conectada a una red pública. No solamente es importante, sino que también puede llegar a ser compleja. Los niveles de seguridad que se pueden implementar son muchos y dependerá del usuario hasta donde quiera llegar (Beekman, 1996).*

La seguridad informática y de datos difiere mucho de simplemente tener un Firewall. Se aborda un proceso de seguridad recomendado a utilizar (al menos) las siguientes herramientas:

- Un firewall o combinación de ellos.
- Un sistema de Detección de Intrusos o IDS.
- Sistemas de actualización automática de software.
- Sistemas de control de la integridad de los servidores, paquetes, etc.
- Un sistema de administración y control para monitorear la seguridad.

Para Whitten la información es el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales, en la cual hace alusión en sus definiciones como se refleja a continuación

> *Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática (Whitten, 1995).*

A partir de las definiciones de Whitten , Beekman y Rodea, la seguridad informática es mantener en estado intacto la información o aplicaciones dentro de otro sistema, lo cual se puede llevar a cabo mediante medios externos de seguridad o internos dependiendo el grado de seguridad.

2.4.1. Importancia de la Seguridad Informática

Qué importancia tiene la seguridad informática, es lo que a continuación definen tres autores diferentes, las cuales se reflejan a continuación.

> *La seguridad hoy en día es uno de los principales problemas encontrados en el área de informática, cuando se habla de seguridad por lo general se piensa en un término*

> *privacidad de la información en el cual se pueden incluir aspectos tales como: contraseñas, accesos a la información, mensajes cifrados y en definitiva, todo lo relacionado con la protección y confiabilidad de los datos (Mediavilla, 1998).*

Además, el autor Mediavilla, nos menciona que también se tienen que considerar otros aspectos como son: la privacidad, la integridad y disponibilidad.

> *La informática debe concebirse en un sentido amplio y con un carácter propio. Si bien no existe una definición precisa del alcance de esta disciplina, es importante señalar que la misma ha surgido como una convergencia durante varias décadas entre las telecomunicaciones, las ciencias de la computación y la microelectrónica, incorporando a su vez conceptos y técnicas de la ingeniería, la administración, la psicología y la filosofía, entre otras disciplinas. Algunas áreas de la informática como es la de la inteligencia artificial tienen una estrecha relación con los algoritmos de búsqueda y de optimización de la investigación de operaciones y con los conceptos de psicología cognitiva (Minguet, 1994).*

> *La informática encuentra en los procesos de manufactura un lugar idóneo para aportar ventajas competitivas que las industrias de cualquier tipo requieren. Ya sean organizaciones de fabricación discreta o de procesos, las empresas requieren el uso integral de la información en cada eslabón de la cadena de suministro: saber qué demanda el mercado, contar con lo necesario para satisfacer esos requerimientos, definir los precios, la distribución y la manufactura misma, entre muchos otros aspectos que intervienen en el diseño, la fabricación y la comercialización de un producto (Areees, 2004)*

De acuerdo a los autores Mediavilla, Minguet y Arees afirman que a través de la informática el hombre consigue lograr aquellas cosas que solo no puede, es una herramienta como los simples instrumentos de manufacturas que se usó en el pasado para poder trabajar la tierra, ahora usa las computadoras y medios de comunicación instantáneos para poder agilizar todos los procesos de su vida.

FIGURA 2: *Seguridad Informática*
Fuente: Elaboración Propia

2.4.2. Seguridad de la Aplicación

La seguridad de aplicaciones puede efectuarse en cualquier forma principalmente dentro de un sistema que contenga muchas aplicaciones que son de vital importancia analizamos 3 diferentes puntos de vista para generar una opción general.

> *La seguridad en las aplicaciones se refiere tanto a los componentes de la computadora como a los que no lo son; en el caso de los componentes de la computadora comprende datos, programas y archivos que se procesan en el sistema; los elementos que no son de la computadora, incluyen recolección, entrega de datos, e información del archivo maestro para el procesamiento (Mediavilla, 1998)*

Según el autor Mediavilla, la seguridad de la aplicación no siempre se refiere al sistema, el cual se ejecuta dentro de un equipo computacional, también hay que tomar en cuenta la seguridad del procesamiento de la información que se realiza de manera manual.

2.5. SISTEMA GESTOR DE BASE DE DATOS

Un Sistema Gestor de Base de Datos (SGBD) es un conjunto de programas que permiten el almacenamiento, modificación y extracción de la información en una base de datos, además de proporcionar herramientas para añadir, borrar, modificar y analizar los datos.

Los usuarios pueden acceder a la información usando herramientas específicas de consulta y de generación de informes.

> *Un Sistema Gestor de Base de Datos Consiste en una colección de datos interrelacionados y un conjunto de programas para acceder a esos datos. El Objetivo primordial de un SGBD es proporcionar un entorno que sea a la vez conveniente y eficiente para ser utilizado al extraer y almacenar información de la base de datos (Kort, 1995).*

Según el autor Kort, un Sistema Gestor de Base de Datos es un conjunto de programas, las cuales administran una colección de datos, que interrelacionados conforman una base de datos, es así pues los gestores de base de datos, permiten almacenar gran cantidad de datos, hoy en día, incorporados a estos programas las aplicaciones web, y otros programa facilitan los accesos esa colección de datos.

La aparición de los SGBD fue fruto de la necesidad de cambiar el concepto de almacenamiento de datos. Antes de los SGBD (década de los setenta), la información se trataba y se gestionaba utilizando los típicos sistemas de gestión de archivos que iban soportados sobre un sistema operativo.

Pero quizá el mayor problema que presentaba la gestión de archivos era la dependencia de la estructura del fichero con el programa. Puesto que la estructura del fichero dependía directamente del programa que lo gestionaba, en el momento que se cambiara esa estructura había que adaptar el propio programa y volver a compilar, lo que entonces llevaba largo tiempo.

2.5.1. Base de Datos

Se define una base de datos como una serie de datos organizados y relacionados entre sí. Los Cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

> *"Colección o depósito de datos, donde los datos están lógicamente relacionados entre sí, tienen una definición descripción comunes y están estructurados de una forma articular. Una Base de Datos es también un modelo del mundo real y, como*

tal, debe poder servir para toda una gama de usos y aplicaciones", (Conference des Statisticiens Européens, 1977)

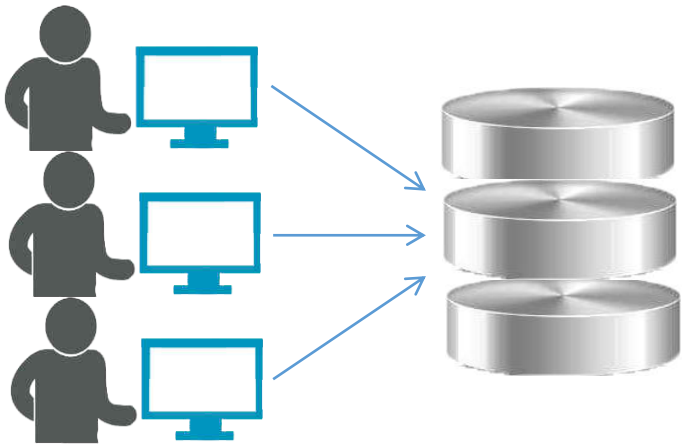


FIGURA 3: *Sistema Gestor de la Base de Datos*
Fuente: Conference des Statisticiens Européens

"Colección integrada y generalizada de datos, estructurada atendiendo a las relaciones naturales de modo que suministre todos los caminos de acceso necesarios a cada unidad de dato, con objeto de poder atender todas las Necesidades de los diferentes usuarios", (Deen, 1985).

"Colección o depósito de datos integrados, almacenados en soporte secundario (no volátil) y con redundancia controlada. Los datos, que han de ser compartidos por diferentes usuarios y aplicaciones, deben mantenerse independientes de ellos, y su definición (estructura de la base de datos) única y almacenada junto con los datos, se ha de apoyar en un modelo de datos, el cual ha de permitir captar las interrelaciones y restricciones existentes en el mundo real. Los procedimientos de actualización y recuperación, comunes y bien determinados, facilitarán la seguridad del conjunto de los datos", Piattinit. (2006).

Las bases de datos proporcionan la infraestructura de almacenamiento y consulta de información requerida, para los sistemas de apoyo a la toma de decisiones y apara los sistemas de información estratégicos. Por este motivo es importante conocer la forma en que está estructurada la base de datos, el control de acceso de usuario y su administración del servidor donde reside la información.

2.5.2. Componentes del Sistema Gestor de Base de Datos

Los SGBD son paquetes de software muy complejos que deben proporcionar una serie de servicios que van a permitir almacenar y explotar los datos de forma eficiente. Los componentes principales son los siguientes:

2.5.2.1. Lenguajes de SGBD

Lenguaje de definición de datos DDL: Te permite llevar a cabo las tareas de definición de las estructuras que almacenarán los datos, así como los métodos o funciones que permitan consultarlos.

Lenguaje de manipulación de datos DML: Te permite consultar o manipular los datos, organizados por el modelo adecuado. El más popular es el SQL.

Lenguajes de cuarta generación: Son lenguajes de programación diseñados con el objetivo de desarrollar aplicaciones orientadas a las bases de datos.

Lenguaje de control de datos: Este tipo de lenguaje incluye una serie de comandos SQL que permiten al administrador controlar el acceso a los datos que tengan una base de datos.

2.5.2.2. Diccionario de Datos

El diccionario de datos es el lugar donde se guarda toda la información de todos los datos que forman la base de datos. Dentro de él se encuentra la lista de todos los elementos que forman parte del flujo de datos de todo el sistema.

En su contenido está las descripciones de todos los demás objetos (archivos, programas,) que existen en el sistema, almacena el conjunto numeroso de esquemas y especifica cada archivo y su

ubicación, también incluye información acerca de qué programas utilizan qué datos, y a que usuarios les interesa un informe u otro.

Está integrado dentro de la misma base de datos, puede tolerar descripciones de los modelos conceptual, lógico, interno y externo. Está guardado en un medio con acceso directo por si llegásemos a perder información poder recuperarla con facilidad.

2.5.2.3. Administrador de Base de Datos (DBA)

El Administrador de bases de datos es el profesional de tecnologías de la información y la comunicación, responsable de los aspectos técnicos, tecnológicos, científicos, inteligencia de negocios lógicos de bases de datos

> *Es la persona o equipo de personas profesionales responsables del control y manejo del sistema de base de datos, generalmente tiene(n) experiencia en DBMS, diseño de bases de datos, Sistemas operativos, comunicación de datos, hardware y programación (Gutiérrez, 2008).*

Los sistemas de base de datos se diseñan para manejar grandes cantidades de datos, la manipulación de los datos involucra tanto la definición de estructuras para el almacenamiento de la Base de Datos como la provisión de mecanismos para la manipulación de la DB, además un sistema de base de datos debe de tener implementados mecanismos de seguridad que garanticen la integridad de la DB, a pesar de caídas del sistema o intentos de accesos no autorizados.

> *Persona que toma las decisiones estratégicas y de política con respecto a la DB de la empresa, y el DBA es quién proporciona el apoyo técnico necesario para poner en práctica esas decisiones. Por tanto, el DBA está encargado del control general del sistema en el nivel técnico (Gutiérrez, 2008).*

Un objetivo principal de un sistema de base de datos es proporcionar a los usuarios finales una visión abstracta de los datos, esto se logra escondiendo ciertos detalles de cómo se almacenan y mantienen los datos.

2.6. SEGURIDAD EN SISTEMA GESTOR DE BASE DE DATOS

La seguridad del gestor de base de datos está compuesta por 3 componentes principales, las cuales son la confiabilidad, integridad y disponibilidad.

2.6.1. Confiabilidad

La confiabilidad es otro requerimiento indiscutible y probablemente el más importante, una base de datos no confiable es simplemente inutilizable. Para la mayoría de las aplicaciones alojadas, en especial las utilizadas en sistemas de tiempo real, la confiabilidad es una propiedad no negociable que deben tener todos los componentes.

Un sistema de manejo de bases de datos confiable es aquel que puede continuar procesando las solicitudes de usuario aun cuando el sistema sobre el que opera no es confiable. En otras palabras, aun cuando los componentes de un sistema distribuido fallen, un DDMBS confiable debe seguir ejecutando las solicitudes de usuario sin violar la consistencia de la base de datos.

La confiabilidad engloba varias actividades y una de ellas es el planteamiento de modelos de confiabilidad, esto es fundamentalmente la probabilidad de supervivencia del sistema.

Se expresa como una función de las confiabilidades de los componentes o subsistemas, que generalmente, estos modelos se encuentran dependiendo del tiempo.

2.6.2. Integridad.

En general, el término integridad hace referencia a una cualidad de íntegro e indica "Que no carece de ninguna de sus partes." y relativo a personas "Recta e intachable". En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

Los cambios en la Base de Datos pueden perderse debido a un error del sistema o a un fallo en el suministro de energía.

Una de las funciones importantes de un DBMS relacional es preservar la integridad de sus datos almacenados en la mayor medida posible

FIGURA 4: *Integridad*
Fuente: Elaboración Propia

2.6.3. Disponibilidad

Se cumple si las personas autorizadas pueden acceder a tiempo a la información.

El disponer de la información después del momento necesario puede equivaler a la no disponibilidad. Otro tema es disponer de la información a tiempo pero que esta no sea correcta, e incluso que no se sepa, lo que puede originar la toma de decisiones erróneas.

Otro caso grave es la no disponibilidad absoluta. Por haberse producido algún desastre. En este caso a medida que pasa el tiempo el impacto será mayor, hasta llegar a suponer la no continuidad de la entidad.

En relación con ello deben existir soluciones alternativas, basadas en medios propios o contratados, copias actualizadas de la información crítica y de programas en un lugar diferente, y un verdadero plan de continuidad que permita restablecer las operaciones en un tiempo inferior o igual al prefijo.

Para ello los usuarios habrán determinado previamente la criticidad de las aplicaciones y el impacto en sus áreas por parte de un comité, se habrán determinado las prioridades.

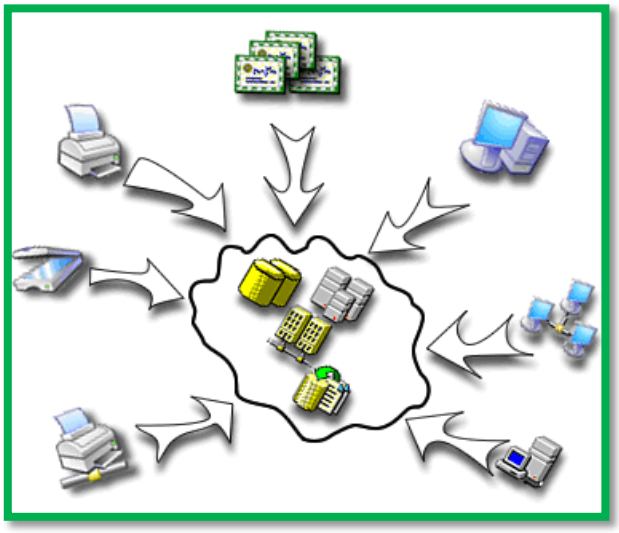


FIGURA 5: *Disponibilidad de la Base de Datos*
Fuente: Elaboración Propia

2.7. INTEGRIDAD REFERENCIAL EN SGBD

2.7.1. Restricciones de Integridad

En el mundo real existen ciertas restricciones que deben cumplir los elementos existentes; es decir, una persona sólo puede tener un número de C.I y una única dirección oficial. Cuando se diseña una base de datos se debe reflejar fielmente el universo del discurso que estamos tratando, lo que es lo mismo, reflejar las restricciones existentes en el mundo real.

Los componentes de una restricción son los siguientes:

- La operación de actualización (inserción, borrado o eliminación) cuya ejecución ha de dar lugar a la comprobación del cumplimiento de la restricción.
- La condición que debe cumplirse, la cual es en general una proposición lógica, definida sobre uno o varios elementos del esquema, que puede tomar uno de los valores de verdad (cierto o falso).
- La acción que debe llevarse a cabo dependiendo del resultado de la condición

En general, se puede decir que existen tres tipos de integridad:

2.7.2. Integridad de Dominio

Las restricciones de los dominios son la forma más simple de restricción de integridad. El sistema las verifica fácilmente siempre que se introduce en la base de datos un nuevo elemento de datos.

La cláusula create domain se puede usar para definir nuevos dominios. Por ejemplo, las instrucciones: CREATE DOMAIN dentero4 AS integer DEFAULT 0.

SQL también proporciona las cláusulas drop domain y alter domain para borrar o modificar dominios que se hayan declarado anteriormente.

2.7.3. Integridad de Entidad

Establece que la clave primaria de una tabla debe tener un valor único para cada fila de la tabla, si no, la base de datos perderá su integridad.

Una clave primaria es la columna o colección de columnas que identifican de forma única a una fila determinada en una tabla. La clave primaria proporciona una forma importante de distinguir una fila de otra

> *El componente básico de un archivo en un sistema de archivos es un elemento dato, el cual es la unidad nombrada más pequeña de datos que tienen significado en el mundo real – por ejemplo, apellido, nombre, calle, número de identidad, y partido político (Teorey, Lightstone, Nadeau, & Jagadish, 2011).*
>
> *Los valores que almacenas en la base de datos son datos. Los datos son estáticos en el sentido de que permanecen en el mismo estado hasta que los modificas mediante algún proceso manual o automatizado (Hernández, 2013).*
>
> *Puede definirse al dato como un hecho conocido que puede ser almacenado y que tiene un significado implícito. Los datos son hechos puros o aislados a partir de los cuales se produce la información requerida (Singh, 2011).*

2.7.4. Integridad Referencial

A menudo se desea asegurar que un valor que aparece en una relación para un conjunto de atributos determinado aparezca también en otra relación para un cierto conjunto de atributos. Esta condición se denomina integridad referencial.

El caso más normal es cuando queremos garantizar que el valor almacenado en una clave externa ésta también como clave primaria en la relación referenciada. En caso contrario, se dice que la tupla de la relación referenciarte esta colgante.

Las tuplas colgantes pueden ser aceptables o no, dependiendo del modelo de datos. En el caso de que no sean aceptables, hay que imponer una integridad referencial o dependencia de subconjunto.

2.7.5. Disparadores (Triggers)

Un disparador es una orden que el sistema ejecuta de manera automática como efecto secundario de la modificación de la base de datos.

Para diseñar un mecanismo disparador hay que cumplir dos requisitos:

- Especificar las condiciones en las que se va a ejecutar el disparador. Esto se descompone en un evento que causa la comprobación del disparador y una condición que se debe cumplir para ejecutar el disparador.
- Especificar las acciones que se van a realizar cuando se ejecute el disparador.

Una vez se almacena un disparador en la base de datos, el sistema de base de datos asume la responsabilidad de ejecutarlo cada vez que ocurra el evento especificado y se satisfaga la condición correspondiente.

2.7.6. Necesidad de los Disparadores

Los disparadores son mecanismos útiles para alertar a los usuarios o para realizar de manera automática ciertas tareas cuando se cumplen determinadas condiciones.

Obsérvese que los sistemas de disparadores en general no pueden realizar actualizaciones fuera de la base de datos.

2.7.7. Seguridad y Autorización

2.7.7.1. Violaciones de la Seguridad

Existen varias formas de acceso que pueden ser mal utilizadas. Concretamente hay que impedir las operaciones de lectura no autorizada, las modificaciones no autorizadas, y la destrucción de datos no autorizado

Para proteger la base de datos hay que adoptar medidas de seguridad en varios niveles: A nivel de Base de datos, a nivel de Sistema operativo, de redes, seguridad física y por último pero no menos importante, a nivel humano.

Las dos últimas son especialmente importantes, ya que romper la seguridad a esos niveles más bajos normalmente conlleva el poder saltársela a niveles más altos. Piénsese, por ejemplo, lo que podría hacer un intruso que obtuviera, mediante engaños, el identificador de usuario y la contraseña del administrador, o con acceso físico a las máquinas y a los discos que gestionan y almacenan la base de datos.

2.7.7.2. Autorizaciones

Un esquema de seguridad muy utilizado es las autorizaciones, que permitiría realizar (o no) determinadas operaciones sobre los datos. Por ejemplo, podemos tener una autorización para lectura, otra para inserción, otra para modificación y otro para borrado. Se le pueden asignar a un usuario todos los tipos de autorización, ninguno o una combinación de ellos.

Además de estas autorizaciones, se pueden tener autorizaciones para trabajar con índices, modificar el esquema, etc.

La capacidad de crear nuevas relaciones queda regulada mediante la autorización de recursos. El usuario con la autorización de recursos que crea una relación nueva recibe automáticamente todos los privilegios sobre la misma.

La forma superior de autoridad es la concedida al administrador de la base de datos. El administrador de la base de datos puede autorizar usuarios nuevos, reestructurar la base de datos, etcétera. Esta forma de autorización es análoga a la proporcionada al súper usuario u operador del sistema operativo.

2.7.7.3. Concesión de Privilegios

Un usuario al que se le ha concedido una autorización puede ser autorizado a transmitirla a otros usuarios. Sin embargo, hay que tener cuidado con el modo en que se hace, para poder asegurar que la misma pueda retirarse en el futuro.

La transmisión de la autorización de un usuario a otro puede representarse mediante un grafo. Los nodos de este grafo son los usuarios. La raíz de todos los grafos será el administrador de la base de datos.

Un usuario tiene autorización si y solo si hay un camino desde el administrador de la base de datos hasta el nodo que representa a ese usuario.

Esto se hace así para evitar que un par de usuarios eludan las reglas de retroceso de autorizaciones concediéndose autorización mutuamente.

2.7.7.4. El concepto de Papel (Rol)

Los papeles o roles son una forma de simplificar la asignación de autorizaciones a los usuarios. Las autorizaciones se conceden a los papeles, de igual modo que se conceden a usuarios individuales. En la base de datos se crea un conjunto de papeles. Se concede uno o varios papeles a cada usuario de la base de datos.

Una alternativa similar, pero menos preferible, sería crear un identificador de usuario cajero y permitir que cada cajero se conectase a la base de datos usando este identificador. El problema con este esquema es que no sería posible identificar exactamente al cajero que ha realizado una determinada transacción, conduciendo a problemas de seguridad.

2.7.7.5. El Privilegio de Conceder Privilegios

Un usuario o papel al que se le concede un privilegio no está autorizado de manera predeterminada a concederlo. Si se desea conceder un privilegio a un usuario y permitirle que lo transmita a otros usuarios hay que añadir la cláusula with grant option a la orden grant correspondiente.

2.7.7.6. Cifrado y Autenticación

Para información extremadamente reservada es necesario cifrar los datos. Los datos cifrados no se pueden leer a menos que el lector sepa la manera de descifrarlos. El cifrado también forma la base de los buenos esquemas´ para la autenticación de usuarios en una base de datos.

CAPÍTULO III
MARCO METODOLÓGICO

3.1. METODOLOGÍA MABDEX-II

La metodología MABDEX-II, fue publicada por la Universidad Nacional de Costa Rica, la cual está disponible a nivel mundial, para aquellas instituciones y personas que están dedicadas a la administración de base de datos, esta metodología comprende los procesos principales como administración de base de datos, administración de seguridad de sistema gestor de Base de datos, Mantenimiento entre otros, el presente proyecto de grado ha utilizado como base fundamental, dicha metodología, para la implementación del Sistema de Seguridad como Modelo en el Sistema Gestor de Base de datos Siringuero.

La metodología de Administración de Base de Datos (MABDEX-II), tiene los siguientes procesos fundamentales:

- Creación de Base de Datos
- Mantenimiento de Base de Datos
- Seguridad de Base de Datos
- Respaldo de la Base de Datos
- Recuperación de la Base de Datos

El presente proyecto de grado ha utilizado esta metodología para la implementación del sistema de seguridad como modelo en el Gestor de la Base de Datos Siringuero, de los procesos descritos anteriormente, se ha utilizado los siguientes:

- mantenimiento de base de datos
- Seguridad de Base de datos

Los siguientes procesos utilizados por el presente proyecto de grado se detallarán a continuación, describiendo cada uno de los pasos fundamentales, que llevó a desarrollar adecuadamente la implementación del Sistema de Seguridad en el Gestor de Base de Datos Siringuero.

3.1.1. Mantenimiento de Componentes de Una Base de Datos

Para el mantenimiento de los componentes de la base de datos es recomendable realizar un estudio previo de la empresa, para así verificar el funcionamiento de estos componentes y para determinar si existe sobresaturación de la información, esto con el fin de tener una idea más clara de lo que puede hacerse sobre la base de datos para que esta esté optimizada.

Dentro de los procesos de mantenimiento de una base de datos se encuentran:

- Mantenimiento de Tablespace
- Modo Seguro de Transacciones
- Índices
- Bitácoras

3.1.1.1. Mantenimiento de Tablespaces

Para realizar el mantenimiento de tablspaces la metodología MABDEX II propone realizar en dos pasos, la primera "Inspeccionar periódicamente el tamaño usado por los tablespaces (debe existir un límite), en tanto la segunda considera, " tener parámetros para medir el nivel de saturación", este es uno de los pasos que en todos los gestores de base de datos se deberían seguir, sin embargo, los manejadores de base de datos hoy por hoy automatizan estos procesos, tal cual es el postgresql 9.5.4, y los posteriores.

Así mismos MABDEX-II, propone para el mantenimiento de tablespaces, establecer los siguientes procesos:

- Creación de Tablespace:
- Compactación de Tablespace
- Eliminación de Tablespace
- Mover Tablespace
- Adición de DataFile
- Ampliacion de Datafile

3.1.1.2. Modo Seguro de Transacciones

El modo seguro de Transacciones permite que la base de datos realice respaldos automáticos de todas sus bitácoras sin necesidad de deshabilitarla. Cada vez que una bitácora alcanza su capacidad máxima de almacenamiento se produce un cambio de bitácora, es decir, los datos pasan a otra bitácora con más capacidad en la cual se almacenarán. Esto permite que la base de datos trabaje 24x7, o sea, que no se tenga que deshabilitar para realizar respaldos en las bitácoras. Se recomienda establecer el modo seguro de transacción desde el inicio de la instalación de la base de datos, ya que así asegurará los respaldos de la misma.

3.1.1.3. Índices

Un índice es una estructura diseñada para obtener un acceso más rápido a los datos contenidos dentro de una tabla. Es independiente de los datos almacenados en la tabla y cuando se encuentra bien definido reduce significativamente la búsqueda, aumentando el rendimiento, oracle utiliza árboles tipo B para balancear el tiempo de acceso a cualquier fila. Inmediatamente luego de crear el índice, este comienza a mantenerse al tanto de las inserciones, actualizaciones y eliminaciones de registros de la tabla en la cual se ha implementado.

Existen tres tipos de índices cuya naturaleza depende de la forma en que haya sido creado. Estos tipos son:

- Índice Primario: Es aquel que tiene la restricción adicional de que el grupo de columnas indexadas define una única fila o llave primaria.
- Índice Foráneo: Se realizan consultas por campos distintos a los de la clave primaria, por ello hay que crear un índice por los campos por los que se accede.
- Índice Adicional: Se realizan cuando existen varias instrucciones que requieren ordenamiento, por ejemplo, cuando se utiliza el order by. Sin embargo, las consultas no deben ser alteradas cuando se coloca un índice.

Es importante revisar con frecuencia los índices para que no se fragmenten, a su vez hay que desfragmentarlos dependiendo del porcentaje de fragmentación que estos presentan.

Un índice sólo es efectivo cuando es utilizado. Es por eso que debe asegurarse que la frecuencia de uso sea muy alta y que su implementación vaya a mejorar el rendimiento de las consultas efectuadas a la tabla donde reside el índice. Sin embargo, no es muy conveniente el uso de varios índices dentro de una misma tabla porque con cada operación de inserción, actualización o eliminación que se lleva a cabo sobre una tabla, sus índices se deben recrear. La creación, organización, borrado y análisis de índices deberán llevar un registro de documentación.

3.1.1.4. Bitácoras

Para un buen mantenimiento de las bitácoras de una base de datos es necesario tener presente la organización de la empresa; es decir que tantas transacciones se reportan diariamente, y que también respaldado se quieren tener esas transacciones (en la mayoría de las empresas estas bitácoras son primordiales en caso de una posible caída de la base de datos).

A la hora de crear una base de datos se debe hacer un estudio previo del manejo de la empresa y la cantidad de recursos disponibles para la construcción de la Base de Datos, con estos datos ya cuantificados es posible determinar el número de bitácoras, así como el tamaño necesario para cada una de ellas.

En caso de que la base ya haya sido creada y lo que se necesite sea darles mantenimiento a las bitácoras, es muy importante también el estudio preciso del número promedio de transacciones diarias de la empresa, para así asegurar que el tamaño y el número de bitácoras a adicionar sea el más preciso, y brinde el mejor funcionamiento de la base de datos.

3.1.2. Seguridad de la Base de Datos

La seguridad de las bases de datos es importante para evitar la fuga de información de la empresa, además, de lograr una razonable estabilidad de la información y prevenir futuros accesos no autorizados que interrumpan el flujo normal de la empresa.

Este tema abarca los siguientes puntos:

- Seguridad de accesos
- Seguridad de usuarios.

3.1.2.1. Seguridad de Accesos

La seguridad de accesos se refiere al nivel de seguridad de los datos almacenados en la Base de Datos para evitar alguna alteración de la información.

La política de toda empresa con respecto a la seguridad de accesos deberá contemplar los siguientes ítems:

La información almacenada en la Base de Datos deberá recibir un apropiado nivel de protección.

La información se deberá categorizar para así obtener su frecuencia de uso y grado de protección que deberá tener.

Se deberá crear un sistema para clasificar la información para así definir apropiadamente su nivel de protección.

3.1.2.2. Seguridad de Usuarios

La seguridad de usuarios es usada para darles privilegios a los distintos usuarios de una base de datos. Estos privilegios serán para ejecutar sentencias SQL, alterar el funcionamiento de la Base de Datos o para alterar la forma de la Base de Datos.

Deberá de existir una política definida para la seguridad de usuarios y accesos de estos a la Base de Datos

Se deberá crear horarios de acceso para los diferentes usuarios y así registrar todo acceso no autorizado o fuera de horario que los usuarios tengan a la Base de Datos.

Se deberán de crear roles para los distintos usuarios de la Base de Datos, clasificarlos y catalogarlos, para su correcta asignación a los usuarios.

3.2. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS EN SGBD

3.2.1. Requerimiento de Seguridad

La gerencia de TIC, debe identificar sus requerimientos de seguridad para ello cuenta con los siguientes insumos:

- **Evaluación de Riesgo**

  La evaluación de riesgo debe ser capaz de ayudarle a identificar eventos que podrían afectar negativamente a sistemas gestores de base de datos. Eso incluye los daños potenciales que podrían causar tales eventos, la cantidad de tiempo necesaria para recuperar/restaurar bases de datos, y las medidas preventivas o controles que deben mitigar las probabilidades de que esos eventos ocurran.

  Para comenzar con la evaluación de riesgo, empiece identificando los procesos de negocios más críticos que aparecieron en el análisis de impacto al negocio.

  El análisis de riesgos implica la identificación de los mismos, la evaluación de la probabilidad de que el evento ocurra, y la definición de la gravedad de las consecuencias de ese evento. También podría ser útil realizar una evaluación de vulnerabilidad, que ayuda a identificar situaciones en las cuales la organización podría ponerse en mayor riesgo al no llevar a cabo ciertas actividades. Un ejemplo podría ser el riesgo cada vez mayor que existe de ataques de virus si no se utiliza el antivirus más actual. Finalmente, los resultados del análisis de riegos se resumen en un informe para la dirección, que incluye actividades recomendadas de mitigación. Podría ser útil buscar vulnerabilidades mientras se realiza el análisis de riesgo.

- **Requisitos Para el Procesamiento de la Información**

  Durante el análisis y evaluación de riesgo se debe generar los requisitos, o establecer catálogos de requisitos de los cuales, se analizará con profundidad y se dará respuesta a los riesgos y las vulnerabilidades que pueda existir en un sistema gestor de base de datos, dentro de una organización.

3.2.2. Selección e Implantación de Controles

Una vez identificado los requerimientos de seguridad y los factores de riesgo, se deben seleccionar e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable.

Los controles deben seleccionarse teniendo en cuenta el costo de implementación, en relación con los riesgos a reducir.

3.3. NORMAS DE SEGURIDAD DE SISTEMAS Y GESTIÓN DE RIESGO

3.3.1. Norma ISO/IEC 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

ISO 27001 propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas o sea tratada en reuniones etc.

Norma que especifica los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI documentado dentro del contexto global de los riesgos de negocio de la organización. Especifica los requisitos para la implantación de los controles de seguridad hechos a medida de las necesidades de organizaciones individuales o partes de las mismas”

3.4. HERRAMIENTAS

Las herramientas utilizadas para la elaboración del presente proyecto de grado son las siguientes:

3.4.1. Postgresql 9.6

PostgreSQL es un gestor de bases de datos orientadas a objetos (SGBDOO o ORDBMS en sus siglas en inglés) muy conocido y usado en entornos de software libre porque cumple los estándares SQL92 y SQL99, y también por el conjunto de funcionalidades avanzadas que

soporta, PostgreSql puede funcionar en múltiples plataformas lo que lo sitúa al mismo o a un mejor nivel que muchos SGBD comerciales.

PostgreSql se distribuye bajo licencia BSD, lo que permite su uso, redistribución, modificación con la única restricción de mantener el copyright del software a sus autores,

A su vez la versión postgresql 9.6, despliega un sin número de mejoras y ventajas de las cuales podemos señalar a continuación:

- **Escalabilidad en máquinas multiprocesador:**

    - Las versiones 9.5 y 9.6 aportan numerosas ventajas entre las que destacamos una mayor escalabilidad.
    - La shared_buffer de PostgreSQL puede almacenar hasta centenares de gigabytes sin ningún tipo de problema
    - Escalabilidad lineal con el número de procesadores, al menos hasta 128 cores/máquina
    - Mejoras notables en el uso de tablespaces para maximizar la concurrencia
    - Cuenta con el soporte del uso de múltiples procesadores para atender una única consulta con Full/SeqScan

- **Concurrencia máxima:**
    - Mejor implementación de MVCC, sin limitaciones en el tamaño y duración de transacciones
    - Implementación completa de SSI (Serializable Snapshot Isolation), para garantizar la consistencia de los datos (Oracle no dispone de SSI completo)
    - Locking mínimo en operaciones con tablas relacionadas (relaciones maestro detalle con Foreign Keys de múltiples niveles que ejecutan actualizaciones concurrentemente).

En postgresql 9.6. No hay contención por el uso de cada almacenamiento en despliegues de alta disponibilidad (cada nodo es independiente) y el rendimiento en lectura escala linealmente con el número de discos que se asignen (siempre y cuando el patrón de consultas lo permita.

Trae como novedad el uso automático de “abbreviated keys” para mejorar significativamente el rendimiento de operaciones indexadas sobre datos textuales

Incorpora soporte de TABLESAMPLE, para optimizar el procesado de tablas enormes, además de método de indexado BRIN, que genera diccionarios “resumidos” para tablas.

- **Disponibilidad Optima**

En general, las sentencias DDL son transaccionales. En caso de fallo, se pueden revertir completamente los cambios. Esto permite llevar a cabo gran cantidad de operaciones sobre la estructura de los datos sin bloqueos, y además puede seguir ejecutando SELECT / INSERT / UPDATE / DELETE durante un ALTER.

3.4.2. Servidor Ubuntu

Ubuntu es un sistema operativo basado en GNU/Linux y que se distribuye como software libre, el cual incluye su propio entorno de escritorio denominado Unity. Su nombre proviene de la ética homónima, en la que se habla de la existencia de uno mismo como cooperación de los demás.

Está orientado al usuario promedio, con un fuerte enfoque en la facilidad de uso y en mejorar la experiencia del usuario. Está compuesto de múltiple software normalmente distribuido bajo una licencia libre o de código abierto. Estadísticas web sugieren que la cuota de mercado de Ubuntu dentro de las distribuciones Linux es, aproximadamente, del 49 %, y con una tendencia a aumentar como servidor web.

Su patrocinador, Canonical, es una compañía británica propiedad del empresario sudafricano Mark Shuttleworth. Ofrece el sistema de manera gratuita, y se financia por medio de servicios vinculados al sistema operativo y vendiendo soporte técnico. Además, al mantenerlo libre y gratuito, la empresa es capaz de aprovechar los desarrolladores de la comunidad para mejorar los componentes de su sistema operativo. Extraoficialmente, la comunidad de desarrolladores proporciona soporte para otras derivaciones de Ubuntu, con otros entornos gráficos, como Kubuntu, Xubuntu, Ubuntu MATE, Edubuntu, Ubuntu Studio, Mythbuntu, Ubuntu GNOME y Lubuntu.

3.4.3. Servidor Tomcat

Tomcat es un contenedor de servlets, puede utilizarse como un servidor de aplicaciones Web con HTML, servlets y JSPs, o como complemento al servidor Apache, Bien integrado en eclipse Implementación de referencia para Java Server Pages (JSP) y Java Server Faces (JSF)

Para que Tomcat funcione es necesario que se encuentre instalado el JDK de Java y que exista la variable de entorno JAVA_HOME que apunte al directorio de instalación del JDK, si no se encuentra podemos definirla con export JAVA_HOME=[ruta jdk] en Linux y con set JAVA_HOME=[ruta jdk] en Windows. Para instalar Tomcat simplemente debemos descomprimir el contenido del archivo en un directorio, también podemos usar la versión con instalador para plataformas Windows.

3.4.4. Lenguaje de Programación J2EE

J2EE, la plataforma creada por SUN en el año 1997 es según nuestra opinión la que ofrece mejores perspectivas de desarrollo para empresas que quieran basar su arquitectura en productos basados en software libre. J2EE, nos ofrece entre otras las siguientes ventajas:

Soporte de múltiples sistemas operativos: Al ser una plataforma basada en el lenguaje Java, es posible desarrollar arquitecturas basadas en J2EE utilizando cualquier sistema operativo donde se pueda ejecutar una máquina virtual Java.

Organismo de control: La plataforma J2EE está controlada por el JCP, un organismo formado por más de 500 empresas. Entre las empresas que lo forman están todas las más importantes del mundo informático (SUN, IBM, Oracle, SAP, HP, AOL, etc.) lo que garantiza la evolución de la misma.

Soluciones libres: En la plataforma J2EE es posible crear arquitecturas completas basadas única y exclusivamente en productos de software libre. No sólo eso, sino que los arquitectos normalmente disponen de varias soluciones libres para cada una de las partes de su arquitectura.

3.4.5. Lenguaje de Vistas JSP

Java Server Pages (JSP),) es una tecnología basada en el lenguaje Java que permite incorporar contenido dinámico a las páginas web. Los archivos JSP combinan HTML con etiquetas especiales y fragmentos de código Java.

El código fuente de una página JSP puede contener:

- Directivas: Indican información general de la página, como puede ser importación de clases, página a invocar ante errores, si la página forma parte de una sesión, etc.
- Declaraciones: Sirven para declarar métodos o variables.
- Expresiones: Expresiones Java que se evalúan y se envían a la salida.

3.4.6. Nmap

Es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon, Fue creado originalmente para Linux aunque actualmente es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Este software posee varias funciones para sondear redes de computadores, incluyendo detección de equipos, servicios y sistemas operativos. Estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la red incluyendo latencia y congestión de la misma.

3.4.7. Ping

Como programa, ping es una utilidad diagnóstica en redes de computadoras que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP por medio del envío de paquetes ICMP de solicitud (ICMP Echo Request) y de respuesta (ICMP Echo Reply). Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.

Ejecutando Ping de solicitud, el Host local envía un mensaje ICMP, incrustado en un paquete IP. El mensaje ICMP de solicitud incluye, además del tipo de mensaje y el código del mismo, un número identificador y una secuencia de números, de 32 bits, que deberán coincidir con el mensaje ICMP de respuesta; además de un espacio opcional para datos. Como protocolo ICMP no se basa en un protocolo de capa de transporte como TCP o UDP y no utiliza ningún protocolo de capa de aplicación.

3.4.8. Consola Ubuntu

Hoy en día en Linux todavía podemos usar la Terminal para hacer algunas tareas, de hecho se usa mucho y es por la sencilla razón de que para algunas cosas es mucho más rápido y más fácil hacerlas desde la Terminal que desde el entorno gráfico, aunque parezca mentira. Además, parece que al tener que teclear algo va a ser más difícil hacerlo que si lo hiciésemos con el ratón en un entorno gráfico, pero no es así, desde el entorno gráfico es más cómodo porque no tenemos que estar buscando las letras en el teclado, sin embargo con el tiempo descubres que es mejor usar la Terminal para algunas cosas.

CAPÍTULO IV
MARCO INSTITUCIONAL

4.1. UNIVERSIDAD AMAZÓNICA DE PANDO

4.1.1. Reseña Histórica de la U.A.P.

La Universidad Amazónica de Pando, una Institución de formación superior, fue aprobada bajo la presidencia del Dr. Hernán Siles Suazo, en el VI Congreso de Universidades, realizado en Tarija en el año 1983 y creada por D.S No. 20511.

Mediante cabildo abierto en el año 1993, el pueblo plantea al Comité Ejecutivo de la Central Obrera Departamental, la necesidad del funcionamiento de la Universidad y solicita la transferencia del edificio del Ex Banco del Estado, en favor de la Universidad, y es así que inicia su funcionamiento a partir del 23 de septiembre de 1993.

Por lo tanto, inicia su labor académica en el año 1994 con el nombre de Universidad Técnica de Pando, con las Carreras de: Biología con 173 postulantes y Enfermería con 104, ambas a nivel de Licenciatura, luego de algunos años se la denominó "Universidad Amazónica de Pando" por acuerdo del Comité de Funcionamiento de la misma Universidad.

4.1.2. Misión, Visión y Objetivos Institucionales

La U.A.P. tiene la misión de formar profesionales idóneos de reconocida calidad y excelencia, con conciencia crítica y capacidad para crear, adaptar, transformar la ciencia y tecnología universal para el desarrollo y progreso de la región y la nación, promoviendo la investigación científica e interacción social, difundiendo y acrecentando el patrimonio cultural y la soberanía del país.

Su visión es ser una institución con acreditación regional, nacional e internacional, promueve el aprovechamiento racional y sostenible de los recursos naturales, contribuyendo al desarrollo socioeconómico de la región y del País, mediante la formación de profesionales idóneos y la generación de actividades científico-investigativo e interacción social, con identidad cultural y profundo sentimiento de soberanía nacional.

4.1.3. Objetivos Institucionales

La Universidad Amazónica de Pando tiene como objetivo Impulsar el desarrollo de un sistema educativo promoviendo la transformación hacia la excelencia, pertinencia y equidad, integrando la productividad y el desarrollo sostenible en todas sus áreas, formando profesionales capaces de resolver los problemas reales de la región y la nación (2008 – 2012).

Por otro lado, se propone:

- Formar profesionales de excelencia en pregrado y Postgrado.
- Fortalecer la investigación científica y tecnológica pura y aplicada.
- Perfeccionar la gestión de los procesos universitarios.
- Internacionalización, cooperación y relaciones internacionales.
- Fortalecer la interacción social y extensión universitaria.

4.2. INCORPORACIÓN DE FAUTAPO A LA U.A.P.

La Universidad Amazónica de Pando ha asumido dentro de sus retos principales la transformación curricular de sus programas de estudio con el propósito de mejorar la oferta formativa, basándose en un nuevo enfoque de Formación Basada en Competencias (F.B.C.), no solo por encontrarse en el centro de la política educativa de muchos países internacionales y en diversos niveles, sino, porque permite a todos los docentes desempeñarse con idoneidad, ya que las competencias constituyen la base fundamental para orientar el currículo, la docencia, el aprendizaje y la evaluación desde un marco de calidad, así mismo, brinda principios, indicadores y herramientas para hacerlo, más que cualquier otro enfoque educativo, en respuesta a las demanda del contexto y la necesidad de mejorar permanentemente la calidad y pertinencia de la formación de futuros profesionales tomando en cuenta las necesidades locales y nacionales, actuales y a futuro, en relación al desempeño requerido para un profesional y elevar el nivel de competitividad de otras universidades del País.

Las competencias son un enfoque para la educación y no un modelo pedagógico, pues no pretenden ser una representación ideal de todo el proceso educativo, determinando cómo debe ser el proceso instructivo, el proceso desarrollador, la concepción curricular, la concepción didáctica

y el tipo de estrategias didácticas a implementar. Al contrario, las competencias son un enfoque porque sólo se focalizan en unos aspectos específicos de la docencia, del aprendizaje y de la evaluación.

El enfoque de competencias implica cambios y transformaciones profundas en los diferentes niveles educativos, y seguir este enfoque es comprometerse con una docencia de calidad, buscando asegurar el aprendizaje de los estudiante, adaptándose a nuevos perfiles ocupacionales, al trabajo en equipo, a una mayor flexibilidad, creatividad y capacidad de aprendizaje, liderazgo y a la actualización continua de conocimientos y habilidades que le permitan lograr un desempeño eficiente y un desarrollo integral.

4.3. DIRECCIÓN DE INFORMACIÓN ACADÉMICA

4.3.1. Organigrama de la Dirección de Información Académica

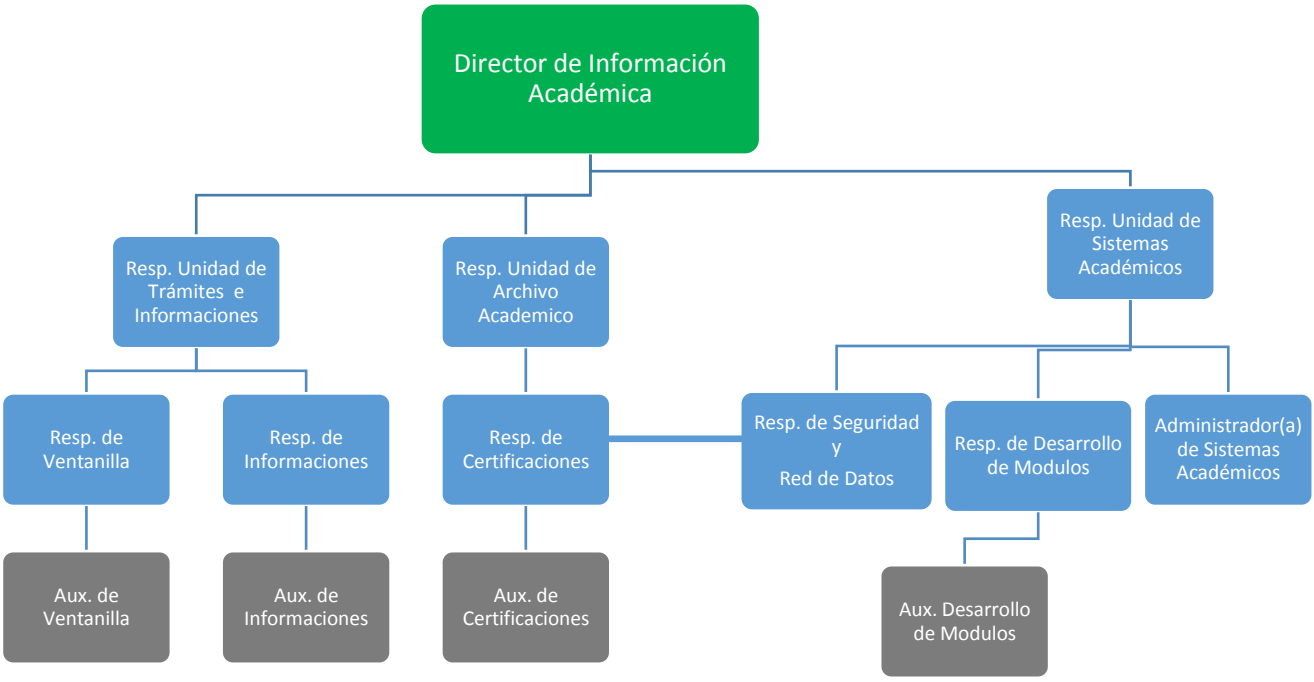


FIGURA 6: *Organigrama de la DIA*
Fuente: Dirección de Información Académica

4.3.2. Misión

Gestionamos información, con el fin de brindar un servicio eficiente a la comunidad universitaria y población en general, aplicando las nuevas tecnologías de información y comunicación, para contribuir al desarrollo académico administrativo en la Universidad Amazónica de Pando.

4.3.3. Visión

Ser una Dirección técnica transparente en la gestión de la información, que brinda un servicio óptimo a la comunidad universitaria y población en general, aplicando de manera óptima y eficiente las nuevas tecnologías de información y comunicación; siendo un referente institucional en la Universidad Amazónica de Pando.

4.3.4. Valores

- Honestidad.
- Ética.
- Compromiso institucional.
- Responsabilidad.
- Respeto.
- Humanismo, respeto a los derechos humanos.
- Tolerancia.
- Equidad de género.
- Equidad generacional.
- Trabajo en equipo.
- Organización.
- Transparencia
- Principios
- Respetar la Autonomía Universitaria de la UAP.
- Respetar el Co-gobierno paritario Docente-Estudiantil.
- Respetar las normas y políticas que se encuentren enmarcados dentro de la UAP, el Sistema Universitario y el Estado Plurinacional de Bolivia

4.3.5. Políticas de Calidad

La Dirección de Información Académica de la Universidad Amazónica de Pando para los procesos de admisión, matriculación y certificación, brinda un servicio oportuno seguro y eficaz en gestión de información con el fin de satisfacer las expectativas de la comunidad universitaria y población en general, con recursos humanos competentes, mejorando continuamente la eficacia del Sistema de Gestión de Calidad y sus procesos en el ámbito de la información y la comunicación.

4.3.6. Objetivos de Calidad

- Mejorar continuamente el sistema de atención a la comunidad universitaria y usuarios en general, reduciendo en un 5 % en el tiempo de entrega de trámite
- Desarrollar mecanismos eficaces de seguridad de la documentación físico-digital de los procesos de admisión, matriculación y certificación, con el resguardo de al menos 2 copias diarias de toda la información registrada en el sistema académico siringuero.

4.4. UNIDAD DE SISTEMAS ACADÉMICOS

4.4.1. Antecedentes

La creación del sistema Siringuero fue realizado por Fautapo, institución dedicada en la innovación tecnológica, después de una serie de pruebas se implementó en la UAP el año 2006.

- A principios de la implementación el sistema Siringuero ha dependido de la USIC, desde los inicios del año 2006 hasta los fines del año 2009, y fue soportado por un administrador de sistemas.
- A partir del año 2010 el sistema Siringuero ha pasado a depender de la Dirección de Información Académico, de la misma forma fue soportado por un administrador de sistemas.
- En el año 2011 el Sistema Siringuero paso a depender de la Unidad de Sistema de Pre y Postgrado dependientes de la Dirección de Postgrado, año también que el sistema de Postgrado fue migrado al Sistema Siringuero.

- En el año 2012 la Unidad de Sistemas de Pre y Postgrado pasa depender de la Dirección Académica de Vice-Rectorado, año en que ingresan nuevas autoridades de la UAP, año también en que se incrementa dos funcionarios.
- El año 2014 pasa a ser Unidad de Sistemas Académicos, dependientes de la Dirección de Información Académica, hasta la fecha y se han incrementado tres funcionarios adicionales.

4.4.2. Objetivos de la U.S.A

Brindar un servicio eficiente de sistemas de información y comunicación académica tomando en cuenta los aspectos tecnológicos de primer nivel, de esta manera pueda satisfacer las necesidades de la comunidad universitaria y la población en general.

4.4.3. Organigrama

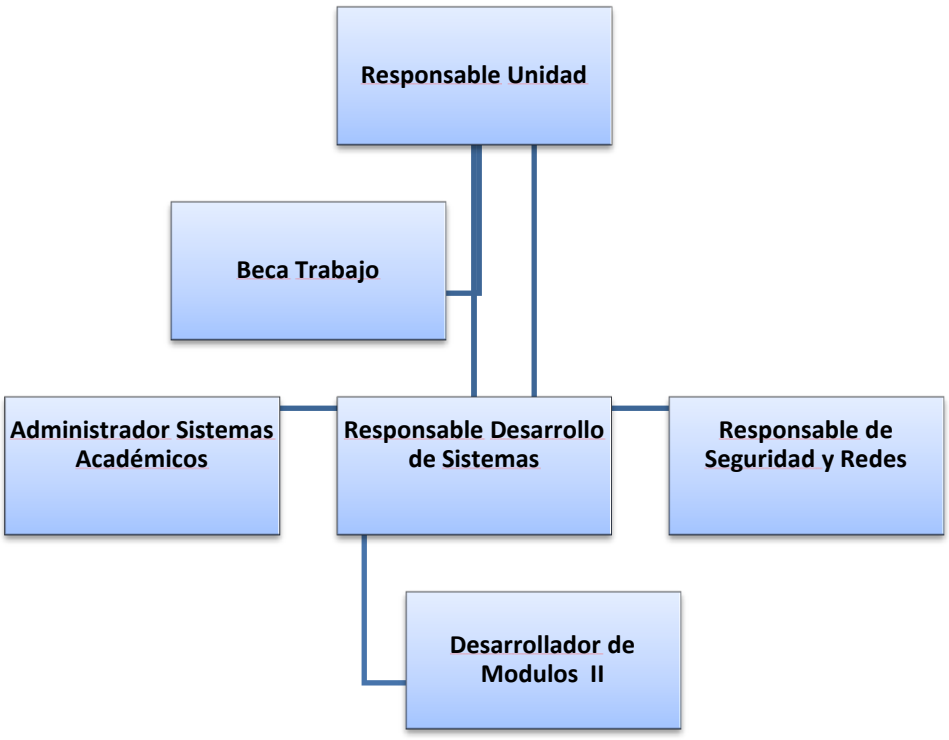


FIGURA 7: Organigrama USA
Fuente: Unidad de Sistemas Académicos

CAPÍTULO V
MARCO APLICATIVO

5.1. REQUERIMIENTOS DE SEGURIDAD DEL GESTOR DE BASE DE DATOS-SIRINGUERO

5.1.1. Análisis de Riesgo del Gestor de Base de Datos-Siringuero

Nro.	Descripción de Requisitos
1.	Configuración de Parámetros para la Matriz de Análisis de Riesgo en SGBD y Controles de Seguridad
2.	Matriz de Análisis de Riesgos
3.	Mapa de Riesgo Inherente
4.	Amenaza de Riesgos Físicos
5.	Amenaza de Riesgos Lógicos

TABLA 1: *Requisitos Control de Riesgos*
Fuente: Elaboración Propia

La tabla 1. establece el catálogo de requisitos de control de riesgo la cual se define en dos etapas, siendo la primera etapa la seguridad física que corresponde al análisis de los riesgos y las vulnerabilidades de la infraestructura y el equipamiento físico del entorno del gestor de base de datos en la Unidad de Sistemas Académicos, siendo la segunda etapa concierne a la seguridad lógica la cual corresponde al análisis de riesgo, vulnerabilidades del software y las implicaciones similares que están involucradas en el funcionamiento del Sistema Gestor de Base de Datos.

5.1.2. Mantenimiento del Gestor de Base de Datos-Siringuero

Nro.	Descripción de Requisitos
1.	Instalación y Configuración del Servidor Ubuntu 16.04
2.	Instalación y Configuración de Aplicaciones del Sistema Siringuero
3.	Instalación de PostgreSql 9.6
4	Migración de la Estructura de la Base de Datos Siringuero
5.	Migración de Funciones, Triggers y Dominios
6.	Mantenimiento de Índices Primarios y Secundarios
7	Detalle de la Infraestructura del Gestor de Base de Datos Siringuero

TABLA 2: *Mantenimiento del Sistema Gestor de Base de datos Siringuero*
Fuente: elaboración propia

En la tabla 2, se establece el catálogo de requisitos referente a la migración del Sistema del Gestor de Base de Datos Postgresql 8.1 a 9.6

Para efectuar la migración se ha realizado una ardua investigación referente a instalación y configuración de prueba y error , la cual corresponde a la instalación del Sistema Operativo Servidor Ubuntu 16.04, PostgreSql 9.6 , implementación de la estructura y los Datos de la versión anterior, a partir de los resultados de las actividades que se han ejecutado, se ha realizado ejecución prueba y error, desde la aplicación del Sistema Siringuero, esto referente a la migración de la Estructura de las funciones y despliegues, de esta manera como última tarea se ha realizado el mantenimiento de la estructura de las tablas y los índices.

5.1.3. Implementación de Medidas de Seguridad del Gestor de Base de Datos del Sistema Siringuero

Nro.	Descripción de Requisitos
1.	Asignación de Contraseña al Súper Usuario Postgres
2.	Creación de Usuarios y Roles
3.	Configuración de Accesos
4.	Configuración de Conexiones
5.	Configuración del Firewall UFW

TABLA 3: *Implementación de Medidas de Seguridad del SGBD Siringuero*
Fuente: Elaboración Propia

En la tabla 3, refleja el catálogo de requisitos para la implementación de medidas de seguridad en el Gestor de Base de Datos Siringuero, para lo cual se ha establecido la configuración a priori del súper usuario postgres, creación, asignación de usuario y roles, configuración de accesos y privilegios para cada usuario y establecimiento de conexiones al gestor de base de datos. De igual forma se ha realizado la instalación del firewall UFW y la configuración de políticas de acceso a la plataforma del Servidor del Gestor de Base de Datos Siringuero.

5.2. ANÁLISIS DE RIESGO EN EL GESTOR DE BASE DE DATOS SIRINGUERO

Se realizó el análisis de riesgo del Sistema Gestor de Base de Datos, aplicando la herramienta de matriz de riesgos desde la óptica de amenazas de riesgo físico como amenazas de riesgo lógico, a continuación se describe de manera detallada cada uno de estos componentes en el presente acápite, tal cual se establece en el catálogo de requisitos:

5.2.1. Matriz de Análisis de Riesgo

Para desarrollar la matriz de análisis de riesgo se ha definido parámetros de probabilidad y valores promedio, los factores de riesgo, amenazas y vulnerabilidades, a partir de esta configuración se obtienen resultados de Análisis de Riesgo Promedio y análisis de factores de riesgo.

5.2.1.1. Parámetros de Probabilidad de Valores Promedio

Para desarrollar la matriz de análisis de riesgo se ha identificado amenazas y factores de riesgo para lo cual, se ha definido valores de magnitud de riesgo y promedios de probabilidades, la escala de probabilidades están definido por ninguna=1, baja=2, mediana=3 y alta=4, a partir de esta escala de probabilidades, se obtiene la magnitud de riesgo de 1 a 3 que corresponde al umbral de riesgo medio, y de 2.6 a 4 corresponde al umbral de riesgo alto, tal cual se observa en la Tabla 4.

5.2.1.2. Matriz de Análisis de Riesgo de Datos e Información, Equipamiento e Infraestructura, Software y Aplicaciones

Para desarrollar la matriz de análisis de riesgo se ha definido factores de riesgos como, software y aplicaciones, datos e información y equipamiento e infraestructura , por otro lado se ha definido la clasificación de factores de riesgos, la integridad, confiabilidad y la disponibilidad, además se ha tomado en cuenta las magnitudes de riesgo, ya que se ha incluido para cada factor de riesgo las amenazas y vulnerabilidades como ser: Actos originados por Agente externo-Hacker, Sucesos de Riesgos Físicos y Sucesos de Riesgos Lógicos .

Una vez definido los índices de la matriz se procedió al registro de la misma, aplicando valores de magnitud de riesgos, para cada factor de riesgos y las amenazas correspondientes.

Se ha realizado la matriz para cada factor de riesgo, tomando en cuenta la clasificación de la magnitud de riesgo, tal cual se observa en las tablas 5,6 y 7 correspondientemente.

En la matriz se puede observar los valores de la magnitud de riesgos resaltados en 3 diferentes colores, en la cual el color verde describe el promedio de la probabilidad baja, el color amarillo describe el promedio de la probabilidad mediana, y el color rojo describe el promedio de la probabilidad alta, tal cual se observan en las Tablas 5,6 y 7.

5.2.1.3. Análisis de Riesgo Promedio

La tabla 8 describe el resultado a partir de la matriz de análisis de riesgo desarrollada, la cual se refleja en las tablas 5,6 y 7, estos resultados son básicamente la intersección de magnitud de daño y probabilidad de amenaza.

5.2.1.4. Análisis de factores de riesgo

La figura 8 describe el análisis de los factores de riesgo en forma de un Grafico estadístico en la cual se puede observar claramente que el factor equipamiento e infraestructura se aproxima al Umbral de Riesgo medio. Así mismo se puede observar los factores datos e información y software de aplicación se encuentra debajo del Umbral de medio riesgo. Esto

Estos significa que las probabilidades de riesgos y las amenazas se encuentras en aspectos físicos del entorno del gestor de base de datos Siringuero.

Parámetros de Probabilidad de Valores Promedio						
Valoración	**Escala**	**Valor min**	**Valor máx.**	**Líneas**	**Umbral Medio Riesgo**	**Umbral Alto Riesgo**
Ninguna	1	1	3		**7**	**10,5**
Baja	2	4	6	**x**	**Y**	**Y**
Mediana	3	8	9	1,0	7,0	10,5
Alta	4	12	16	1,1	6,4	9,5
				1,2	5,8	8,8
				1,3	5,4	8,1
				1,4	5,0	7,5
				1,5	4,7	7,0
				1,6	4,4	6,6
				1,8	4,0	6,0
				1,8	3,9	5,8
				1,9	3,7	5,5
				2,0	3,5	5,3
				2,1	3,3	5,0
				2,2	3,2	4,8
				2,3	3,0	4,6
				2,4	2,9	4,4
				2,5	2,8	4,2
				2,6	2,7	4,0
				2,7	2,6	3,9
				2,8	2,5	3,8
				2,9	2,4	3,6
				3,0	2,3	3,5
				3,1	2,3	3,4
				3,2	2,2	3,3
				3,3	2,1	3,2
				3,4	2,1	3,1
				3,5	2,0	3,0
				3,6	1,9	2,9
				3,7	1,9	2,8

TABLA 4: *Parámetros Probabilidad de Valores Promedio*
Fuente: Elaboración Propia

Matriz de Análisis de Riesgo de Datos e Información

Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]						
Datos e Información	Clasificación			Magnitud de Riesgo 1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	Actos Originados por los Agentes Externos-Hacker						
	Integridad	Confiabilidad	Disponibilidad		Infiltración en la Red de Datos	Infección de Virus	Alteración de Datos y Estructura de Base de Datos	Sabotaje (Ingeniería Social)	Daños por vandalismo	Extorsión	Robo / Hurto de información
					2	3	3	2	1	1	3
Copia de Seguridad BD	x			**3**	6	9	9	6	3	3	9
Reportes Estadísticos Impresos	x			**1**	2	3	3	2	1	1	3
Reportes Estadísticos Digitales	x			**1**	2	3	3	2	1	1	3
Código fuente del Sistema Siringuero	x			**3**	6	9	9	6	3	3	9
Estructura de Base de Datos		x		**3**	6	9	9	6	3	3	9
Procedimientos de SGC			x	**2**	4	6	6	4	2	2	6
Instructivos SGC			x	**2**	4	6	6	4	2	2	6

Bases de Datos Al fresco		**x**		**3**	6	9	9	6	3	3	9
Formularios de SGC			**x**	**2**	4	6	6	4	2	2	6
Informes Técnicos			**x**	**1**	2	3	3	2	1	1	3
Políticas de Seguridad			**x**	**2**	4	6	6	4	2	2	6
Manuales de Usuario			**x**	**2**	4	6	6	4	2	2	6
Transacciones	**x**			**3**	6	9	9	6	3	3	9
Notas Regulares	**x**			**3**	6	9	9	6	3	3	9
Copias de Videos de Cámaras de Seguridad			**x**	**2**	4	6	6	4	2	2	6

TABLA 5: *Matriz de Análisis de Riesgo de Datos e Información*
Fuente: Elaboración propia

Matriz de Análisis de Riesgo de EquipamientoE infraestructura											
Equipamiento e Infraestructura	**Clasificación**			**Magnitud de Riesgo 1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto**	**Sucesos de Riesgo Físicos**						
	Integridad	**Confiabilidad**	**Disponibilidad**		**Temperatura del Ambiente**	**Equipo Computacional Desactualizado**	**Incendio**	**Aire Acondicionado Inestable**	**Funcionamiento del Servidor de Aplicaciones y Base de Datos en un Equipo**	**Falla de corriente (apagones)**	**Falla de Sistema**
					2	2	3	3	3	3	4
Equipos de la red cableada (router, switch, etc.)			x	3	6	6	9	9	9	9	12
Equipos de la red inalámbrica (router, punto de acceso, etc.)			x	3	6	6	9	9	9	9	12
Cortafuego			x	3	6	6	9	9	9	9	12
Servidores			x	2	4	4	6	6	6	6	8
Computadoras de Escritorio			x	3	6	6	9	9	9	9	12
Portátiles			x	2	4	4	6	6	6	6	8
Impresoras			x	4	8	8	12	12	12	12	16
Memorias Flash			x	2	4	4	6	6	6	6	8
Oficina				4	8	8	12	12	12	12	16

TABLA 6: *Matriz de Análisis de Riesgo de Equipamiento e Infraestructura*
Fuente: Elaboración Propia

Matriz de Análisis de Riesgo Software y Aplicaciones												
Software y Aplicaciones	**Clasificación**			**Magnitud de Riesgo 1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto**	**Sucesos de Riesgos Lógicos**						
	Integridad	**Confidencialidad**	**Disponibilidad**		**Sistema Operativo Exento de Configuración**	**Gestor de Base de Datos Desactualizado**	**Configuración por defecto del Gestor de Base de Datos**	**Base de Datos Siringuero exento de Mantenimiento**	**Aplicaciones de Base Obsoletas**	**Exento de Firewall a nivel de Sistema Operativo**	**Antivirus Desactualizado**
					3	3	3	3	2	3	2
Gestor de Base de Datos PostgreSql		X		3	9	9	9	9	6	9	6
Servidor Tomcat			x	3	9	9	9	9	6	9	6
S.O Ubuntu Server			x	2	6	6	6	6	4	6	4
Sprint Frame Work			x	2	6	6	6	6	4	6	4
Lenguaje J2EE			x	2	6	6	6	6	4	6	4
Software de Gestión de Procesos			x	1	3	3	3	3	2	3	2
Paquetes de Office			x	1	3	3	3	3	2	3	2
Aplicaciones de Sistema Al fresco			x	1	3	3	3	3	2	3	2
Software de Diseños			x	1	3	3	3	3	2	3	2

TABLA 7: *Matriz de Análisis de Riesgo Software y Aplicaciones*
Fuente: Elaboración Propia

Análisis de Riesgo Promedio

		Probabilidad de Amenaza		
		Actos Originados por los Agentes Externos-Hacker	**Sucesos de Riesgos Físicos**	**Sucesos de Riesgos Lógicos**
Magnitud de Daño	**Datos e Información**	4,7	0,0	0,0
	Equipamiento e Infraestructura	0,0	8,3	0,0
	Software y Aplicaciones	0,0	0,0	3,6

TABLA 8: *Análisis de Riesgo Promedio*
Fuente: Elaboración Propia

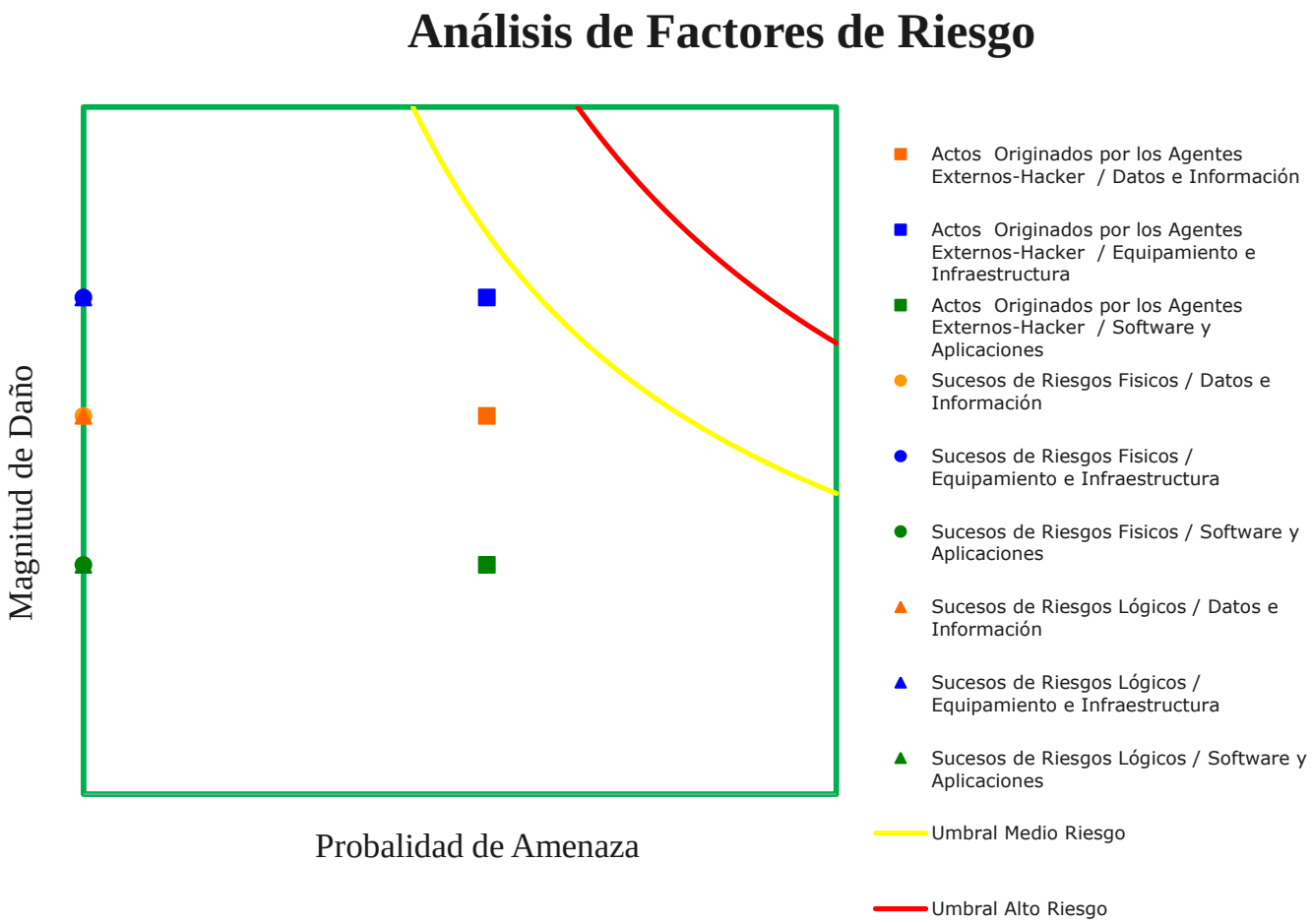


FIGURA 8: *Análisis de Factores de Riego*
Fuente: Elaboración Propia

5.2.2. Sucesos de Riesgos Físico

De acuerdo al análisis de riesgo realizado de la infraestructura del entorno del Gestor de Base de Datos Siringuero, se ha determinado establecer los riesgos concernientes al aspecto físico de los dos componentes constituidos en el catálogo de requisitos.

En tal sentido se puede clasificar los riesgos físicos de la siguiente manera.

5.2.2.1. Riesgos de la Infraestructura del Ambiente del SGBD

El ambiente en el que se encuentra implementado el Sistema Gestor de Base de Datos Siringuero es una de las vulnerabilidades de mayor riesgo para la seguridad de los datos que se resguarda en la base de datos, para ello se ha tomado una imagen la cual describe de manera explícita el estado actual del ambiente.

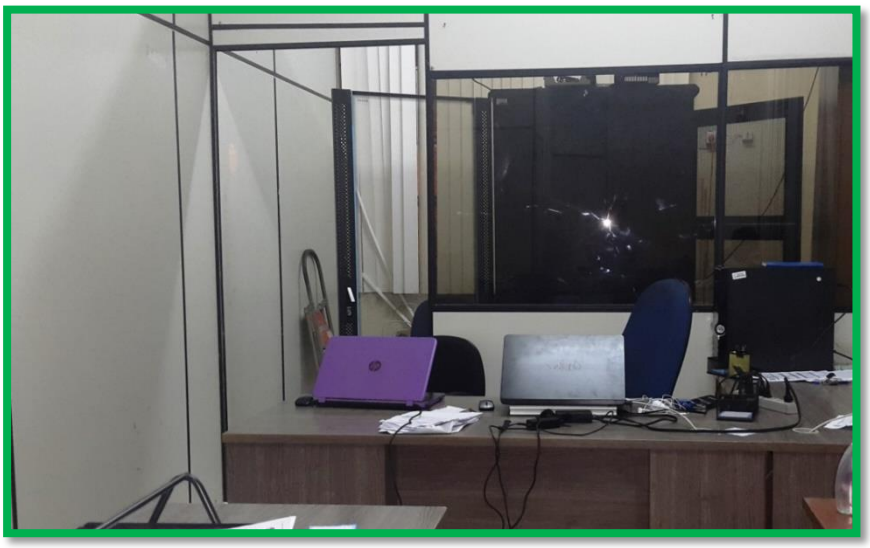


FIGURA 9: *Acceso al Servidor del Sistema Siringuero*
Fuente: Elaboración Propia

En la Figura 9, se observa el acceso a la infraestructura del Rack del servidor del Sistema Siringuero, tal como se muestra en la imagen el acceso no cuenta con restricción alguna, esta es una de las vulnerabilidades al acceso físico, cuyo equipo está expuesto a daños, robos y conectividades de dispositivos, por agentes externos no autorizados que tengan la intencionalidad de dañar la integridad del servidor y de esta manera los datos que alberga dicho servidor.

El servidor del Sistema Gestor de la Base de Datos Siringuero se encuentra implementado en un ambiente inadecuado, tal cual es así no cuenta con condiciones para albergar servidores que estén en producción adecuada. El ambiente actual carece de la refrigeración, conectividad de la energía eléctrica, cableado estructurado de la Red de datos, alarmas de accesos y cámaras de seguridad.

Las divisiones del ambiente del entorno del gestor de base de datos, está elaborado de material inflamable que está expuesto al mínimo error de incendios, tal cual se observa en la Figura 10.

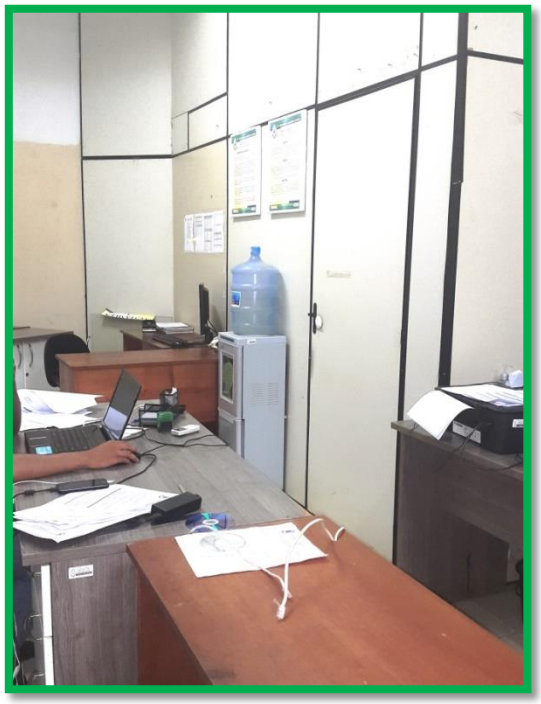


FIGURA 10*: Instalaciones del Ambiente del Gestor de Base de Datos Siringuero*
Fuente: Elaboración Propia

Este ambiente cuenta con tres accesos externos que están expuestos a filtración de agua y humedad en la época de lluvia, y al pleno de la luz solar en el trascurso del día, la cual altera la temperatura interna del ambiente.

El acceso interno es una puerta elaborada de un material de cartón prensado la cual cuenta con una llave de acceso, esta restricción es precaria y vulnerable al acceso de personas no autorizadas al ambiente del servidor del Sistema Siringuero.

Dicho de este modo el análisis del riesgo de la seguridad del entorno del Sistema Gestor de Base de Datos Siringuero, es vulnerable por los aspectos que se ha citado anteriormente, tales como la temperatura del ambiente, accesos inestables, carencias de cámaras y alarmas de seguridad, ambientes no adecuados, entre otros ponen en riesgo la integridad física del servidor del gestor de base de datos Siringuero.

5.2.2.2. Riesgos de Equipos Computacionales

El equipamiento tecnológico instalado en la Unidad de Sistemas Académicos se considera vulnerable por los riesgos que presenta a la hora de poner en funcionamiento el Gestor de Base de Datos Siringuero, tal cual se observa en la Figura 10, la cual describe claramente la situación actual de la instalación de equipos entre computadoras, dispositivos de Red y Alarmas de Seguridad entre otros.

FIGURA 11: *Equipo Computacional SGBD Siringuero*
Fuente: Elaboración Propia

Los equipos computacionales destinados para el funcionamiento del SGBD Siringuero, se han convertido cada vez más en equipos inestables que pueden entrar en pérdida en cualquier instante en su funcionamiento, por el tiempo de uso avanzado de estos equipos.

Uno de los factores por los que no se han adquirido equipos servidores de producción y alternos tantos de Backups de respaldos entre otros, ha sido básicamente por la falta de presupuestos que destina la Universidad , la falencia de los servidores mencionados, hace que se utilice computadoras normales de mesa y de oficina, claramente estos equipos no están destinados para prestar servicio como servidores y gestores de bases de datos ni otro tipos de servicios, el uso de estas computadoras pone en riesgo la integridad física del gestor de base de datos, por ello se considera vulnerable para el resguardo de la seguridad de los datos.

Otro de los equipos que pone en riesgo el funcionamiento del gestor de base de datos relacionados a la conectividad y servicios a conexiones externas son los dispositivos de red, cuyo estado de estos equipos es cada vez más inseguro por la inestabilidad de la energía eléctrica entre otros.

Además se cuenta con 2 Switch programables los cuales son utilizados de manera alternativa por la inestabilidad de energía eléctrica, por estos Switch el Sistema Siringuero extiende sus servicios a las conexiones externas de las redes locales y la salida por internet. Durante las dos últimas gestiones hasta la fecha no se han adquirido ningún otro dispositivo de red que esté de reserva en cuanto presten servicio los dispositivos de red actual.

La carencia de estos dispositivos se considera como un riesgo para la integridad y la funcionalidad del gestor de bases de datos al servicio continuo del sistema Siringuero, ya que podrían entrar en pérdida en cualquier instante los dispositivos de red mencionados, aplacando en totalidad el servicio del sistema mencionado.

Los dispositivos de red mencionados son vulnerables ya que están expuestos al contacto físico de personas externas a los administradores de red y de sistemas, tal cual se observa en la Figura 10, se muestra así mismo la vulnerabilidad por la inadecuada instalación de los cables de red, esta forma de funcionamiento pone en riesgo la seguridad desde todo punto de vista, al no cumplir con normas y estándares de dicha instalación.

Los equipos de alarmas contra accesos, instalados en la parte interna y externa se han deteriorado a medida que han entrado en funcionamiento y en la actualidad no prestan ningún servicio de seguridad a la cual están destinados estos equipos, por lo tanto, no podrán controlarse los accesos

en tanto amerite la restricción de personas no autorizadas al ambiente, en el cual se encuentra instalado el Sistema Gestor de Base de datos Siringuero.

5.2.3. Suceso de Riesgos Lógicos:

Se ha considerado el riesgo de la seguridad lógica a todo aquel software y aplicaciones que se han empleado para la producción del Sistema Gestor de Base de Datos Siringuero, hasta antes de haber implementado el presente proyecto de grado.

Para considerar como factor de riesgo se ha basado en las versiones de las aplicaciones que fueron instaladas y que estás prestaban servicio para el funcionamiento del gestor de base de datos siringuero.

Las cuales se mencionan a continuación:

- **Sistema Operativo Ubuntu Server:** Hasta antes de implementar el presente proyecto de grado, el gestor de base de datos y el Sistema Siringuero prestaba servicio bajo el sistema operativo Ubuntu Server 12.04. , este servidor a pesar de contar con soporte de largo alcance ya se habían lanzado nuevas versiones corrigiendo los riesgos de seguridad y las vulnerabilidades que presentaba dicho servidor, al no haberse migrado a las versiones posteriores presentaba grandes probabilidades de riesgo en cuanto a lo que se refiere a la seguridad de accesos, conectividades y la flexibilidad de configuración. Una de las vulnerabilidades que presenta la versión 12.04 es fundamentalmente la configuración de usuario Root, este factor de configuración pone en gran riesgo la vulnerabilidad de agentes externos. A partir de la versión 13.10 esta vulnerabilidad ha sido corregido obligando a los usuarios que trabajen con la configuración por defecto, dejando la imposibilidad de configurar el usuario Root, el Kernel lanzado par esta versión es Linux 2.6.35, en las posteriores versiones esto ha ido mejorando en las versiones LTS.

- **Servidor Apache Tomcat 5.5:** El Sistema Siringuero al ser implementado bajo la plataforma y modelo MVC y Spring Frame Work, debe trabajar con el servidor Tomcat, la versión mencionada viene funcionando desde la implementación del sistema, es decir desde la gestión 2007 hasta la fecha. Como se podrá observar no se ha actualizado hasta la

fecha la nueva versión del servidor la cual expone los riesgos y las vulnerabilidades, respecto a las nuevas versiones que fueron lanzadas y son estables actualmente.

- **Plataforma MVC Spring FrameWork :** El Sistema Siringuero esta implementado bajo la plataforma Spring Frame Work , la cual incorpora un modelo de funcionamiento MVC, que a priori es exentó de muchas vulnerabilidades, con el simple hecho de la incorporación del lenguaje de programación java, esto libera muchas vulnerabilidades frente a otros lenguajes que son comúnmente utilizados para el desarrollo de aplicaciones web, tales como php, pyton y otros, sin embargo al no haberse migrado a las nuevas versiones se considera vulnerable y pone en riesgo el funcionamiento del Gestor de Base de datos como el Sistema Siringuero.

- **Sistema Gestor de Base de Datos Postgresql 8.1:** La base de datos del Sistema Siringuero fue creado e implementado en la versión de Postgresql 8.1**,** cual fue lanzado en el año 2007, a partir de esta fecha no se ha realizado ningún tipo de migración y/o transferencia de versiones de postgresql hasta antes de haber implementado el presente proyecto de grado. El Gestor de Base de datos del Sistema Siringuero al estar implementado en la versión 8.1, estaba expuesto a un sin números de riesgos y vulnerabilidades que presenta esta versión, para corregir estos riesgos y las vulnerabilidades que están establecidas en las listas comunes de vulnerabilidades CVE, postgres ha lanzado nuevas versiones corrigiendo errores y riesgos de seguridad, tal cual hasta la fecha se cuenta con la versión 9.6 de postgresql, sin embargo hasta el mes de Septiembre del 2016 el Gestor de Base de Datos del sistema Siringuero a un funcionaba con la versión 8.1. la cual fue y es considerada un riesgo enorme para el resguardo de los datos almacenados.

5.3. MANTENIMIENTO EN EL GESTOR DE BASE DE DATOS SIRINGUERO

El mantenimiento del gestor de base de datos tal cual establece la metodología MABDEX-II refiere a la migración de la base de datos, implementada en la versión postgresql 8.1 hacia la versión postgresql 9.3, como a 9.5.4. Y posteriormente se ha migrado a la reciente versión 9.6

esta migración conlleva el mantenimiento de la infraestructura de la base de datos como ser funciones, tablas, índices, dominios y datos, a continuación se describe cada uno de los componentes que se ha establecido en el catálogo de requisitos de mantenimiento en el Sistema Gestor de Base de Datos, tal cual se ha ejecutado las actividades para el mantenimiento de cada uno de los componentes.

5.3.1. Instalación y Configuración del Servidor Ubuntu 16.04

La instalación del gestor de base de datos postgresql 9.6 conllevó además la instalación del sistema operativo Ubuntu Server, por la compatibilidad de las versiones, la versión más reciente del servidor trae consigo por defecto la última versión de postgresql que fue lanzado en agosto del 2016.

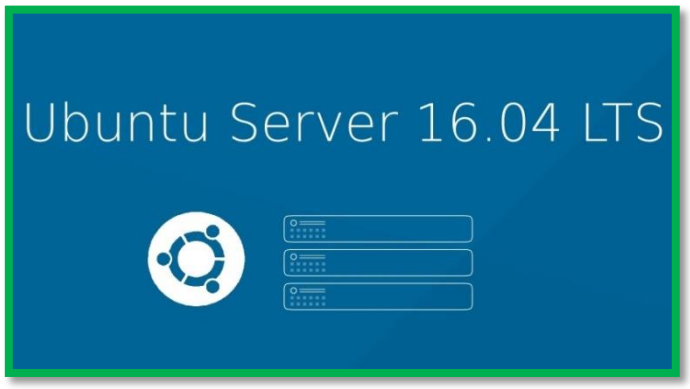


FIGURA 12: *Sistema Operativo Ubuntu Server 16.04*
Fuente: Ubuntu.org.

La versión de Ubuntu server fue lanzado en abril del 2016, esta versión es LTS quedando como última versión de servidores de la familia Ubuntu, en la cual el Gestor de Base de Datos y el Sistema Siringuero se han adaptado de manera excepcional a esta plataforma por lo cual a partir de la gestión 2009 la Unidad de Sistemas ha establecido como sistema operativo base de escritorio y de servidores, para desarrolladores y servicios de sistemas en producción.

Para ello la instalación se ha establecido en un equipo alterno para pruebas y errores mientras la migración del Gestor de la base de datos estaba en curso. Esta última versión del servidor claramente es una versión mejorada de las versiones anteriores en cuanto a la optimización de los

recursos y el kernel que fue implementado para esta versión. La instalación para el funcionamiento adecuado se ha efectuado en el equipo Servidor Dell, con el que cuenta la Unidad de Sistemas Académicos, dicho servidor tiene una memoria de 125 GB, y un disco duro de 16 TB.

Para la configuración del servidor Ubuntu 16.04 se ha realizado de acuerdo a las características, como se observa en la Tabla 9.

Nro.	Componente	Descripción
1	Nombre del servidor	www
2	Usuario del servidor	Sistema
3	IPV4	10.10.10.2
4	DNS	8.8.8.8
5	Nombre de dominio	www.uap.bo
6	Swap	2500000 MB
7	Ext4/	1847152 MB
8	RAM	125000 MB

TABLA 9: *Características de la Configuración de Ubuntu Server*
Fuente: Elaboración Propia

5.3.2. Instalación y Configuración de Aplicaciones del Sistema Siringuero

En la instalación y configuración de aplicaciones que hacen posible el funcionamiento del Sistema Siringuero, se lo realiza desempaquetando archivos compresos desde la unidad emisor hacia la unidad destino, la cual se registra en el directorio /opt, este directorio contiene aplicaciones tales como tomcat, ant ,jdk, Spring frame work y code_qr, para que surta efecto la instalación se configuró tal cual se observa en la Figura 13

Así mismo se describe las características de las aplicaciones en la Tabla 10

Nro.	Aplicación	Versión
1.	Apache Tomcat	5.5
2.	Apache ant	5.5
3	Spring	1.2
4	JDK	1.6
5	Code_qr	1.7

TABLA 10*: Características de las Aplicaciones-Base Sistema Siringuero*
Fuente: Elaboración propia

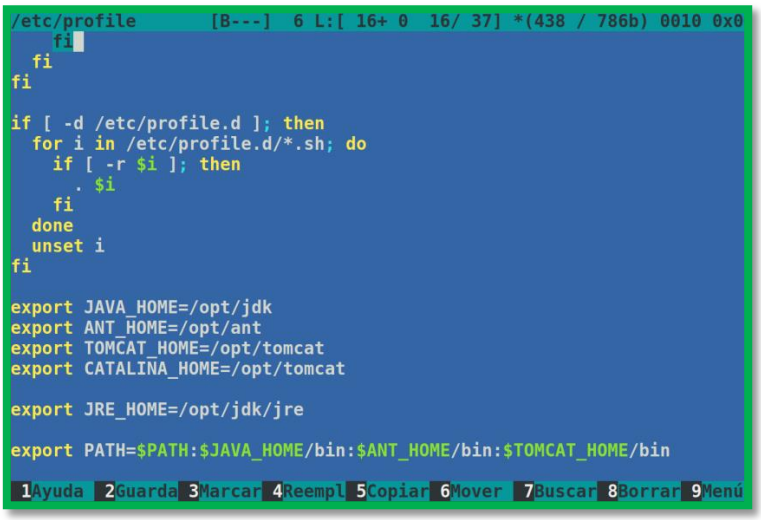


FIGURA 13: *Configuración de la Instalación de aplicaciones del Sistema Siringuero*
Fuente: Elaboración Propia

5.3.3. Instalación de PostgreSql 9.6

Una vez instalado el servidor de aplicaciones y configurado los mismos se realizó la instalación del Sistema Gestor de Base de Datos Postgresql 9.5.4 y 9.6 como componente principal de investigación, para el presente proyecto de grado.

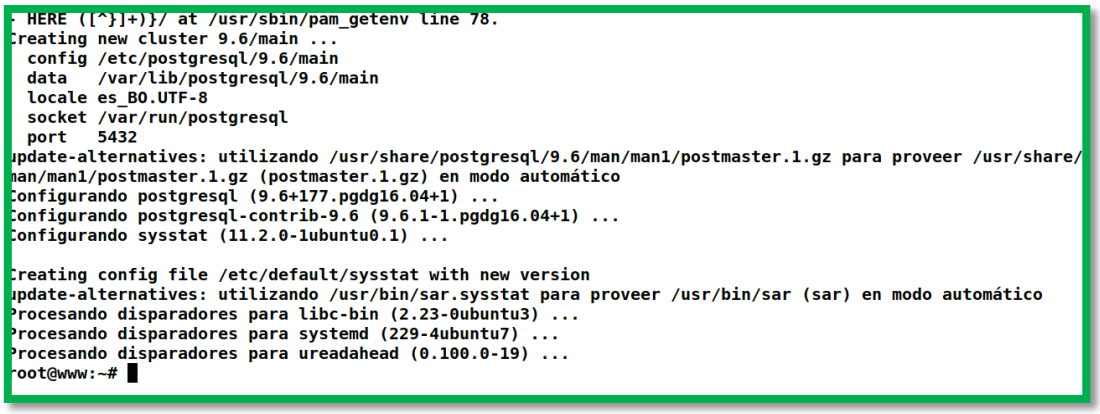


FIGURA 14: *Instalación de PostgreSql 9.6*
Fuente: Elaboración Propia

En la Figura 14 se observa la finalización de la instalación y configuración de Postgresql 9.6, la cual es establecida desde los repositorios de Ubuntu vía internet, tal cual se había mencionado en los acápites anteriores, la versión 9.6 es compatible con el servidor 16.04, tal cual se observa en la Figura 14.

Para la instalación de postgresql 9.6 se debe efectuar el siguiente comando: sudo apt-get install postgresql postgresql-contrib.

5.3.4. Migración de la Estructura de la base de datos Siringuero

Una vez instalado y configurado el Sistema Gestor de Base de Datos Postgresql 9.6, se ha realizado la migración de la estructura y los datos, para efectuar dicho proceso se ha establecido un corte de sistema en la fecha 22 de septiembre a horas 19:00, a partir de este Backups **bd_siringuero_20160922_1900.tar.bz2**, se ha realizado la instalación a la nueva versión del Gestor postgresql tal cual se observa en la Figura 15.

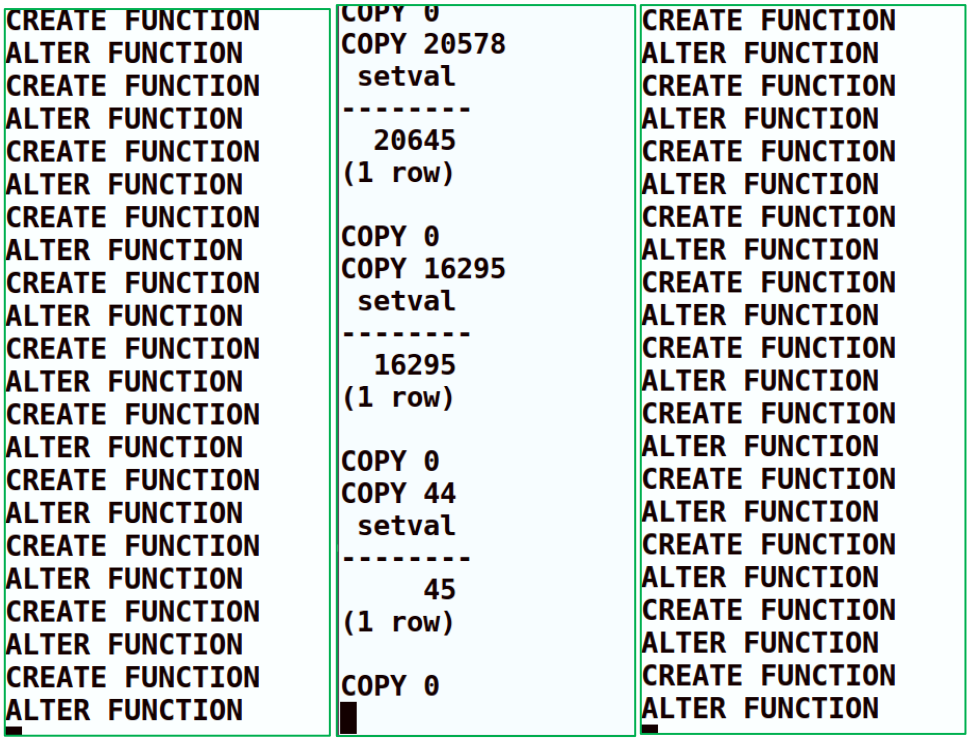


FIGURA 15: *Instalación de Base de Datos*
Fuente: Elaboración Propia

La Figura 15 muestra la instalación de la Base de Datos establecida del Backups que se ha realizado del Gestor de Base de datos 8.1 a la nueva versión del gestor postgresql 9.6, está instalación de base de datos refiere a tal cual se encontraba los datos y la estructura sin previa modificación alguna, la cual a partir de esta instalación se ha realizado lo que respecta la ejecución de prueba y error, hasta establecer la funcionalidad optima del Sistema Gestor de Base de Datos. A partir de la fecha 07 de noviembre del 2016 se ha migrado a la versión 9.6 que fue lanzado el 29 de septiembre del 2016, posterior a la versión 9.5.4, esto dando cumplimiento al instructivo que propone como modelo el presente proyecto de grado, tal cual se observa en anexo.

5.3.5. Migración de Funciones, Triggers y Dominios

Una vez instalada la Base de Datos a la nueva versión del Sistema Gestor de Base de Datos, se ha ejecutado por primera vez el Sistema Siringuero conectado con la nueva versión del motor de Base de Datos, la cual se han producido infinidad de errores, que a priori se mostraban falencias de incompatibilidad en la estructura de las funciones tal cual se muestra en la Figura 15.

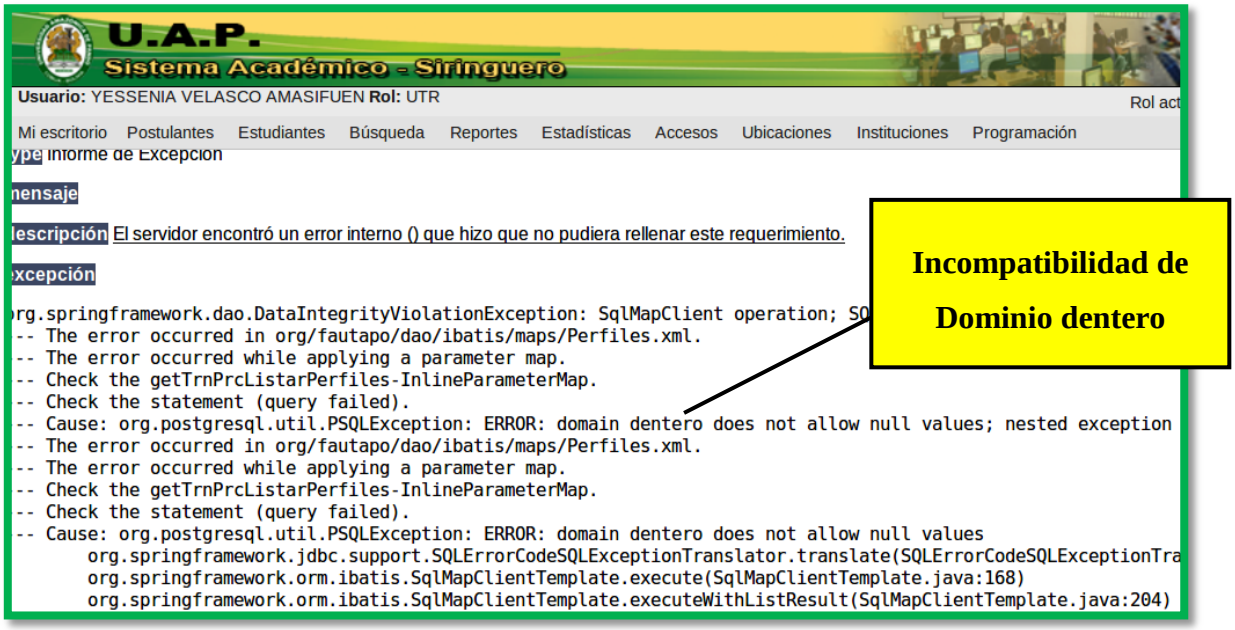


FIGURA 16: *Error de Incompatibilidad en la web Dominio dentero*
Fuente: Elaboración Propia

En la Figura 16 describe uno de los tantos errores de incompatibilidad de códigos y los tipos de datos y dominio establecidos en la base de datos, tal cual se observa la incompatibilidad del dominio dentero, este dominio está establecido para no aceptar valores nulos en cuanto se establece alguna transacción en las tablas, records o variables que se definan de acuerdo a este dominio, evidentemente la nueva versión obliga el tratamiento especial en el manejo de este tipo de dominio, al momento del desarrollo de la infraestructura de funciones tanto sus despliegues que conectan con los XML de Spring Frame Work .

El error que se observa en la Figura 16 Es un ejemplo de errores que presentan las funciones migradas de postgresql versión 8.1, para corregir este error se ha trabajado en base al método de prueba y error, en tal sentido se ha realizado el mantenimiento de las funciones que presentan este tipo de errores, actualizando el dominio pertinente que debiera utilizarse en las estructuras de sentencias Sql, tanto en los parámetros de entradas y los despliegues de las funciones respectivamente.

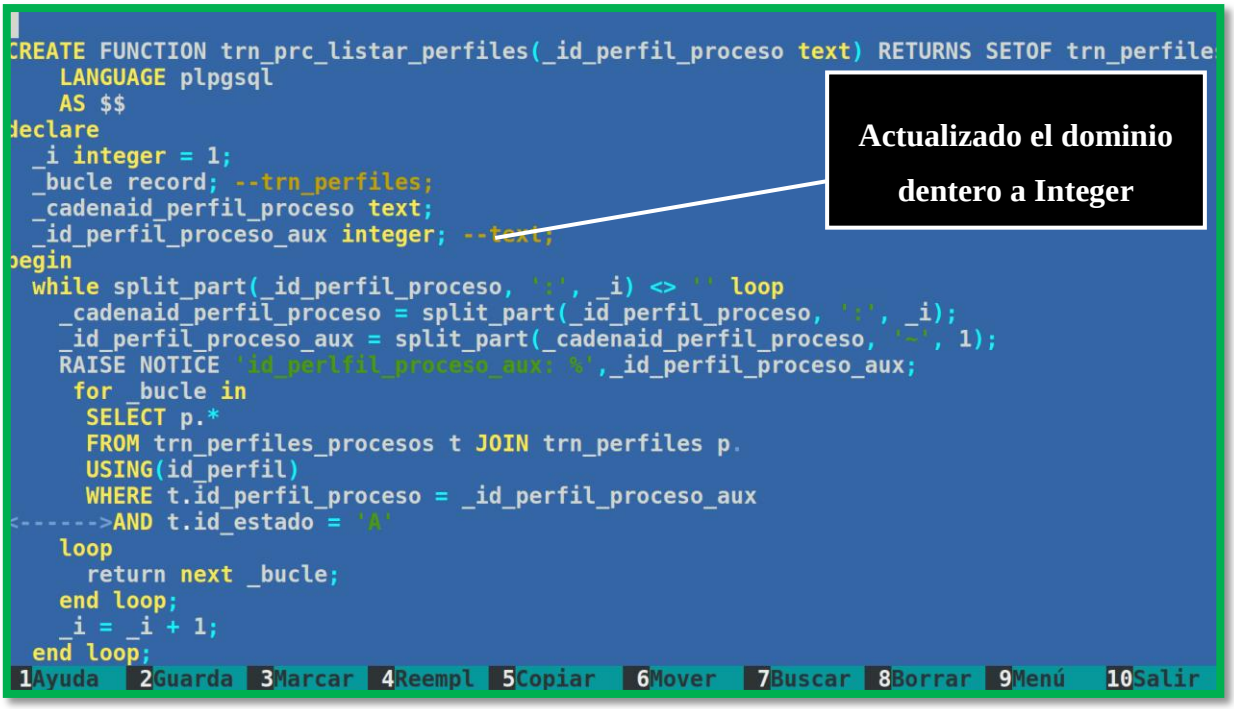


FIGURA 17: *Error de Incompatibilidad en la Función*
Fuente: Elaboración Propia

La Figura 17 Describe la función que fue modificada a partir del error que desplego Sprint Frame Work, tal como se observa en la figura 16, la modificación se ha realizado anulando la declaración de la variable _bucle la cual se declaraba de tipo trn_perfiles, esta forma de declaración de variable admite que _bucle trabaje como una tabla en pleno, tomando en cuenta todos los campos de la estructura de dicha tabla.

La versión 9.6 de PostgreSql restringe de manera estricta el uso de una variable como tabla en pleno ya que en esta tabla existen campos que no admiten valores nulos tales como llaves primarias, secundarias y otros campos definidos como not null.

La descripción de la problemática anterior se ha resuelto declarando la variable _bucle de tipo record, está declaración es aceptada por la versión postgresql 9.6 y las posteriores, las variables de este tipo pasan de ser de una estructura específica definida, a una estructura de uso general, la cual se convierte de la rigidez a la flexibilidad en el almacenamiento y la extracción de datos.

```
postgres@www:/home/func$ psql siringuero<ficha_academica.sql
CREATE FUNCTION
ERROR:  wrong record type supplied in RETURN NEXT
DETAIL:  Returned type dentero2 does not match expected type integer in column 9.
CONTEXT:  PL/pgSQL function mi_est_listar_ficha_academica(integer) line 35 at RETURN NEXT
postgres@www:/home/func$
```

FIGURA 18: *Error de Incompatibilidad en la Base de Datos*
Fuente: Elaboración Propia

Lo descrito anteriormente es una de las tantas correcciones que se ha realizado al momento de migrar las funciones implementadas en la versión postgresql 8.1 a 9.6, en algunas funciones fue necesario modificar los despliegues tal como se observa en la Figura 18, actualizando los campos por dominios adecuados la cual conllevo a modificar la conexión de Spring con el motor de base de datos mediante los XML.

5.3.6. Mantenimiento de Índices Primarios y Secundarios

Uno de los componentes de seguridad de la base de datos es la integridad de los datos, la estructura de las tablas y la infraestructura global de la base de datos, para ello fue necesario realizar el mantenimiento de los índice primarios y secundarios de las tablas, a lo largo de la producción del Sistema Gestor de la Base de Datos del Sistema Siringuero se han realizado distintos cambios y/o modificaciones en la infraestructura del Sistema, a partir de las nuevas normas y políticas que ha adoptado la Universidad Amazónica de Pando, el Sistema Siringuero se ha ido adaptando a estos cambios a partir de la gestión 2007 hasta la fecha.

Durante el proceso de mantenimiento del sistema Siringuero se ha afectado muchas tablas de la Base de Datos, adicionando campos secundarios a partir de las nuevas tablas que se han ido incorporado a la base de datos , estos últimos cambios a partir del funcionamiento de la base de datos no ha cumplido con la normativa de la integridad referencial, dejando aislado de la relación física las tablas y los campos secundarios, en la Figura 18 se observa una de las tantas correcciones que se ha realizado con relación a la integridad referencial de los índice primarios y secundarios, específicamente se describe en dicha figura la actualización del campo id estudiante, en la tabla transacciones que corresponde a la llave primaria de la tabla estudiantes

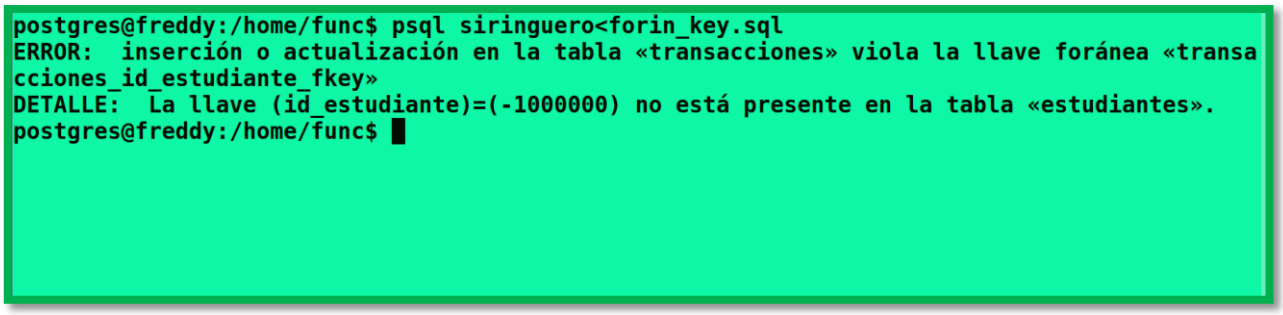


FIGURA 19: *Error de referencia (transacción-estudiantes) de llave foránea*
Fuente: Elaboración Propia

La Figura 19 se observa la ruptura evidente de la referencia de la tabla transacciones con estudiantes ya que la referencia relacional debiera haberse establecido al momento de realizar la modificación de la estructura de la tabla transacciones, sin embargo en su lugar se ha utilizado un dominio que por defecto establece el registro con el valor -1000000.

Al momento de realizar la actualización de la integridad referencial ha desplegado el error tal cual se observa en dicha imagen.

Para realizar la integridad referencial, primero se ha corregido el error tal cual se menciona en la parte de arriba, estableciendo la relación lógica para obtener datos que permita la relación entre ambas tablas tal cual se observa en la Figura 19.

```
CREATE OR REPLACE FUNCTION _actualizar_fkey() RETURNS integer
    LANGUAGE plpgsql
    AS $$
declare
_bucle record;

begin
  for _bucle in
<------>SELECT DISTINCT  e.id_estudiante,t.id_persona
<------>from transacciones t JOIN estudiantes e USING(id_persona)
<------>where t.id_estudiante < 0.
       ORDER BY id_persona
  LOOP
        update transacciones.
        set id_estudiante = _bucle.id_estudiante
        WHERE id_persona = _bucle.id_persona;
  END LOOP;
........
  return 1;
 end;
 1Ayuda  2Guarda  3Marcar  4Reempl  5Copiar  6Mover  7Buscar  8Borrar  9Menú  10Salir
```

FIGURA 20: *Función que corrige el error de la Figura 18*
Fuente: Elaboración Propia

En la Figura 20 se puede observar la función que lleva el nombre (_actualizar_fkey), esta función corrige la ruptura referencial de la llave foránea de la tabla transacciones. Una vez corregido el error se ha establecido la incorporación de la integridad referencial en la tabla transacciones la llave foránea id estudiante de la tabla estudiantes, código que se observa en la Figura 20

```
ALTER TABLE  transacciones
ADD CONSTRAINT transacciones_id_perfil_fkey FOREIGN KEY (id_perfil).
REFERENCES trn_perfiles(id_perfil);
ALTER TABLE  transacciones
ADD CONSTRAINT transacciones_id_programa_fkey FOREIGN KEY (id_programa).
REFERENCES fcl_programas(id_programa);

UPDATE transacciones set id_estudiante=0 where id_estudiante < 0;
ALTER TABLE  transacciones
ADD CONSTRAINT transacciones_id_estudiante_fkey FOREIGN KEY (id_estudiante).
REFERENCES estudiantes(id_estudiante);
```

FIGURA 21: *Código llave foránea id estudiante*
Fuente: Elaboración Propia

De esta manera la descripción realizada anteriormente es una de las tantas incorporaciones de integridad referencial que se ha corregido, en marcos del mantenimiento de índice primarios y secundarios del gestor de base de datos Siringuero.

5.3.7. Estadística del resultado de la migración del SGBD-Siringuero

La tabla 11 muestra los resultados de la migración del Gestor de Base de Datos Postgresql 8.1 a la versión 9.6, esta tabla muestra el estado en el que se encontraba en la anterior versión versus el estado actual, una vez migrada y realizada las actualizaciones y correcciones correspondientes para la adecuada producción del gestor de base de datos siringuero.

Nro.	Estructuras del SGBD	Migradas Postgres 8.1	Actual Postgres 9.6
1.	Total Tablas	350	355
2	Tablas Actualizadas/Nuevas	0	5
3.	Datos Migrados	6234724	6234724
4.	Funciones Migradas	1809	1859
5.	Secuencias	250	355
6.	Funciones Errores/Mejoradas	198	198
7	Trigger Migrados	38	38

TABLA 11: Estadísticas de Resultado de la Migración del SGBD-Siringuero
Fuente: Elaboración Propia

Como se podrá observar en dicha tabla los errores más frecuentes al momento de realizar la migración y establecer pruebas y errores, fueron las estructuras de las funciones implementadas en la versión anterior, en tal sentido se han tenido que realizar correcciones, estableciendo la compatibilidad para la nueva versión. En cuanto a los despliegues que se han corregido para la conectividad con los XML de Spring Frame Work, ha implicado también la modificación de la estructura de los XML del Sistema Siringuero.

5.4. DETALLE DE LA INFRAESTRUCTURA DEL GESTOR DE LA BASE DE DATOS SIRINGUERO

Durante el proceso de la migración del gestor de base de datos postgresql 8.1 a postgresql 9.6 se han identificado y clasificado las tablas de acuerdo a los privilegio de acceso y almacenamiento ,

las cuales sean primarias y/o resultantes, a continuación se describen cada una de las clasificaciones correspondientes.

5.4.1. Tablas Primarias SGBD-Siringuero

Se han identificado las tablas como primarias a todas aquellas que el almacenamiento de datos es independiente, el almacenamiento a estas tablas absolutamente es a partir de la aplicación Frame Work, la cual la vista de ésta es ejecutada por el usuario del Sistema Siringuero. Es decir que el almacenamiento de datos no depende de manera directa o indirecta en el comportamiento del Gestor de Base de Datos del Sistema Siringuero. Esta descripción se observa en el Anexo A

Nro.	Clasificación de la Tablas	Cantidad
1.	Tablas Primarias	118
2.	Tablas Secundarias	232

TABLA 12: *Clasificación de las Tablas.*
Fuente: Elaboración Propia

La tabla 12 describe de manera resumida la clasificación de las tablas primarias y secundarias, tomando en cuenta la cantidad de estas, para mayor detalle la descripción completa se observara en los Anexo A y Anexo B.

5.4.2. Tablas Secundarias SGBD-Siringuero

Se refiere a las tablas secundarias a todas aquellas cuyo almacenamiento es total o parcialmente dependiente de las tablas primarias, y otros componentes internos que son activados en cuanto detecten la inserción y/o actualización en ellas, es decir que estas tablas están compuestas principalmente por llaves foráneas y/o índices secundarios, las cual obliga a que las tablas primarias contengan datos para después realizar la inserción a estas. En cuanto a las salidas de datos el comportamiento es similar, tomando en cuenta que los desarrolladores deben buscar la unión entre las tablas secundarias a primarias. Para mayor detalle ver Anexo B.

5.4.3. Tablas por Privilegios de Accesos

La infraestructura del gestor de base de datos Siringuero se ha clasificado además por privilegios de accesos y a estás se le han otorgado los niveles de prioridad, para lo cual dentro de la Unidad de Sistemas Académicos, se ha creado un Instructivo en la cual se define los niveles de prioridad para determinar la clasificación de las tablas. En la tabla 13 se observa los niveles de prioridad de acuerdo al grado y la importancia de las mismas.

Nro.	Privilegios de Accesos	Nivel
1.	Administrador de Bases de Datos (DBA)	**1**
2.	Súper Usuario	**2**
3.	Usuario	**3**

TABLA 13: *Privilegio de Accesos*
Fuente: Elaboración Propia

La tabla 14 describe los niveles de prioridad de acceso al Sistema Gestor de Base de Datos, para lo cual se ha determinado la jerarquía de la infraestructura, a los cuales los usuarios podrán tener acceso a las tablas en tanto se realizan las actualizaciones, eliminaciones y otras acciones

Nro.	Tablas por Privilegios de Acceso	Nivel de Acceso
1.	Notas	1
2.	Est_libretas	1
3.	Est_libretas_cerradas	1
4.	Transacciones	1
5.	Trn_detalles	1
6	Matriculas	1
7	Est_progrmaciones	1
8.	Usuarios	1

TABLA 14: *Tablas por Privilegios de Accesos (DBA)*
Fuente: Elaboración Propia

La tabla 14 muestra la lista de las tablas que han sido asignadas como primer nivel de prioridad de acceso, y por la importancia de datos que son almacenados en ella, por lo tanto, el administrador de base de datos podrá acceder a ella con todos los privilegios que fue asignado en tanto se realicen las actualizaciones, modificaciones, eliminaciones, y otras acciones que ameriten realizar en el Gestor de Base de datos del Sistema Siringuero.

Nro.	Tablas por Privilegios de Acceso	Nivel de Acceso
1.	Estudiantes	2
2.	Docentes	2
3.	Convalidaciones	2
4.	Dct_asignaciones	2
5.	Mtr_planes	2
6	Grp_evaluaciones	2
7	Prg_detalles	2
8.	Dpto_grupos	2
9.	Tr_tramites	2
10.	Tr_datos	2
11	Roles	2
12	Usr_roles	2
13	Pst_cpo_cupos	2
14	Postulantes	2
15	Lbr_control_impresion	2
16	Prg_controles_academicos	2
17	Lbr_fases	2
18	Lbr_tipos_notas	2
19	Prg_planes	2
20	Trn_perfiles_conceptos	2

TABLA 15: *Tablas por Privilegios de Accesos Súper Usuario*
Fuente: Elaboración Propia

La tabla 15 muestra la clasificación de tablas de acuerdo al segundo privilegio de acceso, que está determinado como Súper Usuario, se ha determinado esta clasificación de acuerdo al grado y la importancia de almacenamiento de datos, sin embargo, el administrador de base de datos podrá acceder con todos los privilegios y designar el rol correspondiente algún usuario que desempeñe funciones en la Unidad de Sistemas Académicos.

La asignación de estas tablas al segundo privilegio de accesos, es porque la modificación y/o actualización de la estructura y datos ya sea permisible o no, no afecten al desarrollo y la producción de manera parcial o total y el funcionamiento global del Sistema Gestor de la Base de Datos hacia el Sistema Siringuero. Esto quiere decir que si en algún momento fuese vulnerada estás tablas o fuesen realizadas algunas modificaciones, no implica la pérdida total o parcial del servicio del sistema hacia los clientes.

CUADRO COMPARATIVO

Nro.	Características Comparativas	Antes de la Implementación del Proyecto	Después de la Implementación del Proyecto
1.	Motor de Postgresql	Postgresql Versión 8.1	Postgresql 9.6 última versión
2	Sistema Operativo	Servidor Ubuntu 12.04	Servidor Ubuntu 16.04
3	Firewall	Ninguna configuración	Configuración del firewall Ubuntu Server UFW
4	Configuración del usuario postgresql	Usuario postgres	Configuración del súper usuario DBA
5.	Configuración de Conectividad	Localhost	Servidor remoto de postgresql y servidor de aplicaciones del Sistemas Siringuero
6.	Actualización de la estructura de funciones	Ningún tipo de mantenimiento	Mantenimiento de 198 funciones tanto en la estructura como en los despliegues.
7.	Plataforma de comparación	JDK 1.5	JDK 1.6
8.	Secuencias	345	355
9.	Copias de Seguridad en el Gestor de Base de Datos	Las copias de seguridad se las realizaba de manera Manual	Actualmente las copias de Seguridad se realizan de manera Automática, 2 veces por día.
10.	Implementación de Medidas de Seguridad	Configuración de roles y usuarios por defecto	Configuración de usuarios y roles de acuerdo a privilegios.

TABLA 16: *Cuadro Comparativo SGBD 8.1 a 9.6*
Fuente: Elaboración Propia

5.5. IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

En relación a implementación de medidas de seguridad en el Gestor de la Base de Datos Siringuero se han realizado las configuraciones de seguridad en el motor de postgresql 9.6 esta configuración se ha realizado al momento de implementar el presente proyecto de grado, las configuraciones que se van a detallar a continuación corresponden a los servidores de Base de Datos y aplicaciones Sprint Frame Work, al final se describirá la configuración del firewall que fue incorporado con la implementación del último Sistema Operativo Servidor Ubuntu 16.04.

5.5.1. Asignación de Contraseña al Súper Usuario Postgres

En la Figura 22 se observa los comandos que se han ejecutado para asignar contraseñas al súper usuario del motor de postgresql 9.6 la cual es establecida por el sistema operativo servidor, como usuario por defecto de postgresql, en tal sentido para realizar las configuraciones respectivas se ha tenido que ejecutar el siguiente comando:

- ✓ psql –c "ALTER USER postgres WITH ENCRYPTED PASSWORD ´bd´";

FIGURA 22: *Asignación de Contraseña al súper usuario postgres*
Fuente: Elaboración Propia

5.5.2. Creación de Usuarios y Roles

Una vez asignada la contraseña al súper usuario postgres, accedemos con todos los permisos y privilegios al motor de bases de datos postgres.

En la Figura 23 se observa los comandos correspondientes para la creación, asignación y establecimientos de privilegios correspondientes a un usuario en particular como súper usuario.

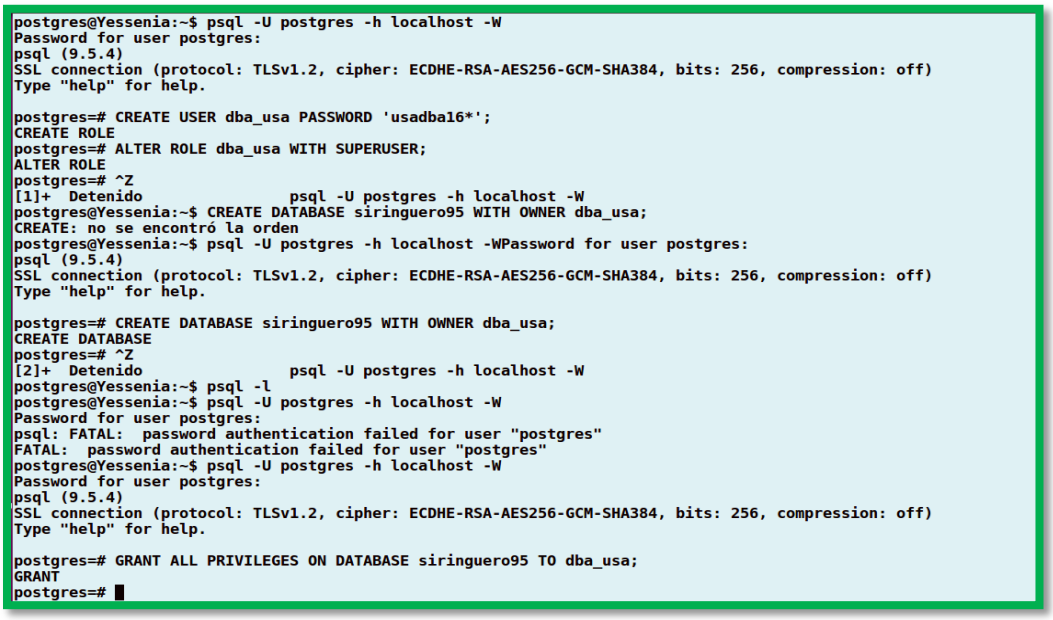


FIGURA 23: *Creación de Usuario y Rol dba_usa*
Fuente: Elaboración Propia

En la Figura 23 se puede observar los comandos que permiten realizar las siguientes acciones

a) Para acceder al motor de postgresql se debe ejecutar el comando psql –U postgres –h localhost –W.
b) Creación de usuario dba_usa la cual se realiza con el comando créate user y password
c) Asignación de rol de super usuario al usuario dba_usa ,la cual establece todos los privilegios que necesita para creación y actualización de la infraestructura de una base de datos, con el comando grant all privileges
d) Creación de una base de datos con el comando create database con la opción y los privilegios de súper usuario dba_usa.

5.5.3. Configuración de Accesos al SGBD postgresql 9.6

Una vez creado el rol dba_usa como súper usuario se debe establecer la configuración de acceso en el servidor del Sistema Gestor de Base de Datos, dando permisos y privilegios de acceso al servidor de aplicaciones, la cual establecerá la conexión con el servidor de base de datos tal cual se observa en la Figura 24, la configuración se observa para el host IPv4 el establecimiento especifico de la base de datos, el usuario que se ha creado en la parte superior de este acápite,

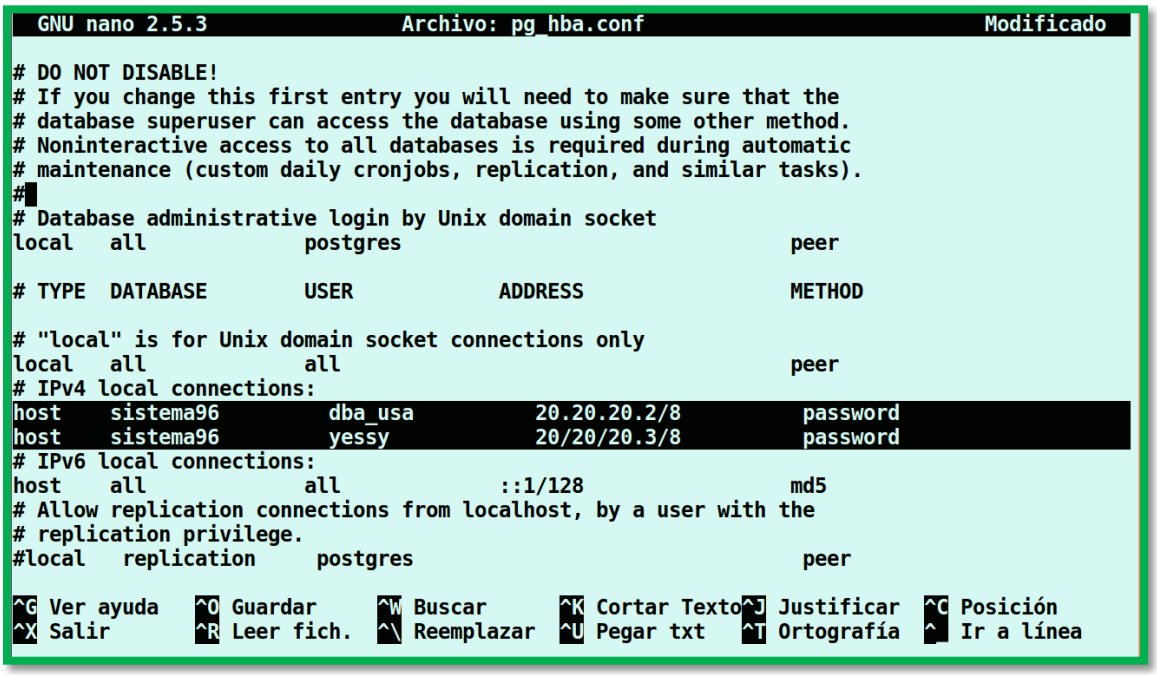


FIGURA 24: Configuración *de Accesos*
Fuente: Elaboración Propia

El ip con el que el servidor de aplicaciones podrá acceder es el 20.20.20.2, esta configuración cierra todos los posibles accesos hacia el servidor de base de datos, dejando sin rangos y otras posibilidades de acceso externas ya sean de equipos que estén conectados en la red local y/o equipos que acceden desde redes externas, en la parte inferior de esta configuración se observa un acceso similar que está autorizado al equipo del administrador de base de datos , la cual está en el mismo rango de red, como se podrá observar en la

Figura 25 la configuración de acceso está realizada para que puedan acceder dos equipos con usuarios diferentes a la misma base de datos(Siringuero95), dotando de una máxima seguridad, estás portaran claves cifradas por el método password, la cual es uno de los métodos que postgresql 9.6 incorpora en la configuración de sus usuarios y claves.

La configuración realizada tal cual se observa en la Figura 24 es una de las medidas de seguridad que establece el presente proyecto de grado, como un aporte fundamental para la adecuada producción del Sistema Gestor de Base de Datos, la cual cumpla con los requisitos de fiabilidad y confiabilidad.

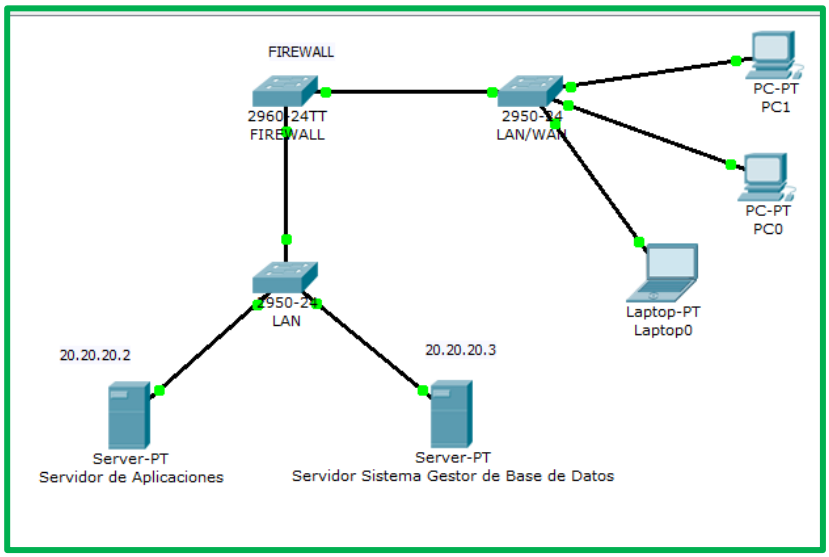


FIGURA 25: *Conexión de Acceso del Sistema Gestor de Base de Datos y Sistema de Aplicación*
Fuente: Elaboración Propia

La figura 25 describe la configuración de accesos de los servidores 20.20.20.2 (Servidor de Aplicaciones) y el 20.20.20.3 (Servidor Sistema Gestor de Base de Datos), los cuales prestarán servicios de manera independiente en equipos diferentes que están ubicados físicamente en distintos lugares, esta forma de configuración permite la plataforma de Spring Frame Work, dejando exento de las vulnerabilidades al servidor del Sistema Gestor de Base de Datos, esta medida de seguridad responde a la solución de los riesgos analizados al principio del presente capítulo, ya que el servidor de base de datos y aplicaciones se encontraban en el mismo equipo servidor. La producción del Sistema Siringuero con esta modalidad de fusión presentaba grandes riesgos de ser vulnerados, pérdida de datos y otros

daños que anteriormente ya se habrían suscitado, sin embargo a partir del 23 de septiembre del 2016 el Sistema Siringuero presta servicios con la configuración tal cual se ha explicado en la parte superior del presente acápite.

5.5.4. Configuración de Conexiones al Sistema Gestor de Base de Datos

Para las conectividades al gestor de base de datos, tanto como el servidor de aplicaciones, el administrador de base de datos deberá realizarla por el puerto 5000, esta configuración se ha realizado en el Sistema Gestor de Base de Datos Siringuero, tal cual se ha propuesto como objetivo del presente proyecto de grado, la configuración por defecto que propone postgresql es el puerto 5432, ya que al ser por defecto es vulnerable para accesos no autorizados.

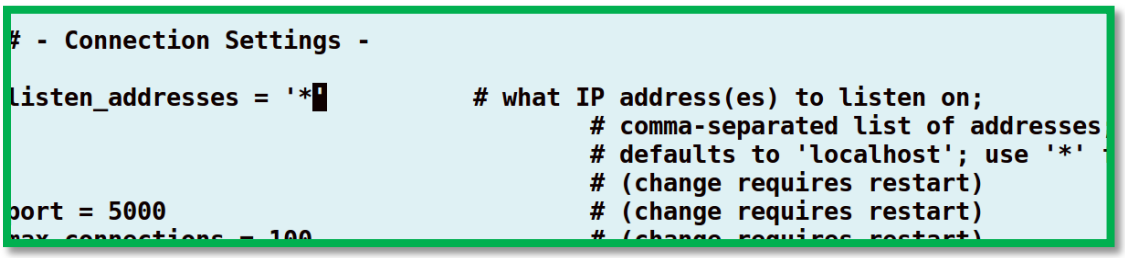


FIGURA 26: *Configuración de Conectividad y Puertos de Postgres*
Fuente: Elaboración Propia

En la Figura 27 se observa la conectividad de Sprint Frame Work (Servidor de aplicaciones) con el Servidor de Sistema Gestor de Base de Datos Siringuero, esta configuración explica la desconcentración de servidores tal cual se ha explicado en el acápite anterior y como se observa en la Figura 25.

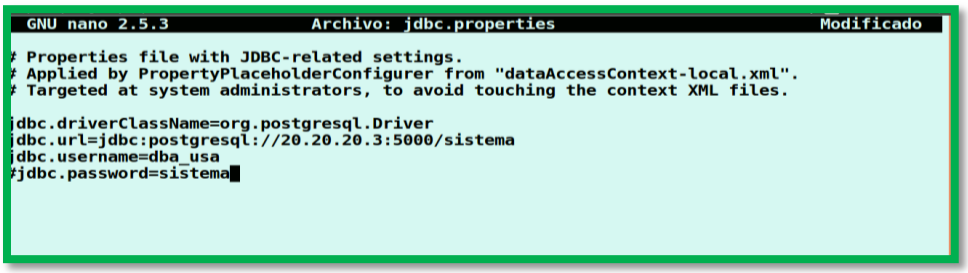


FIGURA 27: *Configuración de Conexiones Aplicación vs Base de Datos.*
Fuente: Elaboración Propia

5.5.5. Configuración de Firewall UFW

Una de las medidas de seguridad que ha sido parte de la implantación del Sistema de seguridad del presente proyecto de grado, como resultado se ha obtenido la configuración de un firewall que incorpora el sistema operativo Ubuntu Server 16.04, el cual refiere a UFW que viene incorporado al momento de realizar la instalación .

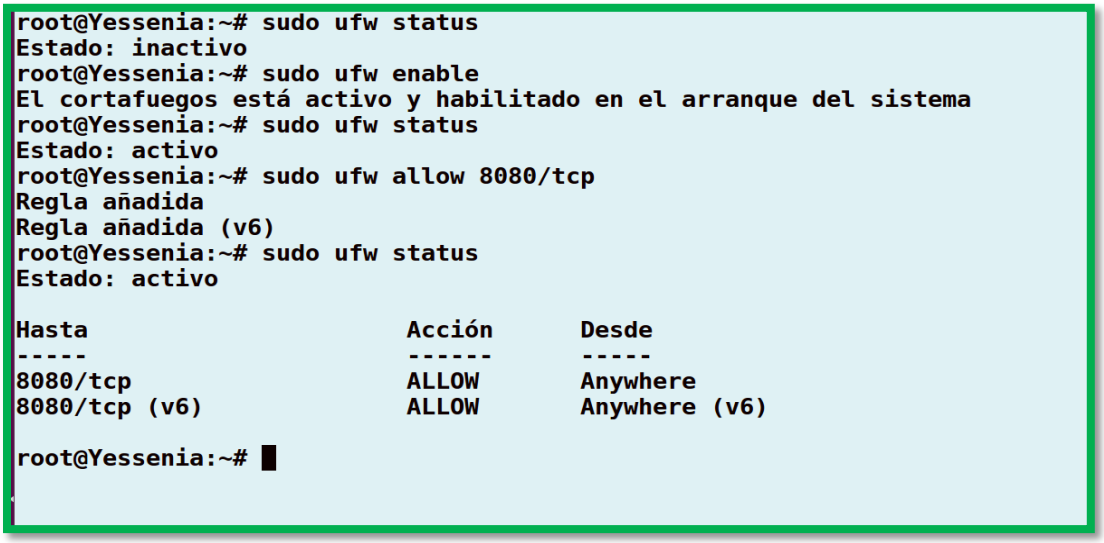


FIGURA 28: *Configuración del Firewall UFW*
Fuente: Elaboración Propia

En la Figura 28 se observa la configuración de las políticas de seguridad, realizadas a nivel de sistema operativo, una de las políticas de seguridad es dejar abierto solamente el puerto 8080/tcp tal cual el servidor de aplicaciones Sprint Frame Work con su servidor toncam utilizan este puerto para prestar servicio durante la producción del Sistema Siringuero.

Otra de las políticas de seguridad es denegar todos los accesos cerrando los puertos, los cuales no podrán ser visibles tanto a nivel del sistema operativo y en el entorno de la red de datos.

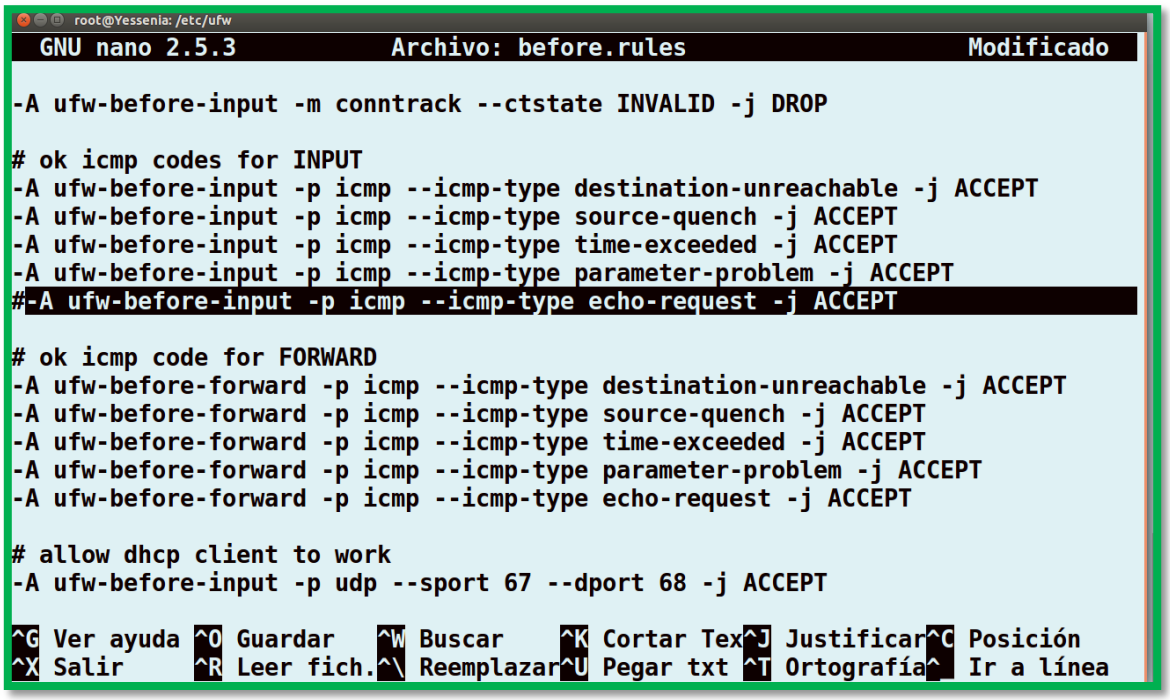


FIGURA 29: Configuración *denegación de Ping*
Fuente: Elaboración Propia

El firewall UFW permite realizar una configuración de tal modo que el equipo servidor en el cual es implementado y configurado esté firewall, hace transparente a todos aquellos cuya petición se realice ICMP, escaneos y sondeos que generalmente realizan los intrusos, hacker o personas dedicadas a vulnerar, ya que utilizan diferentes herramientas (nmap) para realizar tales acciones.

Es decir que literalmente no será visible ni será escuchado por ningún equipo externo conectado a la red tanto local y/o externa, esto libera de las vulnerabilidades y riesgos que puedan presentar en el transcurso del servicio y la producción tanto del sistema de aplicaciones como del Sistema Gestor de Base de Datos Siringuero.

5.6. PRUEBAS DE LA IMPLEMENTACION DEL SISTEMA DE SEGURIDAD EN EL GESTOR DE LA BASE DE DATOS SIRINGUERO

Una vez implementado el Sistema de Seguridad en el gestor de Base de Datos Siringuero se ha realizado las pruebas correspondientes, para la efectividad de la configuración en el nivel de Gestor de Base de Datos y en el nivel de Sistema Operativo.

5.6.1. Pruebas de Seguridad a Nivel del Gestor de Base de Datos

Para esta prueba se ha utilizado la herramienta de consola de Ubuntu, la cual se realiza la conectividad y el acceso al Servidor del gestor de Base de Datos con el comando psql –U siringuero_bd –h 10.10.10.3 -b siringuero –p 5000, una vez ejecutado el comando, si la conectividad fuese exitosa el servidor responde con una petición de contraseña cifrada, esto indica que la configuración de Seguridad en el Gestor de Base de Datos fue exitoso, ya que al tener una respuesta de administración de contraseña, el servidor restringe todo tipo de acceso, permitiendo solo así al usuario y por el método autorizado tal cual se observa en la Figura 30.

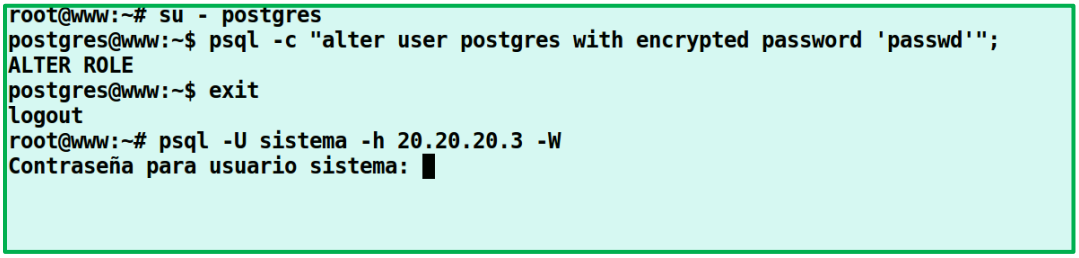


FIGURA 30: *Prueba de Seguridad en el Gestor de Base de Datos*
Fuente: Elaboración Propia

El usuario solicitante debe administrar correctamente el ip solicitado, usuario, base de datos asignado y por el puerto autorizado, caso contrario el servidor del gestor de base de datos reportara mensaje de error de conectividad, rehusando así la autenticación de dicho usuario.

5.6.2. Prueba de Seguridad a Nivel del Sistema Operativo

Se ha instalado y configurado un Firewall a nivel del Sistema Operativo, la cual se ha agregado las políticas tanto en el Servidor de Aplicaciones como en el Servidor de Base de Datos, para realizar la prueba de configuración de las políticas de seguridad se ha utilizado la herramienta Nmap, para lo cual se ha utilizado el comando de escaneo de puertos, nmap 10.10.10.3, este comando devuelve un reporte de los puestos abiertos del host escaneado y el servicio que se ejecuta en dicho puerto, tal cual se observa en la figura 31.

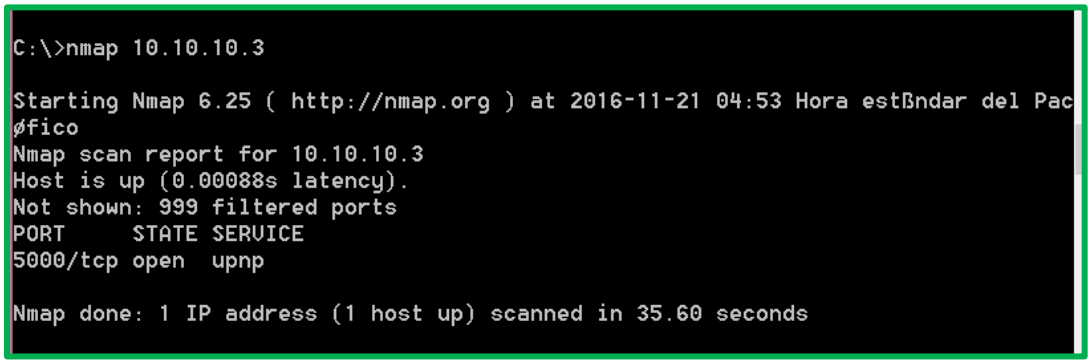


FIGURA 31: *Prueba Antes de Implementar el Firewall a Nivel de Sistema Operativo*
Fuente: Elaboración Propia

El reporte de escaneo que se muestra en la figura 31, fue realizado antes de la configuración de transparencia del servidor la cual deja al descubierto todos los sondeos y escaneos de puerto. La figura 32 muestra la respuesta realizada a la ejecución del comando nmap 10.10.10.3 después de haber realizado la configuración de transparencia del servidor, el cual se observa claramente que nmap no encuentra respuesta alguna a dicho escaneo.

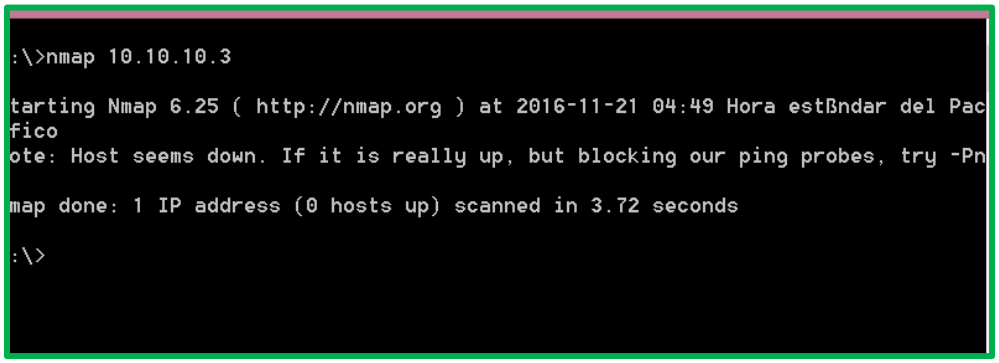


FIGURA 32 *Prueba Después de la Implementación del Firewall UFW*
Fuente: Elaboración Propia

Así mismo se ha utilizado la herramienta ping, para verificar la disponibilidad de host del Servidor Gestor de Base de Datos, con el comando ping 10.10.10.3, esta prueba se ha ejecutado después de haber realizado la configuración de la transparencia del servidor, tal cual se observa en la figura 33.

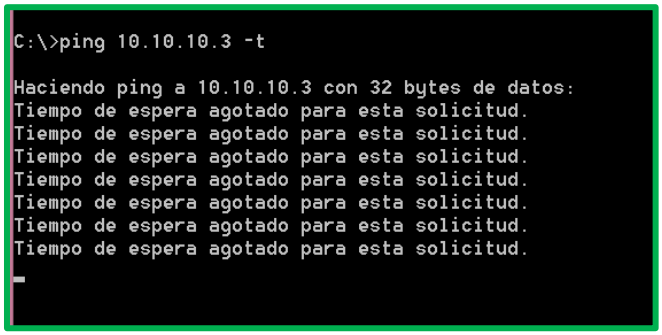


FIGURA 33: *Prueba de transparencia del Servidor*
Fuente: Elaboración Propia

5.7. DESCRIPCIÓN DE MODELO PROPUESTO POR EL PRESENTE PROYECTO DE GRADO

El presente proyecto de grado, propone un instructivo como modelo para la implementación de Sistemas de Seguridad en el Gestor de la Base de Datos del Sistema Siringuero.

El instructivo DIA-USA-INS-009 "Administración del Sistema de Seguridad en el Gestor de Base de Datos Siringuero", es parte del procedimiento DIA-USA-PRO-001 Administración del Sistema Siringuero, el objetivo del instructivo es establecer claramente los pasos para la administración del Sistema de Seguridad a nivel del Gestor de Base de Datos.

En el marco de desarrollo el instructivo presenta los pasos establecido para el análisis de riesgo, mantenimiento y migración del gestor de Base de Datos Siringuero, así mismo establece los pasos adecuados para la implementación de medidas de seguridad a nivel del Gestor de Base de Datos, de la misma manera la instalación y configuración de Firewall a nivel de Sistema Operativo.

El instructivo, al ser parte de un procedimiento implementado en la Unidad de Sistemas Académicos, el responsable de la unidad o el administrador de Sistemas, tienen la obligación de hacer cumplir dicho instructivo, de manera periódica.

Este Instructivo cuenta con el formulario DIA-USA-FOR-019 "Registro de la Implementación de Sistema de Seguridad en SGBD. Siringuero", la cual permite

documentar las actividades que se deben realizar durante el proceso de la administración del Sistema de Seguridad en el Gestor de Base de Datos Siringuero.

El instructivo y el formulario se encuentra de manera detallada en los anexos del presente proyecto de grado.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSONES

A partir de la implementación del Sistema de Seguridad como Modelo en el Gestor de la Base de Datos Siringuero, se ha obtenido varios resultados de acuerdo a los objetivos específicos y se ha alcanzado el objetivo general que se ha planteado en el presente proyecto de grado, en tal sentido se ha llegado a las siguientes conclusiones:

- Se ha desarrollado la matriz de análisis de riesgo para identificar factores de riesgo , amenazas y vulnerabilidades desde la óptica de sucesos físicos y sucesos lógicos, lo cual ha permitido determinar el promedio de umbral de riesgo medio

- Se realizó el mantenimiento de la Base de Datos Siringuero, la cual se actualizó el gestor de Base de datos postgresql 8.1 incorporando la versión actual postgresql 9.6 ya que esta versión incluye correcciones de vulnerabilidades.

- Una vez actualizado el gestor de base de datos a la versión más reciente se realizó la migración de datos, funciones, dominios, índice, secuencias y trigger desde postgresql 8.1 a postgresql 9.5.4, el cual entró en funcionamiento a partir del 23 de septiembre del 2016, luego de migrar a la versión 9.5.4 apareció una nueva versión de postgresql la cual es la versión 9.6, de esta manera se realizó nuevamente la migración correspondiente, el resultado de la ejecución de esta actividad, cumple con el requisito de integridad, en la Base de Datos del Sistema Siringuero.

- Se creó usuarios y roles, diferente al usuario por defecto, está configuración es una de las medidas de seguridad propuestas, ya que al crear un usuario que no es por defecto, nos permite administrar y monitorear el acceso y conectividades con los métodos de cifrados que postgresql 9.5.4 y 9.6 ha incorporado.

- Se ha instalado y configurado un servidor de Gestor de Base de Datos postgresql 9.6 y de Aplicaciones Spring Frame Work, las cuales prestan servicio de manera independiente, vale decir el servidor de aplicaciones realiza acceso al servidor de base de datos, esta desconcentración de servicios resuelve los riesgos de pérdida, daños y vulnerabilidades,

dotando de esta manera de alta seguridad, fiabilidad y confiabilidad en el resguardo de los datos del Sistema Siringuero.

- Al haber logrado la migración de postgresql 8.1 a 9.6, aportan numerosas ventajas entre las que destacamos una mayor escalabilidad, la shared_buffer de PostgreSql puede almacenar hasta centenares de gigabytes sin ningún tipo de problema, escalabilidad lineal con el número de procesadores, al menos hasta 128 cores/máquina, mejoras notables en el uso de espacios entre tablas para maximizar la concurrencia, mejor implementación de MVCC, sin limitaciones en el tamaño y duración de transacciones.

- Se ha instalado y configurado la última versión del Sistema Operativo, Servidor Ubuntu 16.04 la cual fue lanzado el 28 de abril del 2016, esta actualización del sistema operativo corrige de manera automática las vulnerabilidades y se han incorporado actualizaciones de seguridad, dotando de esta manera la fiabilidad en los servicios que presta actualmente la Unidad de Sistemas Académicas de la Universidad Amazónica de Pando.

- Se ha instalado y configurado un Firewall a nivel del Sistema Operativo, en la cual se ha implementado políticas de seguridad, denegando accesos a todos los puertos con excepción el puerto 8080 TCP que utiliza Tomcat, para el servicio de aplicaciones Sprint Frame Work, y el puerto 5000 para servicio de PostgreSql, de la misma manera se ha configurado el firewall, de tal modo que esta convierte de manera transparente al servidor, dejando exento de escaneos, sondeos y escucha desde la red local y extensas que principalmente utilizan los agentes dedicados a vulnerar servidores.

6.2. RECOMENDACIONES

Una vez concluido el presente proyecto de grado se recomienda lo siguiente:

❖ Mantener los servidores de aplicación y de Gestor de Base de Datos bien protegidos, en una sala de acceso restringido en donde el administrador/a solo pueda acceder mediante acceso remoto.

❖ Se recomienda realizar la migración de base de datos , en cuánto postgres lance de manera estable la versión más reciente y que está pueda ser utilizada para prestación de servicios de base de datos con gran envergadura

❖ Realizar el mantenimiento de manera constante los índices primarios y secundarios, ejecutando métodos que optimicen el funcionamiento adecuado del Gestor de Base de Datos.

❖ Se recomienda al administrador de Base de Datos que en cuánto se realiza la configuración e instalación de postgresql, siga de manera efectiva los pasos adecuados que se han escrito en el instructivo DIA-USA-INS-009 Implementación de Medidas de Seguridad en el Gestor de Base de Datos.

❖ Se recomienda al administrador de base de datos realizar la instalación y configuración de un servidor de Backups de Base de Datos Siringuero, la cual el presente proyecto de grado ha dejado exento por falta de presupuesto que la universidad no ha podido adquirir dicho servidor.

❖ Se recomienda al administrador de base de datos pueda instalar y configurar servidores de réplica de gestor de base de datos, la cual postgresql 9.6 incorpora esta posibilidad de almacenamiento en tiempo real.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Ana Aguilera, Tineo Lioned , Jose Cadenas . (2009). *mplementación de Extensiones Difusas de manera Fuertemente Acoplada sobre el RDBMS PostgreSQL .*

Angel Castejon, Miguel Lirio ,Javier Umbe. (2010). *Sistema de Gestión de Bases de Datos.*

Cristosono, R. R. (2005). *Metodología de la Investigación Cientifica .* Lima,Peru.

Cruz, I. D. (2006). *Administracion de la Bases de Datos del Sistema SIGA-COIMATA.* Cobija,Pando.

Damian. (2009). *Seguridad en Bases de Datos .* Venezuela.

Escobar, J. (s.f.). *Integridad y Seguridad en los Gestores de Bases de Datos .*

Fabian, B. C. (2005). *Seguridad Informatica sus Implicancias e Implementación.*

Gerardo Villagomez, Harold Álvarez, Danny Vivanco. (2006). *Implementación de la Migracion de Bases de Datos del Sistemas CANOPUS de Informix 9.4c a Oracle.10 g.* Guayaquil, Ecuador.

Heredia, C. M. (2002). *La protección Juridica a las Bases de Datos .* Bogota.

Lescano, E. Z. (2003). *Seguridad en el Comercio Electronico .* Lima,Peru.

Marc Gibert Ginestà Oscar Pérez Mora. (2010). *Bases de Datos en Postgresql .*

Perez, A. C. (2008). *Seguridad en Bases de Datos en Informix en la Organización.* Mexico.

Pérez, M. (2013). *definicion de seguridad.*

Reyes, G. M. (2011). *Propuestas para impulsar la seguridad informática en materia de educación.* Mexico.

Roberto Hernández Zampieri, Carlos Férnandez Collado, Pilar Baptista . (2010). *Metodología de la Investigación.* México.

Sánchez, J. C. (2009). *Metodología de la Investigación Cientifica y Tecnológica.*

ANEXOS

ANEXO “A”

TABLAS PRIMARIAS

TABLAS PRIMARIAS

NRO	CLASES PRIMARIAS	CANTIDAD DE DATOS
1	Categorias	47
2	Dib_bases_datos	1
3	Dib_componentes	4
4	Dib_consultas	21
5	Eenlaces	709
6	Estados	28
7	Niveles_accesos	2
8	Parámetros	12
9	Tbl_tipos_avisos	2
10	Tbl_tipos_tableros	1
11	Areas_conocimientos	1
12	Bv_estadocs	4
13	Bv_grupos	7
14	Bv_idiomas	6
15	Bv_penalidades	6
16	Bv_roles	6
17	Bv_sancionados	114
18	Bv_tipos_adquisicion	3
19	Bv_tipos_documentos	12
20	Bv_tipos_ejemplares	2
21	Bv_tipos_prestamos	3
22	Cajas_salud	9
23	Cargos	617
24	Cv_rubros	4
25	Dct_tipos_documentos	10
26	Dias	7
27	Do_evaluadores	6
28	Do_formularios	6
29	Est_clasificacion_general	5
30	Eventos_grados_academicos	0
31	Grupos	12
32	Horas	13
33	Mensaje_navidad	16

34	Meses	12
35	Mo_hil_destinatarios	0
36	Mo_sgm_adjuntos	0
37	Mo_tipos_hilos	4
38	Mo_tipos_segmentos	6
39	Modalidad_becas	1
40	Modalidades_graduaciones	2
41	Mtr_modalidad_graduacion	1
42	mtr_tipos_materias	4
43	Multipartinbox	0
44	Paises	25
45	Pga_diagrams	0
46	Pga_forms	0
47	Pga_graphs	0
48	Pga_images	0
49	Pga_layout	23
50	Pga_queries	0
51	Pga_reports	0
52	Pga_scripts	0
53	Pln_tipos_materias	5
54	Prsespadjuntos_iconos	7
55	Prs_grados_academicos	17
56	Tipo_titulaciones_academicas	3
57	Tipos_admisiones_agrupados	4
58	Tipos_asignaciones	6
59	Tipos_aulas	4
60	Tipos_calificaciones	2
61	Tipos_cedulas	2
62	Tipos_centros_investigaciones	0
63	Tipos_clasificaciones	26
64	Tipos_compromisos	2
65	Tipos_controles_academicos	6
66	Tipos_convalidaciones	4
67	Tipos_cursos_temporadas	3
68	Tipos_deudas	2
69	Tipos_docentes	9
70	Tipos_documentos	28

71	Tipos_empresas_telefonicas	4
72	Tipos_estados_civiles	4
73	Tipos_estudiantes	2
74	Tipos_evaluaciones	7
75	Tipos_eventos	15
76	tipos_experiencias	3
77	tipos_grados	3
78	Tipos_instituciones	2
79	Tipos_materiales	0
80	Tipos_modalidades_graduaciones	6
81	Tipos_niveles_academicos	15
82	Tipos_notas	22
83	Tipos_pagos	4
84	Tipos_planes	4
85	Tipos_problemas	0
86	Tipos_producciones	7
87	Tipos_programaciones	4
88	Tipos_regularizaciones	18
89	Tipos_reportes	29
90	Tipo s_secuencias_contratos	9
91	Tipos_secuencias_memos	11
92	Tipos_sexos	2
93	Tipos_titulos	8
94	Tipos_turnos	5
95	Tr_tipos_actuaciones	3
96	Tr_tipos_alertas	2
97	Tr_tipos_correlativos	2
98	Tr_tipos_cuentas	5
99	Tr_tipos_documentos	2
100	Tr_tipos_dominios	3
101	Tr_tipos_duraciones	3
102	Tr_tipos_permisos	6
103	Tr_tipos_procesos	3
104	Tr_tipos_proveidos	4
105	Tr_tipos_validaciones	4
106	Trn_clientes_aranceles	14083
107	Trn_conceptos	1009

108	Trn_convenios	12
109	Trn_tipos_categorias	4
110	Trn_tipos_descuentos	24
111	Trn_tipos_monedas	2
112	Trn_tipos_perfiles	2
113	Trn_tipos_ubicaciones	3
114	trn_valores	6
115	Turnos	3
116	usr_log_accesos	68244
117	wk_dib_consultas	0
118	wk_dib_tablas	0
	Total	85517

ANEXO “B”
TABLAS SECUNDARIAS

TABLAS SECUNDARIAS

Nro	CLASES SECUNDARIAS	CANTIDAD DE REGISTROS
1	Dib _campos	2324
2	Dib_campos_condicion	66
3	Dib_consultas_totales	4
4	Dib_enl_campos	0
5	Dib_foraneas	490
6	Dib_primarias	217
7	Dib_tablas	229
8	Menues	2570
9	Rep_logs	94602
10	Roles	173
11	Tableros	10
12	Temp_tuplas	0
13	Usr_ips	7
14	Usr_roles	921
15	Usr_roles2	560
16	Usuarios	368
17	Almacenes	0
18	Areas_trabajos	0
19	Aulas	52
20	Aux_asignaciones	30
21	Auxiliares	29
22	Bv_accesos	83
23	Bv_bibliotecas	4
24	Bv_categorias	276
25	Bv_devolucion	392
26	Bv_digital	1264
27	Bv_estantes	12
28	Bv_libros	10841
29	Bv_material_digital	2
30	Bv_opciones	26
31	Bv_prestamos	491

32	Bv_reservaciones	0
33	Bv_usuarios	13
34	Bv_usuarios_roles	14
35	Bal_datos	3127
36	Cal_form	3
37	Cal_fr_campos	32
38	Cal_gw_relaciones	32
39	Cal_secuencias	3
40	Cal_tipos_formularios	3
41	Calendario_academico	455
42	Cedulas	636
43	Clf_tipos_documentos	215
44	Cnt_pagos	42120
45	Cnv_detalles	21750
46	Colegios	51
47	Contratos	6078
48	Convalidaciones	4845
49	Cv_curriculum	0
50	Cv_dct_adjuntos	0
51	Cv_sub_rubros	19
52	Cv_valoraciones	16
53	Dct_asignaciones	11275
54	Dct_contratos	1
55	Dct_contratos_correlativo	1
56	Dct_documentos	387
57	Dct_evaluaciones	83
58	Dct_expositores	136
59	Dct_faltas_atrasos	1506
60	Dct_responsabilidad	1
61	Dct_secuencias_contratos	639
62	Dct_secuencias_memos	657
63	Do_evaluaciones_desempenio	11121
64	Do_evaluaciones_escalafon_ind	0
65	Do_evaluadores_usuarios	2
66	Do_indicadores	18
67	Do_indicadores_escalafon	18

68	Do_sub_indicadores	42
69	Do_sub_indicadores_escalafon	18
70	Do_variables_evaluacion_desempenio	99
71	Do_variables_evaluacion_escalafon	93
72	Docentes	1295
73	Dpr_provincias	258
74	Dpto_grupos	12944
75	Est_actas_adicionales	4389
76	Est_adjuntos	19658
77	Est_asignaciones	435
78	Est_clasificaciones	20571
79	Est_compromisos	16293
80	Est_deudas	44
81	Est_documentos	184288
82	Est_kardex_estudiantil	75945
83	Est_libretas	44484
84	Est_libretas_cerradas	1348383
85	Est_menciones	278
86	Est_nuevos	10058
87	Est_programaciones	334299
88	Est_regularizaciones	5440
89	Est_secuencias_certificaciones	54
90	est_secuencias_libretas	8322
91	Est_seginst_cursover_exmesa	3506
92	Est_titulados	1247
93	Estudiantes	23520
94	Event_materiales_entregados	0
95	Eventos_personas	0
96	Facultades	15
97	Fcl_departamentos	18
98	Fcl_prg_intermedios	0
99	Fcl_programas	161
100	Grados_academicos	22
101	Grp_evaluaciones	25704
102	Grs_grupos	337
103	Hrs_periodos	0

104	Inbox	94
105	ins_campus	1
106	ins_sedes	5
107	Instituciones	520
108	kardex_auxiliar	5320
109	lbr_control_impresion	1691
110	lbr_est_secuencias	41407
111	lbr_fases	4801
112	lbr_tipos_notas	14388
113	mat_actas_validadas	1229
114	Materias	5835
115	Matriculas	76015
116	Menciones	36
117	mo_hilos	0
118	mo_segmentos	0
119	mo_sgm_destinatarios	0
120	modelos_ahorros	0
121	mtr_archivados	9004
122	mtr_electivas	12
123	mtr_entregados	12885
124	mtr_planes	10775
125	niveles_academicos	0
126	niveles_educacionales	0
127	Notas	328106
128	notas_ahorros	0
129	notas_no_matriculados	0
130	Outbox	196
131	pas_departamentos	81
132	Periodos	1
133	Personas	20273
134	Postulantes	27193
135	postulantes2	19961
136	prg_admisiones	0
137	prg_cnt_electivas	4
138	prg_controles_academicos	118
139	prg_detalles	1174

140	prg_grados_academicos	170
141	prg_modalidades_graduaciones	0
142	prg_planes	306
143	prg_planes_pagos	103
144	producciones_intelectuales	0
145	Programaciones	154544
146	prs_clasificaciones	2164
147	prs_colegios	16620
148	prs_compromisos	12060
149	prs_diplomas	0
150	prs_documentos	160640
151	prs_esp_adjuntos	21
152	prs_espacios	18
153	prs_expedidos_dips	12
154	prs_experiencias_academicas	147
155	prs_experiencias_academicas_externos	306
156	prs_experiencias_profesionales	846
157	prs_formacion_profesional	0
158	prs_historicos	0
159	prs_problemas	0
160	prs_producciones_intelectuales	86
161	prv_localidades	2487
162	pst_cpo_programas	507
163	pst_documentos	3142
164	pst_libretas	0
165	pst_matriculas	0
166	pst_personas	22972
167	pst_programaciones	0
168	pst_prs_colegios	19797
169	Semestre	236
170	ss_items	156
171	tipos_admisiones	18
172	tipos_ensenyanzas	1
173	tipos_equipamientos	0
174	tipos_graduaciones	2
175	tipos_niveles	5

176	tipos_publicaciones	0
177	tipos_secuencias_certificaciones	54
178	tipos_secuencias_libretas	1186
179	tipos_usos	0
180	tipos_ventanillas_servicios	8
181	titulaciones_academicas	548
182	Títulos	33
183	tr_adjuntos	0
184	tr_clientes_tramites	1
185	tr_datos	8040
186	tr_datos_aux	223749
187	tr_datos_log	4
188	tr_datos_log_aux	1960
189	tr_datos_log_respaldo	443
190	tr_datos_respaldo	724377
191	tr_dib_campos_acl	2
192	tr_dm_tuplas	118
193	tr_dominios	67
194	tr_gw_relaciones	1602
195	tr_informes	224
196	tr_pr_actividades	1418
197	tr_pr_actividades_alertas	1
198	tr_pr_form	271
199	tr_pr_fr_acl	3616
200	tr_pr_fr_campos	1890
201	tr_pr_fr_log	1405
202	tr_pr_fr_log_aux	174796
203	tr_pr_fr_log_respaldo	145143
204	tr_procesos	278
205	tr_proveidos	11
206	tr_proveidos_aux	17417
207	tr_proveidos_respaldo	5368
208	tr_tramites	786
209	tr_tramites_aux	30803
210	tr_tramites_log	4129
211	tr_tramites_log_aux	195228

212	tr_tramites_log_respaldo	494984
213	tr_tramites_respaldo	77180
214	Transacciones	242554
215	trn_cursos	4345
216	trn_detalles	425362
217	trn_parcelados_detalles	42
218	trn_perfiles	949
219	trn_perfiles_conceptos	7327
220	trn_perfiles_conceptos3	5061
221	trn_perfiles_materias	3044
222	trn_perfiles_procesos	964
223	trn_sedes_recibos	16
224	trn_tipos_cambios	2
225	trn_tramites_parcelados	56
226	trn_valores_detalles	4
227	ubicaciones_organicas	135
228	Universidades	17
229	Versiones	178
230	wk_dib_campos	0
231	wk_dib_campos_condicion	0
232	z_choque_materias	0
Total Registro Clases Secundarias		**6149207**

ANEXO “C”

INSTRUCTIVO-DIA-USA-INS-009

HISTORIAL DE CAMBIOS

Versión	Fecha	Acápite	Detalle
v.00	2016-10-23	Todos	Documento inicial

CONTENIDO

1. OBJETIVO

Describir la estructura conceptual del instructivo, para establecer la administración del sistema de seguridad en el gestor de la base de datos Siringuero, la cual almacena los datos de estudiantes y docentes de la Universidad Amazónica de Pando.

2. ALCANCE

El establecimiento de la Administración de un sistema de seguridad como modelo en el gestor de base de datos siringuero, abarca al servidor donde se encuentra instalado el Sistema Siringuero y el sistema gestor de base de datos postgresql.

3. RESPONSABILIDADES

El responsable de hacer cumplir el presente instructivo es el encargado/a de la Unidad de Sistemas Académicos.

El responsable que ejecutará las actividades del presente instructivo es el administrador/a del Sistema Siringuero

4. TÉRMINOS Y DEFINICIONES

Postgresql: Gestor de Bases de Datos Orientadas a Objetos

SGBD: Sistemas Gestor de Base de Datos

Siringuero: Sistema Académico.

USA: Unidad de Sistemas Académicos

5. FORMULARIOS

DIA-USA-FOR-019: Registro de la Implementación de Sistema de Seguridad en SGBD. Siringuero.

6. DIAGRAMA DE FLUJO

No aplica

7. DESARROLLO

De manera breve y concreta se describe las actividades que se realizan de acuerdo al presente instructivo.

7.1. Análisis de Riesgo en el entorno del Gestor de Base de Datos Siringuero

Lo primero que se debe realizar es el análisis de riesgo de seguridad del gestor de la base de datos siringuero, el cual se debe tomar en cuenta el riesgo físico como lógico.

- Análisis de Riesgo Físico:

En cuánto a análisis de riesgo físico se debe considerar el entorno físico en el que se encuentra instalado el gestor de base de datos siringuero, en tal sentido se debe describir lo siguiente:

a) Acceso al interno y externos al ambiente (Puertas y ventanas), deben contar con medidas de seguridad y no exento de vulnerabilidades.
b) Temperatura adecuada del ambiente
c) Cámaras y alarmas de Seguridad
d) equipos y dispositivos de red en buenas condiciones
e) equipos servidores del gestor de base de datos siringuero en buen estado

- Análisis de Riesgo Lógico:

En cuanto a riesgos lógicos se debe considerar lo siguiente:

a) Sistema Gestor de Base de Datos Postgresql Actualizado a la Última versión
b) Sistemas operativo servidor , última versión y actualizado
c) Aplicaciones Sprint Frame Works actualizado en última versión
d) Aplicaciones Firewall instalados y configurados de acuerdo a las políticas de seguridad(denegación de todos los puertos con excepción del puerto 8080/TCP)

7.2. Mantenimiento en el Gestor de Base de datos Siringuero

Para realizar adecuadamente el mantenimiento del gestor de la base de datos siringuero se deben seguir los siguientes pasos.

a) Se debe realizar el mantenimiento en cuanto se haga la transferencia de datos de una versión anterior a una nueva versión de postgresql (migración de base de datos) para lo cual se debe realizar los siguientes pasos.

- Sacar copia de la base de datos de la versión anterior
- Instalar la nueva versión de postgresql estable que sea lanzado recientemente
- Cargar la base de datos a la nueva versión
- Configurar la aplicación de conexión base de datos Sprint Frame Work

b) Ejecutar el sistema Siringuero y ejecutar prueba y error, para lo cual se debe realizar los siguientes pasos:

- Realizar prueba de funcionamiento tanto en las vistas de usuarios tomando en cuenta accesos y salidas.
- Actualizar funciones de acuerdo a la compatibilidad de la nueva versión de postgresql(en cuanto surjan errores)
- Realizar pruebas y errores de los controladores, implementación y conectividad (xml, sql map,impl,mi facade).

c) Realizar mantenimiento de la estructura de la base de datos los cuales se deben tomar en cuenta los siguiente pasos.

- Prueba y error de la estructura de las tablas
- Establecer las relaciones entre tablas(secuencias y referencias)

7.3. Implementación de Medidas de Seguridad

Una vez instalado y configurado el sistema gestor de base de datos postgresql, se debe instalar medidas de seguridad la cual se deben seguir los siguientes pasos

a) Crear usuario y roles de acuerdo a los métodos que incorpora la nueva versión de postgresql

b) Configurar accesos (pg_hba.conf), se debe establecer el usuario, la base de datos y el ip de donde va acceder el servidor de aplicaciones, además el método de acceso.

c) Configurar la conectividad y el puerto (postgresql.conf), la cual se debe establecer lo siguiente:

- Habilitar la opción listen address, dispositivos de escucha
- Habilitar el puerto 5432 (se sugiere cambiar de puerto) por seguridad

d) Instalación y configuración del firewall WFW

8. REFERENCIAS

No alpaca

9. ARCHIVO FORMULARIOS

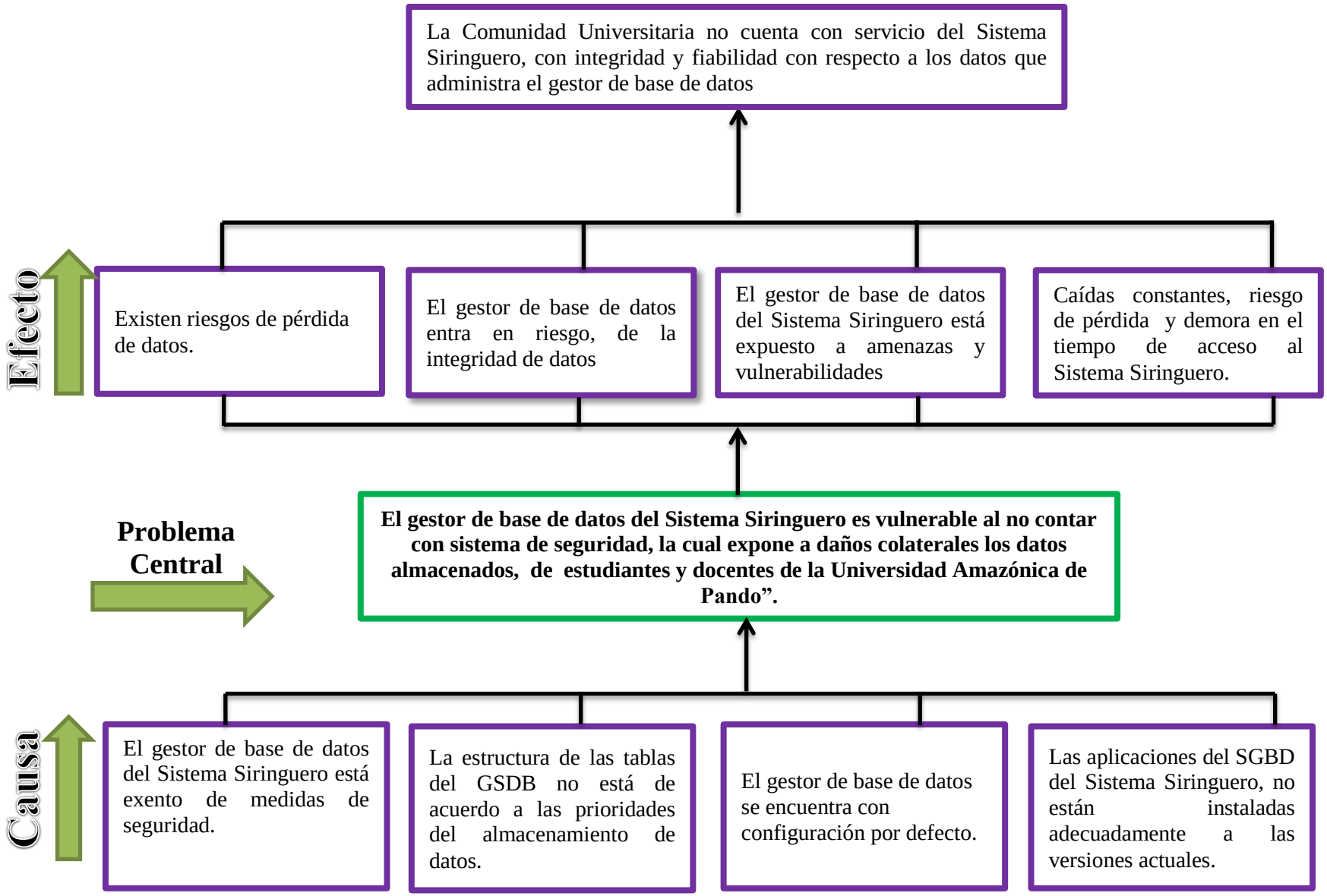
Nº	Codificación	Descripción	Lugar de archivo	Tiempo de custodia (año)
1	DIA-USA-FOR-019	Registro de la Implementación de Sistema de Seguridad en SGBD. Siringuero	USA	5

ANEXO “D”

FORMULARIO-DIA-USA-FOR-019

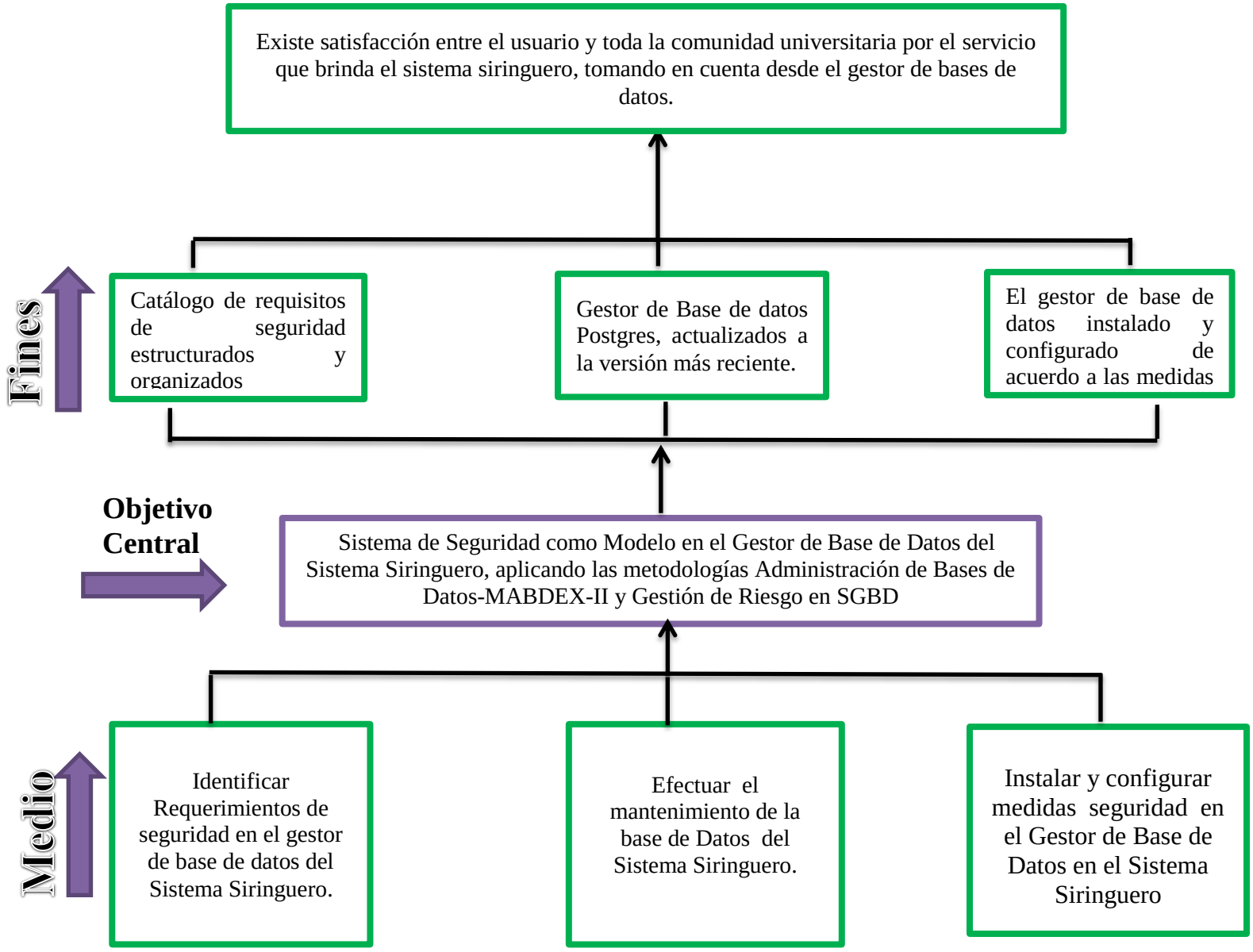
ANEXO “E”

ÁRBOL DEL PROBLEMAS


La Comunidad Universitaria no cuenta con servicio del Sistema Siringuero, con integridad y fiabilidad con respecto a los datos que administra el gestor de base de datos
Efecto
Existen riesgos de pérdida de datos.
El gestor de base de datos entra en riesgo, de la integridad de datos
El gestor de base de datos del Sistema Siringuero está expuesto a amenazas y vulnerabilidades
Caídas constantes, riesgo de pérdida y demora en el tiempo de acceso al Sistema Siringuero.
Problema Central
El gestor de base de datos del Sistema Siringuero es vulnerable al no contar con sistema de seguridad, la cual expone a daños colaterales los datos almacenados, de estudiantes y docentes de la Universidad Amazónica de Pando".
Causa
El gestor de base de datos del Sistema Siringuero está exento de medidas de seguridad.
La estructura de las tablas del GSDB no está de acuerdo a las prioridades del almacenamiento de datos.
El gestor de base de datos se encuentra con configuración por defecto.
Las aplicaciones del SGBD del Sistema Siringuero, no están instaladas adecuadamente a las versiones actuales.

ANEXO “F”

ÁRBOL DE OBJETIVOS


Existe satisfacción entre el usuario y toda la comunidad universitaria por el servicio que brinda el sistema siringuero, tomando en cuenta desde el gestor de bases de datos.
Fines
Catálogo de requisitos de seguridad estructurados y organizados
Gestor de Base de datos Postgres, actualizados a la versión más reciente.
El gestor de base de datos instalado y configurado de acuerdo a las medidas
Objetivo Central
Sistema de Seguridad como Modelo en el Gestor de Base de Datos del Sistema Siringuero, aplicando las metodologías Administración de Bases de Datos-MABDEX-II y Gestión de Riesgo en SGBD
Medio
Identificar Requerimientos de seguridad en el gestor de base de datos del Sistema Siringuero.
Efectuar el mantenimiento de la base de Datos del Sistema Siringuero.
Instalar y configurar medidas seguridad en el Gestor de Base de Datos en el Sistema Siringuero