UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GESTIÓN DE BASES DE DATOS II VERSIÓN

TEMA:

"ELABORACIÓN DE UNA METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE VULNERABILIDADES DE BASE DE DATOS Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AUTOMEKANO CÍA. LTDA., DE LA CIUDAD DE AMBATO".

Trabajo de Investigación, previo a la obtención del Grado Académico de Magíster en Gestión de Bases de Datos.

Autora: Ingeniera Carolina Anabel Bonilla Vaca

Director: Ingeniero Marco Vinicio Altamirano Ruiz, Mg.

Ambato – Ecuador

2017

A la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas Electrónica e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por el *Ingeniero, José Vicente Morales Lozada Magíster* e integrado por los señores: *Ingeniero Kléver Renato Urvina Barrionuevo Magíster, Ingeniero David Omar Guevara Aulestia Magíster y el Ingeniero Milton Patricio Navas Moya Magíster,* designados por la Unidad Académica de Titulación de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "*Elaboración de una Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos y su incidencia en la Seguridad de la Información de la Empresa Automekano Cía. Ltda., de la ciudad de Ambato*", elaborado y presentado por la señorita *Ingeniera Carolina Anabel Bonilla Vaca,* para optar por el Grado Académico de Magíster en Gestión de Bases de Datos; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. José Vicente Morales Lozada, Mg.
Presidente del Tribunal

Ing. Kléver Renato Urvina Barrionuevo, Mg.
Miembro del Tribunal

Ing. David Omar Guevara Aulestia, Mg.
Miembro del Tribunal

Ing. Milton Patricio Navas Moya, Mg.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: "ELABORACIÓN DE UNA METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE VULNERABILIDADES DE BASE DE DATOS Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AUTOMEKANO CÍA. LTDA., DE LA CIUDAD DE AMBATO", le corresponde exclusivamente a la *Ingeniera Carolina Anabel Bonilla Vaca* Autora bajo la Dirección del *Ingeniero Marco Vinicio Altamirano Ruiz Magíster* Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniera Carolina Anabel Bonilla Vaca

C.C. 180349897-9

AUTORA

Ingeniero Marco Vinicio Altamirano Ruiz, Mg.

C.C. 180291638-5

DIRECTOR

DERECHOS DE AUTORA

Autorizo a la Universidad Técnica de Ambato para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniera Carolina Anabel Bonilla Vaca

C.C. 180349897-9

AUTORA

DEDICATORIA

El presente esfuerzo y dedicación lo entrego a Dios, que me permite tener cada día nuevas oportunidades de ser mejor persona.

A mi familia que tanto amo, mi mami Gladys, mi papi Carlos, mis hermanas Pauly y Gaby y mis sobrinos Heidi y Benjamín que siempre los llevo en mi corazón por ser las personas más importantes de mi vida.

Y finamente dedico cada esfuerzo de mi vida a mí misma, porque he sabido luchar incansablemente por cada una las metas y objetivos que me he propuesto, por tener ese valor para salir adelante ante toda adversidad, siempre constante y perseverante por cumplir cada uno de mis anhelos y sueños.

Anabel Bonilla

AGRADECIMIENTO

Muy agradecida con Dios por todas las cosas que ha hecho posible cada día de mi vida.

A mi madre que ha sido mi fortaleza, mi luz en el camino y lo más grande que Dios me pudo dar, a mi padre por sus consejos y apoyo incondicional. A mis hermanas Pauly y Gaby que han sido mis compañeras en cada etapa de mi vida, esas mujeres valientes y luchadoras que me han motivado día a día y que me han regalado a mis dos tesoros más grandes Heidi y Benjamín que son dueños de mi corazón.

A esta noble institución que me abrió las puertas de sus aulas, para formar de mí una profesional con ética y valores intachables, que ama su profesión y brinda cada día lo mejor de sí para aportar al crecimiento de su entorno y su País.

Al Ingeniero, Marco Vinicio Altamirano Ruiz, Mg. por guiarme en cada fase del presente trabajo de investigación, lo que ha permitido que pueda culminar una etapa más de mi formación como profesional.

La Autora

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GESTIÓN DE BASES DE DATOS

TEMA:

"ELABORACIÓN DE UNA METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE VULNERABILIDADES DE BASE DE DATOS Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AUTOMEKANO CÍA. LTDA., DE LA CIUDAD DE AMBATO".

AUTOR: *Ingeniera Carolina Anabel Bonilla Vaca*
DIRECTOR: *Ingeniero Marco Vinicio Altamirano Ruiz, Mg.*
FECHA: *08 de abril del 2016*

RESUMEN EJECUTIVO

La empresa Automekano Cía. Ltda., de la ciudad de Ambato al igual que cualquier otra empresa moderna del país, cuenta con un sistema de información transaccional que almacena la información en una base de datos, la misma que puede estar expuesta a muchos factores como la presencia de amenazas y vulnerabilidades de seguridad que pudieran afectar al sistema de base de datos como tal e incidir en la seguridad de la información de la empresa.

La información recabada con las técnicas instrumentales empleadas permitió enfocar la investigación para determinar que la empresa no contaba con una metodología que permita detectar y mitigar las vulnerabilidades de base de datos, es así que, a través del estudio y comparación de metodologías de testeos y análisis de seguridad existentes, se pudo determinar que la metodología abierta OSSTMM cuenta con varios fases de análisis y métodos de testeos de seguridad que pudieron ser tomados como línea base para establecer una propuesta investigativa para la

elaboración de una Metodología Detección y Mitigación de Vulnerabilidades de Base de Datos (DMV-BDD); la misma que para ser demostrada implicó la ejecución y realización de sus diferentes etapas con la ayuda de técnicas y herramientas para testeo de seguridad, además del análisis de vulnerabilidades de base de datos, que finalmente ayudó a la detección de varias vulnerabilidades críticas y severas en el sistema de base de datos de la empresa.

La metodología propuesta demostró no solo la existencia de vulnerabilidades sino también permitió presentar las recomendaciones de mitigación que permitirán a la empresa corregir, prevenir y fortalecer la seguridad de su base de datos, de tal manera que se pueda mejorar todos los aspectos de la seguridad de información como son la confidencialidad, integridad y disponibilidad de la información.

Finalmente se puede indicar que la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos (DMV-BDD) contempla características que le permiten ser un aporte investigativo a la comunidad, ya que es un instrumento de investigación consistente y que puede repetirse, además de ser posible aplicarla en empresas similares, ya que tiene una validez más allá del periodo de tiempo "actual".

La metodología propuesta para poder aplicarse, el investigador solo necesita tener conocimientos básicos de seguridad de información y tener algunos méritos de analista y testeador de seguridad.

Descriptores: *Información, Base de Datos, Sistema de Información, Seguridad de la Información, Análisis, Detección, Mitigación, Amenaza, Riesgo, Metodología.*

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GESTIÓN DE BASES DE DATOS

THEME:

"DEVELOPMENT OF A METHODOLOGY OF DETECTION AND MITIGATION VULNERABILITY DATABASE AND ITS IMPACT ON INFORMATION SECURITY IN COMPANY AUTOMEKANO CÍA. LTDA., FROM AMBATO CITY".

AUTHOR: Engineer *Carolina Anabel Bonilla Vaca*
DIRECTED BY: Engineer *Marco Vinicio Altamirano Ruiz, Mg*.
DATE: *April 08, 2016*

EXECUTIVE SUMMARY

Automekano Limited Company in the Ambato city, like any other modern company in the country, It is provided with an information system that saves in a database, it can be exposed to many factors such as the presence of threats and security vulnerabilities that could be affect the database system so that its incidence in the security of information.

The information obtained by the instrumental techniques allowed to focus research to determine that the company not have a methodology to detect and mitigate vulnerabilities database, so that, through the study and comparison of methodologies of testing and analysis existing security, it was determined that the methodology OSSTMM has several phases of analysis and methods of security testing that could be taken as a base to establish a research proposal for making a Methodology Detection and Mitigation Vulnerability Database (DMV-BDD); the same one that to be demonstrated implied the execution and achievement of different stages with the

help of techniques and tools for security testing, in addition to the analysis of vulnerabilities database, finally it helped to detection of several critical and severe vulnerabilities in the company database systems.

The proposed methodology demonstrated the existence of vulnerabilities, also allowed to present mitigation recommendations that will be enable the company to correct, prevent and strengthen the security of its database, so you can improve all aspects of security information such as integrity, availability and confidentiality of information.

Finally, it may indicate that the methodology Detection and Mitigation Vulnerability Database (DMV-BDD) have characteristics that it allow to be a research contribution to the community as it is an instrument of consistent investigation and which may be repeated, In addition being possible to apply in similar companies, as it has a validity period beyond the "current" time.

The methodology proposed for the researcher to apply only needs to have basic knowledge of information security and have some merits of analyst and security tester.

Descriptors: *Information, Database, Information System, Information Security, Analysis, Detection, Mitigation, Threats, Risks, Methodology.*

INTRODUCCIÓN

El Proyecto de Investigación tiene como tema**:** "Elaboración de una Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos y su incidencia en la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato", está organizado por capítulos, que contienen lo siguiente:

El Capítulo I descrito como EL PROBLEMA DE LA INVESTIGACIÓN contiene: el planteamiento del problema, la contextualización, el análisis crítico, la prognosis, la formulación del problema, las interrogantes, la delimitación del objeto de investigación, la justificación, los objetivos generales y los objetivos específicos.

El Capítulo II descrito como MARCO TEÓRICO está compuesto por: los antecedentes investigativos, la fundamentación filosófica, la fundamentación legal, las categorías fundamentales de la variable independiente y dependiente, la hipótesis y el señalamiento de variables.

El Capítulo III descrito como METODOLOGÍA contiene: la modalidad básica de la investigación, el nivel o tipo de investigación, la población y muestra, la operacionalización de variables y el plan de recolección y procesamiento de información.

En el Capítulo IV denominado ANÁLISIS E INTERPRETACIÓN DE RESULTADOS, se detalla el análisis de resultados e interpretación de datos que ayudan a la verificación de la hipótesis.

En el Capítulo V señalado como CONCLUSIONES Y RECOMENDACIONES, contiene las mismas en base a la teoría investigada y en base a la propuesta que permite validar y concluir la importancia de realizar la propuesta de la investigación.

En el Capítulo VI detalla LA PROPUESTA, se presenta la elaboración y resultados de la solución al problema, que para este caso es el desarrollo de las etapas de la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos.

Como complemento se tiene la bibliografía tentativa y los anexos.

CAPÍTULO I

EL PROBLEMA

1.1. Tema

“Elaboración de una Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos y su incidencia en la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato”.

1.2. Planteamiento del problema

1.2.1. Contextualización

En la actualidad la información es el activo más valioso de las empresas, todas las actividades que se abstraen de las tareas cotidianas se procesan en un sistema de información mediante el uso de medios tecnológicos y se almacena en un repositorio de información conocido como base de datos.

Concebida la importancia de la información digital, el presente tema de investigación permite plasmar en una metodología la gestión adecuada para la seguridad de la información que permita prevenir amenazas o riesgos de seguridad que atente contra la información de la base de datos.

A nivel mundial muchas organizaciones y empresas de toda índole, para poder realizar sus actividades diarias de forma ágil, eficiente y eficaz, trasforman sus procedimientos manuales a procesos automatizados mediante el uso de sistemas de información, a diario se trabaja con información digital como resultado de las

actividades empresariales; lo que implica el uso de tecnologías de información como: sistemas de información, bases de datos, redes de comunicación, entre otros. Este tipo de innovaciones tecnológicas proporcionan grandes beneficios al mundo empresarial, pero también podría causar potenciales amenazas y riesgos a la seguridad de su información, ocasionando diversos tipos de daños y perjuicios como: robo de información, fraude, espionaje, sabotaje, vandalismo, entre otros; a los que se les conoce también como ataques informáticos o vulnerabilidades tecnológicas.

El portal web (**Computerhoy, 2015**) publica un artículo denominado: Los ataques cibernéticos más peligrosos del 2015; donde se describen muchos casos donde se vulneró la seguridad de muchas de las bases de datos, para lo cual destacan los siguientes casos:

Hacking Team

En junio del 2015, Hacking Team, una empresa italiana que vende herramientas de espionaje y vigilancia a gobiernos y empresas, sufrió en primera persona el ataque de un hacker desconocido. Este ciberdelincuente filtró la base de datos, los correos electrónicos internos y parte del código fuente que habían desarrollado.

Ashley Madison

En julio de este año un grupo de hackers accedieron a la base de datos de este popular portal de citas y publicaron información muy comprometida sobre los usuarios de este servicio. En teoría, los ciberdelincuentes reclamaban más seguridad e iniciaron sus ataques para demostrar a Ashley Madison que eran muy vulnerables. Sin embargo, no está clara la intención de los hackers ni los detalles del caso. Este escándalo recorrió el mundo porque la identidad de más de 11 millones de usuarios fue expuesta en Internet y esto provocó toda clase de reacciones.

VTech

VTech es una empresa china especializada en juguetes para el aprendizaje. La compañía sufrió un ataque contundente y se filtraron los datos privados de más de 4.8 millones de padres y 200.000 niños. Finalmente, la cifra de afectados llegó hasta los 6.7 millones. El caso de VTech recorrió el mundo por las graves implicaciones que supone la filtración masiva de la información personal de los menores.

Hello Kitty

Hello Kitty sufrió el mismo tipo de ataque de VTech y los hackers llegaron a robar información de 3.3 millones de clientes. Lo curioso es que la compañía desconocía que era víctima de un ataque informático muy sofisticado hasta que un investigador de seguridad denunció el tema ante las autoridades pertinentes.

OPM

La Oficina de Administración de Personal gestiona los datos de todos los empleados públicos norteamericanos, incluido el personal militar. El ataque se realizó en marzo, pero el caso salió a la luz en junio del 2015. En un primer momento se desconocían las dimensiones del problema y finalmente la cifra de afectados se elevó hasta más de 21 millones de perfiles robados**.**

Cada día que pasa las amenazas, vulnerabilidades y riesgos de la información van en aumento debido a factores externos que los fomentan, principalmente factores económicos que impulsan a miles de individuos a buscar la manera de atacar a las empresas u organizaciones, ante esta problemática latente es importante que se continúen realizando investigaciones de nuevos métodos de análisis y detección vulnerabilidades de seguridad que permita prevenir y mitigar este tipo de problemas de seguridad de las bases de datos empresariales.

Como se puede evidenciar las amenazadas y/o riesgos que desafía la información digital de cualquier organización o empresa, se hacen cada vez más comunes en cualquier medio o ámbito organizacional y es preocupante como estas se vuelven cada vez más sofisticadas.

Fraude informático deja 4.287 víctimas en tres años.

Desde el 2009 el aumento de denuncias es dramático, en ese año se reportaron solamente 168 casos, mientras que en lo que va de 2012 llegan a 1.564. La Fiscalía General del Estado promueve un marco legal flexible para ser incluido en el nuevo Código Penal Integral.

Los delitos informáticos tienen un apogeo mundial y Ecuador no es ajeno a esa tendencia, señaló el Fiscal General de Estado, Galo Chiriboga, quien enfatizó que ese podría ser un gran problema en el futuro si no se logran identificar claramente los tipos penales de los delitos que se cometen a través de la tecnología. (**EL TELÉGRAFO, 2012: 10**).

Sin duda alguna en el Ecuador así como en todo el mundo, las cifras que ponen en evidencia los peligros que corre la información digital de las organizaciones y empresas van en aumento, a medida que los procesos manuales se van modernizando con la ayuda de la implementación de tecnologías de información y como parte fundamental del crecimiento empresarial del país, las diferentes amenazas y riesgos a los que se enfrenta la información tiene mayor probabilidad de ocurrir; debido a que gran parte de las empresas ecuatorianas no le dan la importancia necesaria a la protección de la información digital, al parecer por ahora están enfocadas en la implementación de nuevas tecnologías que les lleve a modernizar sus procesos, pero aún no están conscientes que existen varios factores que podría ser objetos para la vulneración de la seguridad de la información digital, lo que indudablemente converge a que individuos malintencionados puedan sacar provecho de esto; razón por la que todo proceso de innovación tecnológica en las empresas del país, deben ir de la mano con la debida gestión de las posibles amenazas y riesgos a los que se expone la información digital.

La empresa Automekano Cía. Ltda., al igual que cualquier otra empresa del país no está exenta de estar expuesta a ser objeto de amenazas y vulnerabilidades de seguridad, tales como accesos no autorizados a la información que se almacena en su base de datos, lo que podría ocasionar consecuencias tan simples que alteren el desempeño empresarial o tan complejas como la paralización de las operaciones del negocio, que resulte en el posible incumplimiento de los objetivos de la empresa.

Las tecnologías que intervienen en las actividades del negocio de la empresa Automekano Cía. Ltda., no cuentan con metodologías que permitan realizar análisis de seguridad de información de la base de datos, dando como resultado el desconocimiento de la posible existencia de vulnerabilidades, así como se pone en evidencia la inexistencia de métodos que permiten prevenir y mitigar vulnerabilidades de seguridad de la base de datos y de los sistemas que conviven o interactúan con la misma; posibles factores que hacen que la información empresarial que es un activo invaluable no tenga formas de garantizar la confidencialidad , integridad y disponibilidad de la información contenida en la base de datos empresarial.

1.2.2. Análisis crítico

La empresa Automekano Cía. Ltda., cuenta con un sistema de información transaccional con el fin de brindar eficiencia y agilizar la gestión y administración de cada una de sus actividades, dando como resultado el procesamiento de la información que finalmente se almacena en una base de datos.

La información digital es el activo más importante para la empresa, es preocupante evidenciar que durante el proceso de investigación, se haya descubierto el escaso uso de metodologías de detección y mitigación de vulnerabilidades de base de datos, así como también la omisión de ejecución de procesos actualización en el Sistema Gestor de Base de Datos, lo que puede converger en posibles amenazas o el incremento de brechas de seguridad, poniendo así en un estado crítico a la información, ya que se encuentra constantemente expuesta a una serie de posibles riesgos, lo que resultaría poco factible establecer un entorno seguro para la información por la posible pérdida de las tres características básicas de la seguridad de la información como son: la confidencialidad, la integridad y la disponibilidad.

El resultado de todo lo manifestado podría ser causante de que la empresa Automekano Cía. Ltda., no tenga establecidas metodologías para realizar detección de vulnerabilidades de forma periódica, las mismas que ayuden a detectar amenazas y riesgos de seguridad, con lo que se lograría la reducción de posibles problemas en la información, además de poder prevenir y mitigar amenazas y riesgos, así como fortalecer la seguridad de la base de datos, con lo que se podría evitar consecuencias para la empresa que a corto o a largo plazo llegue a un punto que no pueda tener la capacidad de cumplir todos los objetivos del giro del negocio.

Árbol de problemas

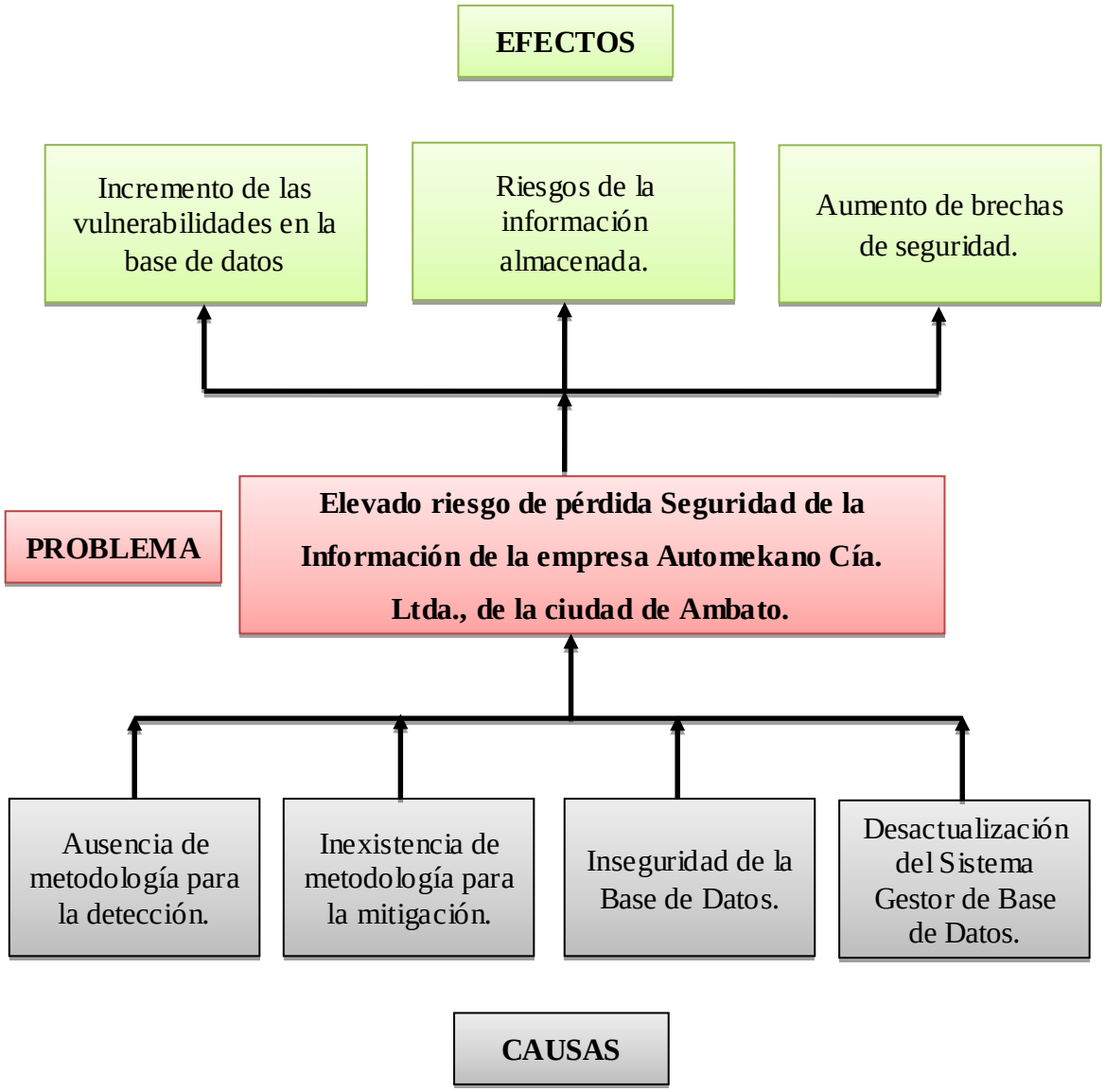


Figura N° 1. Árbol de Problemas

Elaborado por: Investigadora

1.2.3. Prognosis

Al encontrarse la información almacenada y centralizada en una base de datos, focalizamos todo el funcionamiento del sistema de información de la empresa en un solo repositorio centralizado de datos.

La ausencia de metodologías de detección y mitigación de vulnerabilidades en la base de datos, podría poner en riesgo la información, atentando así contra la seguridad del activo más impórtate de la empresa; la omisión de actualizaciones del Sistema Gestor de Base de Datos se convertiría en una amenaza, ya que si un atacante pudiera aprovechar de una o varias vulnerabilidades existentes, podría atentar contra la seguridad de la información. Normalmente se podría detectar varias amenazas y riesgos a partir de la detección de la existencia de vulnerabilidades e independientemente de que se comprometa o no la seguridad del sistema de información.

Al comprometerse la seguridad de la información, se correría el riesgo de que la información pueda ser conocida y utilizada sin autorización por cualquier persona dentro o fuera de la empresa, pudiendo perderse así la confidencialidad de la misma, ocasionando perjuicios incalculables para la empresa.

Otro riesgo latente se tendría si la información sufriera modificaciones no autorizadas, lo que traería consecuencias significativas para la integridad de la información, lo que podría afectar a las actividades de gestión y administración empresarial.

Finalmente, el riesgo más alto para la empresa sería la pérdida de disponibilidad de la información, que significaría la inaccesibilidad a la información, afectando las actividades normales, la mima que, podría presentarse por periodos cortos de tiempos como horas, largos como días o semanas, o incluso periodos no definidos de tiempo; lo que probablemente causaría grandes pérdidas a la empresa y la incapacidad para cumplir sus objetivos.

1.2.4. Formulación del problema

¿Es factible elaborar una Metodología para la Detección y Mitigación de Vulnerabilidades de Base de Datos para mejorar la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato?

1.2.5. Interrogantes

- ¿Es posible realizar un análisis de vulnerabilidades de base de datos de la empresa Automekano Cía. Ltda., basada en la metodología OSSTMM (Open Source Security Testing Methodology Manual – Manual de Metodología de Testeo de Seguridad de Código Abierto)?

- ¿Es factible establecer y documentar recomendaciones para la mitigación de las vulnerabilidades de base de datos de la empresa Automekano Cía. Ltda.?

- ¿Se puede documentar la metodología que permita detectar y mitigar vulnerabilidades de base de datos para mejorar la seguridad de la información de la empresa Automekano Cía. Ltda.?

1.2.6. Delimitación del objeto de investigación

Delimitación del contenido:

Campo: Ingeniería de Sistemas.
Área: Base de datos
Aspecto: Seguridad de la Información.

Delimitación espacial

El trabajo de investigación se realizará en la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

Delimitación temporal

La investigación se realizará desde abril del 2016 a octubre del 2016.

1.3. Justificación

La elaboración de una Metodología para la Detección y Mitigación de Vulnerabilidades de Base de Datos, significaría un aporte valioso a la seguridad de la información de la empresa Automekano Cía. Ltda., además representaría poder contar con un sistema de información estable y seguro que permita la gestión y desarrollo de las actividades empresariales.

Gracias al apoyo de la Gerencia General de la empresa y al gran interés y colaboración del Jefe de Sistemas en el desarrollo del presente proyecto de investigación; a futuro con la aplicación de la presente investigación se obtendrán beneficios como la posibilidad de prevenir y eliminar todas las vulnerabilidades, amenazas y riesgos de información detectados, que permitirá lograr un aumento en la seguridad de la base de datos y poder contar con la confidencialidad, integridad y disponibilidad de la información, para que la ejecución de las actividades empresariales nunca se vean perjudicadas.

La elaboración de la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos que plantea el presente proyecto, contemplará características que le permitirán ser un aporte investigativo a la comunidad en lo referente a metodologías de análisis de seguridad de sistemas de base datos, detección de vulnerabilidades de base de datos, así como en el planeamiento de posibles acciones para la prevención y mitigación, lo que permitirá fortalecer la seguridad de la base de datos.

Finalmente la metodología podrá ser utilizada como un instrumento de investigación consistente y que puede ser utilizada y aplicada de forma repetitiva en empresas similares, debido a que la metodología a desarrollarse proyecta tener una validez más allá del periodo de tiempo “actual”. A todo esto cabe destacar también que podrá ser aplicada por investigadores que solo necesitaran tener conocimientos básicos de

seguridad de información y tener algunos méritos de analistas y testeadores de seguridad.

La factibilidad de elaboración del presente proyecto de investigación se realizará en base a tres aspectos importantes:

Factibilidad técnica. **-** La empresa Automekano Cía. Ltda., de la ciudad de Ambato, cuenta con un repositorio de información alojada en una base de datos, que permite la realización de la metodología para la detección y mitigación de vulnerabilidades de base de datos, fundamentado en la metodología abierta de testeo de seguridad OSSTMM.

Factibilidad operativa. **-** Existe la aprobación del Gerente General y el apoyo del Departamento de Sistemas de la empresa Automekano Cía. Ltda., para realización de la presente investigación, lo que permitirá el uso de las herramientas para el análisis de seguridad en la base de datos de la empresa en pro de la seguridad de la información.

Factibilidad económica. - Es factible ya que la investigadora cubrirá con los gastos económicos que implica todas las etapas del desarrollo del presente proyecto de investigación.

1.4. Objetivos

1.4.1. General

Determinar la incidencia de una Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos en la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

1.4.2. Específicos

- Realizar un análisis del método actual que se utiliza para detectar vulnerabilidades de base de datos de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

- Determinar las posibles recomendaciones para prevenir y mitigar las vulnerabilidades encontradas en la base de datos de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

- Proponer una metodología que permita detectar y mitigar vulnerabilidades de base de datos de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes investigativos

Existen investigaciones previas acerca de las metodologías de detección y mitigación de vulnerabilidades de base de datos. Rescatado del análisis e investigación bibliográfica de manuales, tesis, artículos científicos y revistas relacionados con las vulnerabilidades de base de datos.

La Universidad Nacional de Costa Rica y la Facultad de Ciencias Exactas y Naturales, Escuela de Informática, publica el trabajo de investigación titulado "*Vulnerabilidades de Sistemas Gestores de Base de Datos*" en cuyas recomendaciones **Villalobos (2008: 134)** describe considerar una buena política de seguridad, basada en prevención preferiblemente de tal forma que se pueda describir el aseguramiento de la configuración, realizar un cambio periódico de claves, implementar software que permita realizar monitoreos constantes, la aplicación de un buen diseño de interfaces para evitar los ataques de inyección, fortalecer la seguridad a través de procesos de cifrado, contemplar establecer programas para auditorías y lograr el fortalecimiento con la aplicación de parches.

Los administradores de las bases de datos o los administradores de seguridad deben estar actualizados con los nuevos tipos de ataques, para lo que se deben enfocar en la creación de controles para alcanzar seguridad de las mismas.

Un artículo publicado por Oracle sobre seguridad de bases de datos, describe que la administración de bases de datos debe considerar los siguientes pasos para un lograr un protocolo de seguridad:

1. Instalar solo lo requerido.
2. Cerrar todas las cuentas expiradas.
3. Habilitar la protección del Diccionario de Datos.
4. Otorgar sólo los privilegios necesarios.
5. Autenticar correctamente sus clientes.
6. Restringir el acceso al sistema operativo.
7. Restringir el acceso a la red.
8. Proteger y cifrar.
9. Usar el Firewall adecuadamente.
10. Instalar parches.
11. Cambiar los parámetros por defecto.

Y otros más. Pero lo principal es prevenir.

La Universidad Autónoma del Carmen de México, publica el trabajo de investigación titulado *"Protección a la base de datos de una PYME"*, **García y Formoso (2013: 6)** describen la siguiente conclusión:

> La información almacenada en las bases de datos de una Pyme debe ser el valor a proteger por parte de todos los miembros de la organización, sin embargo no significa que todos tengan el acceso a la misma, es de gran importancia propiciar buenos hábitos y planes de seguridad que permitan a la Pyme dedicarse a producir con la garantía y seguridad que la información siempre estará bien resguardada y que en el caso de verse afectados por algún tipo de delito, este no implicaría mayor preocupación ya que la información perdida muy difícilmente podrá ser usada por otras personas.

La Charotar University of Science & Technology (CHARUSAT) de Changa, publica el trabajo de investigación titulado "*Database Security – Attacks and Control Methods (Seguridad de base de datos Ataques y Métodos de Control)"*, los autores **Malik y Patel (s.f.: 8)**. concluyen en su investigación:

> En resumen, la protección de acceso comienza con quién puede acceder a los datos y qué tipo de atacantes de datos desea acceder.

> Hay un montón de posibilidades para mejorar las técnicas utilizadas para la seguridad de la base de datos.
>
> Según la encuesta el 84% de las empresas consideran que la seguridad de base de datos es adecuada, 73% de las empresas que predicen base de datos adjuntos va en aumento día a día, 48% de los agresores son los usuarios autorizados, 48% de los usuarios han hecho mal uso de sus privilegios.
>
> También se han discutido las cuestiones relacionadas con la seguridad de base de datos. Se presentan varias propuestas de modelos de seguridad discrecional y obligatoria para la protección de las bases de datos convencionales. Sin embargo, no hay un estándar para el diseño de estos modelos de seguridad. El trabajo presentado en este documento ofrece información recogida de las diferentes amenazas y sus problemas de seguridad de la base de datos. Se puede extender para definir, diseñar e implementar una política de seguridad efectiva en un entorno de base de datos y proporcionar una visión consolidada de la seguridad de base de datos. De acuerdo con la encuesta de este trabajo, se centró en las amenazas y sus posibles contramedidas que pueden ser posibles para asegurar los datos en bases de datos.

La Revista Internacional de Investigación Avanzada en Ciencias de la Computación e Ingeniería de Software publica el trabajo de investigación titulado "*Database Security: Threats and Challenges*" en el que los autores **Rohilla y Kumar (2013: 813)** concluyen lo siguiente:

> Las bases de datos son un blanco favorito para los atacantes debido a sus datos. Hay muchas formas en que una base de datos puede verse comprometida. Hay varios tipos de ataques y amenazas de las que una base de datos debe ser protegida. Se han encontrado soluciones a la mayoría de las amenazas mencionadas anteriormente, aunque algunas soluciones son buenas mientras que algunos son sólo temporales. Las diversas amenazas a la base de datos se analizan en este trabajo.

2.2. Fundamentación filosófica

La presente investigación se relaciona con el paradigma filosófico crítico propositivo; es crítico ya que se realiza un análisis objetivo del problema de una realidad contingente y propositivo porque plantea una propuesta de solución al

problema investigado basado en la existencia de múltiples realidades técnicamente construidas.

2.3. Fundamentación legal

La **Asamblea Nacional (2014: 37-37)**, de conformidad con las atribuciones que le confiere la Constitución de la República del Ecuador y la Ley Orgánica de la Función Legislativa, discutió y aprobó el CÓDIGO ORGÁNICO INTEGRAL PENAL.

> En sesión del 28 de enero del 2014, el Pleno de la Asamblea Nacional conoció y se pronunció sobre la objeción parcial del Código Orgánico Integral Penal enviada por el señor Presidente Constitucional de la República.
>
> Libro primero - la infracción penal. Título IV - Infracciones en particular. Capítulo tercero: Delitos contra los derechos del buen vivir. Sección tercera.
>
> **Delitos contra la seguridad de los activos de los sistemas de información y comunicación.**
>
> **Artículo 229.- Revelación ilegal de base de datos. -** La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.
>
> Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.
>
> **Artículo 230.- Interceptación ilegal de datos. -** Será sancionada con pena privativa de libertad de tres a cinco años:
>
> 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

2.4. Categorías fundamentales

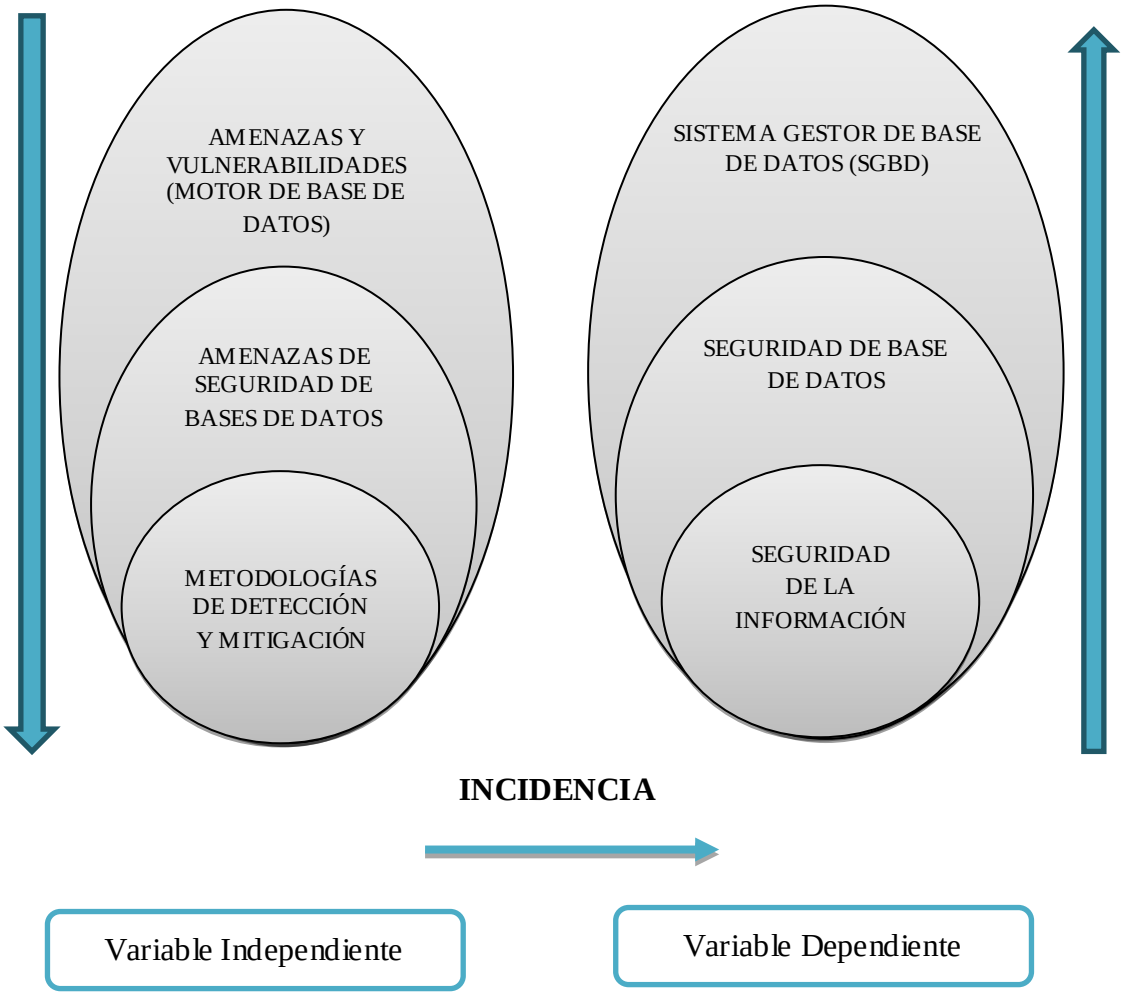


Figura N° 2. Categorías Fundamentales

Elaborado por: Investigadora

Constelación de ideas de la variable independiente

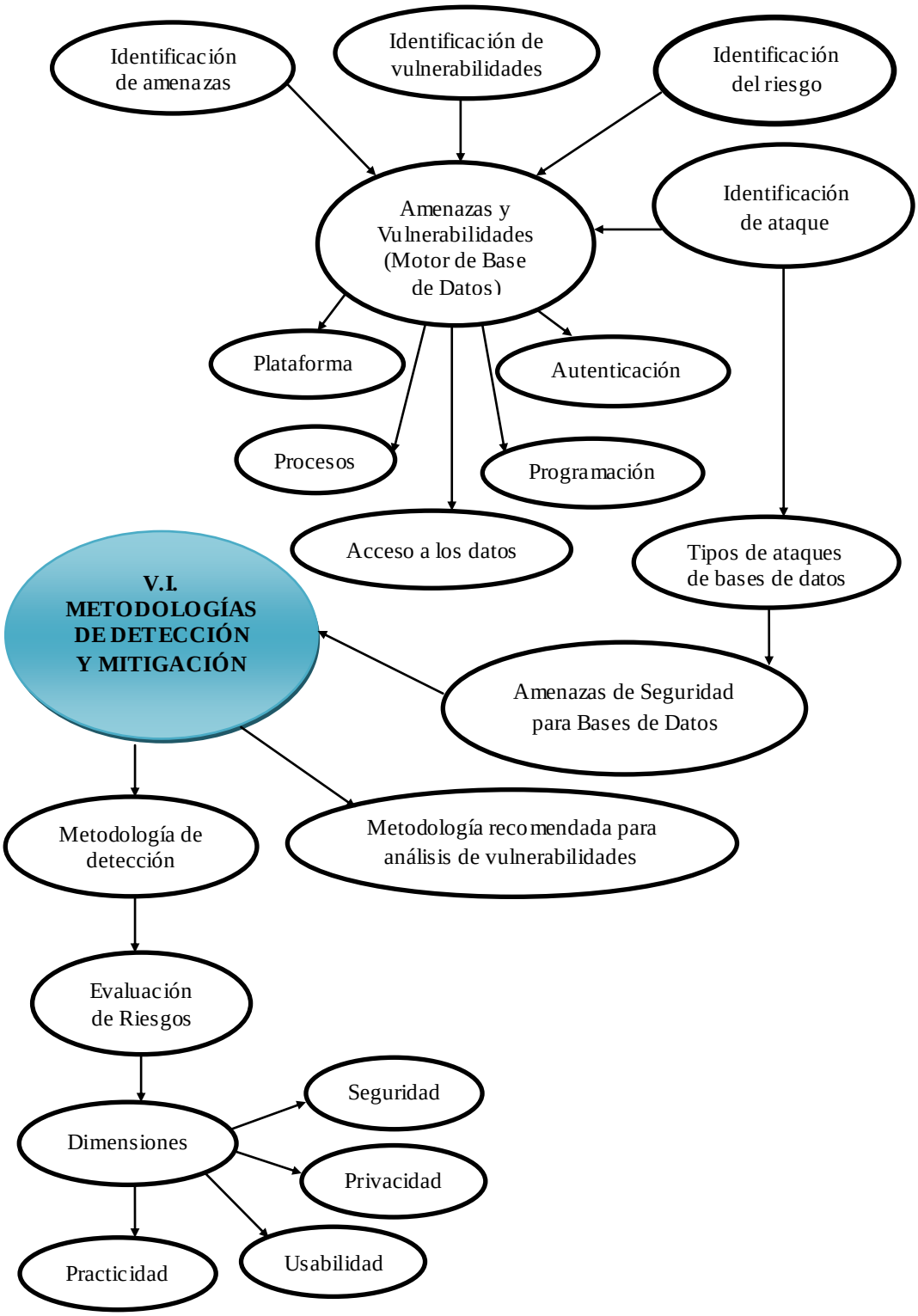


Figura N° 3. Constelación de ideas de la variable independiente

Elaborado por: Investigadora

Constelación de ideas de la variable dependiente

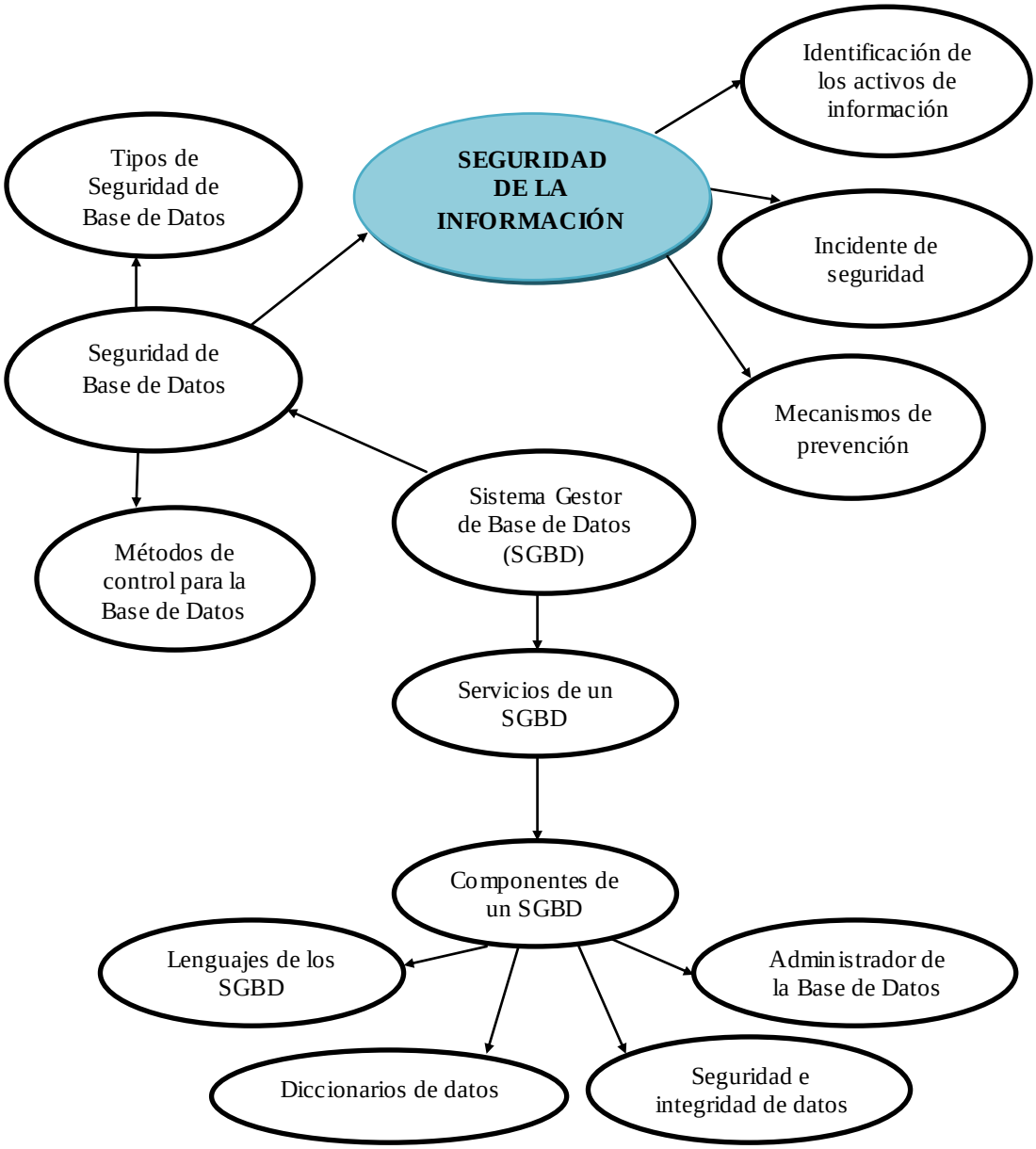


Figura N° 4. Constelación de ideas de la variable dependiente

Elaborado por: Investigadora

2.4.1. Categorías fundamentales de la variable independiente

- **Identificación de amenazas**

Microsoft (2002), en su documentación oficial da a conocer el Modelo de Amenazas STRIDE, en el modelo se pone en consideración las diferentes amenazas a las que pueden estar expuestos los sistemas de información; STRIDE está derivado de un acrónimo de las siguientes seis categorías de amenazas importantes como:

1) La suplantación de identidades, implica el acceso ilegal y el posterior uso de información de autenticación de otro usuario.

2) Una de las amenazas más comunes es la manipulación y/o alteración de los datos que implica la modificación mal intencionada o maliciosa de los datos.

3) Igualmente se destaca la amenaza de repudio que específicamente se asocia a los usuarios que no aceptan o refutan las acciones que realizan, dichas acciones pueden ser operaciones ilegales en un sistema que carece de métodos de rastreo de dichas operaciones; si un sistema tendría la capacidad de contrarrestar amenazas de repudio, se pude decir que se cumple uno de los parámetros de Seguridad de Información conocido como No Repudio.

4) La amenaza de divulgación de información, comprende la exposición de la información a usuarios que no tienen acceso a dicha información, implica también cuando un intruso tiene acceso a los datos que transitan de un punto a otro en la red de comunicaciones.

5) El Modelo de Amenazas describe también como quinto elemento la negación de servicio o Denegación de servicio (DoS), que técnicamente es la no disponibilidad de un servicio a los usuarios del mismo.

6) Finalmente se señala la amenaza de elevación de privilegios, que es cuando un usuario gana accesos privilegiados que nunca le fueron otorgados en el sistema, con lo que el usuario podría comprometer o destruir el sistema. Otras formas de

elevación de privilegios pueden lograr los atacantes una vez que se ha ingresado al sistema violando sus seguridades.

Figura N° 5. Modelo de Amenazas STRIDE - Microsoft

Elaborado por: Investigadora

- **Identificación de vulnerabilidades**

Según **De Freitas (2009: 49)**, describe: "*una vulnerabilidad es un error que representa un problema potencial, es decir, es una condición de debilidad, que le permite a una amenaza producir un daño en la organización*".

Según **Acosta (2013: 32)** describe que las vulnerabilidades son: "*debilidades en los sistemas informáticos y/o de comunicaciones, que pueden estar presentes dentro de procesos u operaciones y que podría ser explotadas por una amenaza, con el propósito de obtener acceso no autorizado a la información o de interrumpir procesos críticos*".

- **Identificación de riesgos**

A continuación, identificaremos según el criterio de varios autores la determinación de riesgo:

Según **Martínez (2010: 62)** determina que riesgo es: *''la posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización*''.

Según los términos de la **ISO27000 (2005)** la descripción de riesgo es la siguiente: "*Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias*".

- **Ataque informático**

Consiste en aprovechar debilidades o fallas en el software y en el hardware e incluso, en las personas que forman parte de un ambiente informático **Mieres, (2009: 4)** manifiesta además que los beneficios de un ataque informático son la obtención de primacías por lo general de índole económico que causan un efecto negativo en la seguridad del sistema y en los activos de la organización.

- **Amenazas y vulnerabilidades (motor base de datos)**

La biblioteca del sitio web oficial de **Microsoft (2016)**, determina una matriz de amenazas y vulnerabilidades (motor de base de datos) para dar a conocer que todos los sistemas pueden tener ciertas características que se podría aprovechar con fines malintencionados y sí existiera cualquier característica que exponga datos u otra información puede constituir un riesgo si se implementa incorrectamente, cabe destacar que no todos los riesgos son iguales, hay riesgos que podría considerar cambios de procedimientos, cambios de configuración/cambios de código. A continuación brevemente se describen algunas amenazas y vulnerabilidades:

AMENAZAS Y VULNERABILIDADES

AMENAZAS Y VULNERABILIDADES DE LOS PROCESOS	
Amenazas / Vulnerabilidades	**Descripción**
Directivas de seguridad	Registro de los procesos y procedimiento que debe seguir una organización para evitar realizar un seguimiento y responder a las amenazas de seguridad. Las directivas pueden estar relacionadas con: el acceso adecuado a los sistemas, la aplicación de revisiones a los firewalls, así como mecanismos de prevención antivirus.
Principio de "privilegios mínimos"	Según el principio de "privilegios mínimos", un sistema sólo debería permitir el nivel de acceso necesario a un objeto protegible. Además, el acceso sólo debería estar habilitado para quienes tienen una necesidad directa y sólo durante un tiempo especificado. Las aplicaciones pueden estar codificadas para proporcionar más acceso del necesario y las cuentas podrían tener demasiados accesos.
Boletines de seguridad	Siempre que se publica información de seguridad tan pronto como se comprueba y se prueba en distintas plataformas. Las organizaciones que no están al corriente de estos boletines ponen en peligro sus sistemas al no implementar las instrucciones de seguridad adecuadas.

AMENAZAS Y VULNERABILIDADES DE LA PLATAFORMA	
Amenazas / Vulnerabilidades	**Descripción**
El sistema no está actualizado (no se han aplicado las actualizaciones de software)	Siempre que se publican actualizaciones de software para mejorar la seguridad de cualquier motor de base de datos. Si no se siguen o se aplican estas actualizaciones de software, el sistema será más vulnerable a los ataques.
Vulnerabilidades de seguridad de los puertos de red	La red es la principal vía de acceso para los ataques contra los motores de base de datos. Si los puertos estándar están abiertos a Internet, se favorecerán los ataques.
Configuración incorrecta de las cuentas de servicio	Las cuentas de servicio del motor de base de datos suelen tener más acceso a la plataforma o a la red del que necesitan.
Área expuesta demasiado grande	Las características y capacidades del motor de base de datos pueden estar expuestas cuando no es necesario.
Procedimientos almacenados innecesarios habilitados	Algunos procedimientos almacenados extendidos permiten el acceso al sistema operativo o al registro.

AMENAZAS Y VULNERABILIDADES DE AUTENTICACIÓN	
Amenazas / Vulnerabilidades	**Descripción**
Contraseñas no seguras	Las contraseñas sencillas están expuestas a los ataques por fuerza bruta o de diccionario.
Cuentas de usuario sin auditar	Los usuarios (entidades de seguridad) a menudo cambian de puesto o dejan la organización. Si no se cambia el acceso a una cuenta de usuario, se puede seguir teniendo acceso al sistema con el nivel de permisos anterior.
AMENAZAS Y VULNERABILIDADES DE PROGRAMACIÓN	
Amenazas / Vulnerabilidades	**Descripción**
Inyección de código SQL	Consiste en incrustar una consulta malintencionada en una legítima.
Contraseñas incrustadas	Algunas aplicaciones guardan las cadenas de conexión en el programa o en archivos de configuración.
AMENAZAS Y VULNERABILIDADES DE ACCESO A LOS DATOS	
Amenazas / Vulnerabilidades	**Descripción**
Cifrado aplicado incorrectamente	El cifrado ofusca los datos o la información de conexión en el motor de base de datos. No cifrar los datos cuando es necesario o hacerlo cuando no lo es, supone un riesgo y una complejidad innecesarios.
Certificados aplicados incorrectamente	Los certificados son un mecanismo para comprobar la autenticación. El sistema de base de datos puede utilizar los certificados para diversos propósitos, desde las conexiones a los datos. El uso inadecuado de los certificados autofirmados y los períodos de validación extendidos reducen la eficacia de la seguridad global.
Claves de sistema de base de datos sin copias de seguridad	Una instancia del motor de base de datos y las bases de datos que contienen, puede tener claves que se utilizan para distintos propósitos de seguridad. Esto incluye el cifrado.

Tabla N° 1. Amenazas y vulnerabilidades (motor de base de datos)

Elaborado por: Investigadora

- **Tipos de ataques de bases de datos**

Juntamay y Macas (2011: 52), define el tipo de ataques relacionados con base de datos, donde se puede distinguir dos grupos, los ataques qué *No Requieren Autenticación,* que generalmente requieren de la presentación de credenciales válidas antes de lanzar el ataque como ocurre con la explotación de Buffer Overflow y los *Ataques que Requieren Autenticación,* que deben ser lanzados por los poseedores de credenciales, para lo que se intenta obtener un nombre de usuario y contraseña válidos en el sistema objetivo mediante técnicas tales como la adivinación y los ataques de fuerza bruta o diccionario donde el usuario posee acceso al sistema objetivo y cuenta con muchas más oportunidades al momento de lanzar un ataque.

- **Amenazas de seguridad para bases de datos**

Los autores **Rohilla y Kumar (2013: 811)** citaron varias amenazas de seguridad, que van desde los aspectos internos como una mala administración de una base de datos hasta los aspectos externos como los que se describen a continuación:

AMENAZAS DE SEGURIDAD PARA BASES DE DATOS	
AMENAZAS	**DESCRIPCIÓN DE AMENAZAS**
Abuso de exceso de privilegios	Cuando los usuarios de la base de datos o las aplicaciones, se otorgan privilegios de acceso que exceden los requerimientos de su función de trabajo u objetivo, que pueden ser objeto de abuso con fines maliciosos.
Abuso legítimo de privilegios	Abuso de privilegios de base de datos legítimos para fines no autorizados, por parte de usuarios de bases de datos, administradores o un administrador de sistema que podría realizar cualquier actividad ilegal o poco ético.
Elevación de privilegios	Las vulnerabilidades en el software de base de datos y los atacantes muchas veces pueden convertir sus privilegios de acceso de un usuario normal a las de un administrador.
Plataforma de vulnerabilidades	Las vulnerabilidades en los sistemas operativos y servicios adicionales instalados en el servidor de base de datos pueden dar lugar a un acceso no autorizado, la corrupción de datos o de denegación de servicio.

Inferencia	Incluso en las DBMS (Data Base Management System) seguras, es posible que los usuarios diseñen inferencias a partir de la información que obtienen de la base de datos, cuando el usuario puede adivinar o concluir la información más sensible de la información recuperada de la base de datos o con algún conocimiento previo.
SQL Injection	En un ataque donde un atacante que inserta (o "inyecta") sentencias SQL no autorizadas en un canal de datos SQL vulnerable que pueden incluir procedimientos almacenados y los parámetros de entrada de la aplicación Web que se pasan a la base de datos donde se ejecutan.
DBMS (Data Base Management System) sin parches	Los proveedores de base de datos liberan parches, de modo que la información sensible permanecerá protegida contra amenazas, cuando se deja sin parchear, los hackers pueden alterar el diseño del parche, o con frecuencia pueden explotar las vulnerabilidades sin parches, dejando un DBMS aún más vulnerables que antes que fue lanzado el parche.
Características innecesarias activadas de la DBMS	En un DBMS (Data Base Management System) puede haber características innecesarias, que están habilitadas predeterminadamente y que se debe deshabilitar para evitar ataques efectivos en una base de datos.
Configuraciones erróneas	Los errores de configuración de bases de datos proporcionan puntos de acceso débiles para los hackers para eludir los métodos de autenticación y obtener acceso a información sensible.
Desbordamiento de Búfer	Cuando un programa o proceso intenta almacenar más datos en una memoria intermedia de lo que estaba previsto ocurre un desbordamiento de búfer.
Registros de auditoría débiles	Una directiva de auditoría de base de datos asegura la grabación automática, oportuna y adecuada de las transacciones de bases de datos, la ausencia de esta directiva plantea un grave riesgo para las bases de datos y pueden causar inestabilidad en las operaciones.
Denegación de servicio	En este tipo de ataque a todos los usuarios (incluidos los usuarios legítimos) se les niega el acceso a los datos en la base de datos. La Denegación de Servicio (DOS) se puede crear a través de muchas técnicas.
Canal secreto	Un canal secreto es un medio indirecto de comunicación en un sistema de ordenador que pueden utilizarse para debilitar la política de seguridad del sistema. Un programa que se ejecuta en un nivel secreto se impide escribir directamente al elemento de datos no clasificados.
Protocolo de comunicación de vulnerabilidades	Un gran número de fallos de seguridad se identifica en los protocolos de comunicación de base de datos de todos los distribuidores de bases de datos. Las actividades fraudulentas que dirigen estas vulnerabilidades pueden variar de acceso a los datos a la explotación ilegal de los datos y la denegación de servicio

	y más.
Amenazas avanzadas persistentes	Este tipo de amenazas ocurre cuando organizaciones grandes y bien financiadas hacen asaltos altamente enfocados a las grandes tiendas de los datos críticos. Estos ataques son implacables, definidos y perpetrados por grupos calificados, motivados, organizados y bien financiados.
Errores ejecutivos	Algunos ataques no son intencionales, que puede ser llamado "*ataque de usuario autorizado no intencional*" o error privilegiado. Cuando un usuario autorizado inadvertidamente accede a los datos sensibles y modifica o elimina la información por error o accidentalmente.
Ingeniería social	En este tipo de amenaza, los usuarios proporcionan sin saberlo información a un atacante a través de una interfaz o sitio web comprometido a través de un correo electrónico de respuesta que parece ser una solicitud legítima.
Autenticación débil	Los esquemas de autenticación débiles permiten a los atacantes asumir la identidad de los usuarios de bases de datos legítimos por el robo u otras formas de obtención de las credenciales de inicio de sesión.
Copia de seguridad de la exposición de datos	Los medios de almacenamiento de copia de seguridad de base de datos están a menudo completamente sin protección de un ataque, así como un desastre natural como: inundaciones, terremotos, entre otros. Como resultado, varios fallos de seguridad de alto perfil han supuesto robo de bases de datos cintas de respaldo y discos duros.

Tabla N° 2. Amenazas de Seguridad para Bases de Datos

Elaborado por: Investigadora

- **Metodologías de detección**

Herzog, (2003: 11) describe en el ámbito de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1., una metodología de testeo de seguridad para la detección de amenazas y vulnerabilidades que contempla un conjunto de reglas y lineamientos para despejar las incógnitas de CUÁNDO, QUÉ Y CUÁLES eventos son testeados. El autor desarrolla la metodología OSSTMM solo para realizar testeos externos que comprende realizar la detección de vulnerabilidades sin contar con privilegios y evadir así los componentes de seguridad, algunos procesos y alarmas para ganar acceso privilegiado.

Además de proveer un método estandarizado para realizar un exhaustivo test de seguridad de cada sección con presencia en algunos ámbitos como: seguridad física, seguridad inalámbrica, seguridad de comunicaciones, seguridad de la información, seguridad de las tecnologías de internet y seguridad de procesos de una organización. El método es abierto y evaluado por expertos para realizar exhaustivos testeos de seguridad, alcanza estándares internacionales que representa una línea base para muchas más metodologías de testeos de seguridad conocidas y exploradas.

El testeo de seguridad externo tiene una limitación debido a las grandes diferencias que existe entre el testeo externo a interno y el testeo interno a interno, dichas diferencias radican fundamentalmente en los privilegios de acceso, los objetivos que tiene cada una y los resultados asociados con el testeo interno a interno.

El alcance de la metodología de detección y mitigación, así como de un test de seguridad OSSTMM (Open Source Security Testing Methodology Manual – Manual de Metodología de Testeo de Seguridad de Código Abierto), no contempla el tipo de testeo que busca descubrir las vulnerabilidades inexploradas, al contrario, es un test práctico y eficiente de vulnerabilidades conocidas, filtraciones de información, infracciones de la ley, estándares de la industria y prácticas recomendadas.

- **Evaluación de Riesgo**

Antes de abordar este tema, se debe entender brevemente lo que significa el concepto riesgo y todo lo que implica en ámbitos de Seguridad de Información, según **Herzog (2003: 26)**, el riesgo significa que, "*los límites de la presencia de seguridad tendrán un efecto perjudicial en la gente, la cultura de información, los procesos, negocios, imagen, propiedad intelectual, derechos legales o capital intelectual*". **Herzog (2003: 26)** también menciona en su manual cuatro dimensiones en el proceso de análisis y disminuir cualquier riesgo en el ambiente, los mismos que se pueden observar en la siguiente figura:

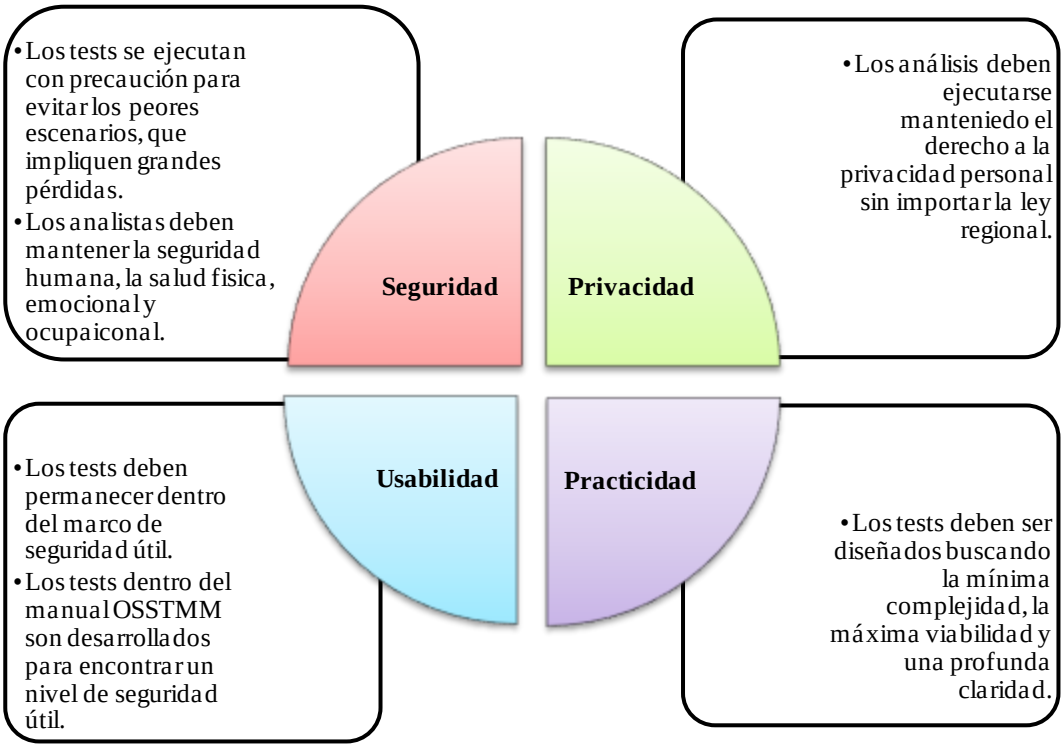


Figura N° 6. Dimensiones en el proceso de análisis

Elaborado por: Investigadora

- **Metodología recomendada para análisis de vulnerabilidades**

La empresa Sisteseg líder en servicios de seguridad de la información (SGSI), planes para continuidad del negocio y auditorias sobre infraestructuras en el mercado, con más de 10 años de experiencia. **Sisteseg (s.f.)** genera algunas recomendaciones generales que se relacionan con el análisis de vulnerabilidades, con el fin de identificar los riesgos a los que están sometidos los activos de TI, dichas recomendaciones mejoran la seguridad de la información.

Una vulnerabilidad, se puede definir como un estado de un sistema (o conjunto de sistemas) que puede:

- Permitir a un atacante acceder a información confidencial
- Permitir a un atacante modificar información
- Permitir a un atacante negar un servicio

Ante la evidencia de vulnerabilidades se necesita contar con una estrategia coherente y efectiva para mitigar estas inquietantes y críticas amenazas de tal manera que a continuación se presentan una serie de actividades y recomendaciones que ayudan a las empresas a realizar un análisis a nivel técnico de las vulnerabilidades de software.

- **Metodología para el análisis de vulnerabilidades**

El análisis de vulnerabilidades que se complementa con el análisis de riesgos, es una actividad principal que se debe realizar para orientar hacia un sistema de gestión de seguridad, para lo que se plantea la realización de las siguientes actividades:

a) Entendimiento de la infraestructura: Esta etapa comprende buscar e identificar cada uno de los componentes de hardware o software que soportan los procesos del negocio. Esta búsqueda e identificación inicia por el análisis de los servicios tecnológicos que la empresa brinda y que procesos se asocian a los mismos.

b) Pruebas: Por medio del uso de herramientas para la detección de vulnerabilidades, además de contar con una base de datos de vulnerabilidades completa y actualizada la misma que sea aceptada por la industria (CERT, SANS, CVE) y que permite determinar el tipo de vulnerabilidad, la severidad, los posibles riesgos e impactos así como las posibles recomendaciones.
Para la realización de las pruebas como tal se debe tomar una decisión costo – beneficio, con el fin determinar el alcance del análisis y las pruebas a realizar.

c) Medidas preventivas: Es tomar las debidas precauciones con el fin de evitar efectos adversos que puedan afectar la disponibilidad de los servicios que brinda la empresa, para lo que se recomienda establecer una hora pertinente para la ejecución de las pruebas; informar a las áreas pertinentes y a los custodios de los activos involucrados sobre la realización de las pruebas; realizar un análisis de riesgos cualitativos sobre la prueba que permita estimar la probabilidad y el impacto; tomar algunas medidas de contingencia como la realización de los debidos respaldos de información de los activos involucrados; además realizar el monitoreo de los servicios durante el proceso de pruebas y el tráfico de la red de comunicaciones.

d) Realización de las pruebas de vulnerabilidades: Es importante evaluar la cantidad de activos a analizar para estimar el tiempo de la prueba y considerar cuando se tiene activos con protecciones de herramientas de seguridad como firewalls, ya que estos dispositivos deben permitir pasar el tráfico generado por la herramienta de análisis de vulnerabilidades.

Existen pruebas que se pueden realizar con el suministro de información para la ejecución o se pueden realizar sin que se necesite dicho suministro de información, como se detalla a continuación pueden existir dos tipos de pruebas:

1. Internas
    a. Sin conocimiento
    b. Con conocimiento
2. Externas
    a. Sin conocimiento
    b. Con conocimiento

e) Pruebas de explotación de vulnerabilidades: Una vez clasificadas las vulnerabilidades más críticas, se debe realizar una prueba sobre ellas con el fin de realizar su explotación. En la medida en que la herramienta sea más inteligente y estructurada el proceso será más corto y no requerirá un perfil tan sofisticado. El proceso de explotación debe incluir el escalar privilegios (tomar control del dispositivo como administrador) con el fin de tomar control total de los sistemas y seguir de manera estricta la forma en que se llevan a cabo los ataques en la vida real.

f) Análisis de resultados: Con base en la información obtenida realizar una reunión técnica para informar de estos resultados y realizar una revisión general de las vulnerabilidades encontradas y la clasificación realizada por la herramienta. En esta reunión deben participar:

1. Oficial de seguridad
2. Dueños de procesos
3. Gerente del área
4. Comité de seguridad

5. Dueños de activos
6. Coordinador del plan de contingencias

g) Plan de remediación de vulnerabilidades: Una vez hecho un análisis formal y detallado de los resultados obtenidos tanto de la prueba de vulnerabilidades como de las de explotación, finalmente se debe proponer un plan de remediación o mitigación específico para las vulnerabilidades, el cual puede ser parte del plan de tratamiento general de riesgos. Este plan de remediación, clasifica con ayuda de la herramienta de vulnerabilidades y de explotación, la criticidad de cada una de las vulnerabilidades encontradas y sugiere cuales deben ser solucionadas en el corto, mediano o largo plazo. Esta decisión sobre el tiempo a implantar el control respectivo a la vulnerabilidad también debe contemplar costo del control, capacidad, administración y facilidad de implementación.

2.4.2. Categorías fundamentales de la variable dependiente

- **Seguridad de la Información**

Según **Flores, (2009: 11)** resume en la *Figura N° 7. Objetivos de la seguridad de la información*, donde se puede identificar que los principales objetivos son las características de confidencialidad, integridad y disponibilidad, se puede observar que cada uno de los objetivos permite implementar controles y detectar amenazas.

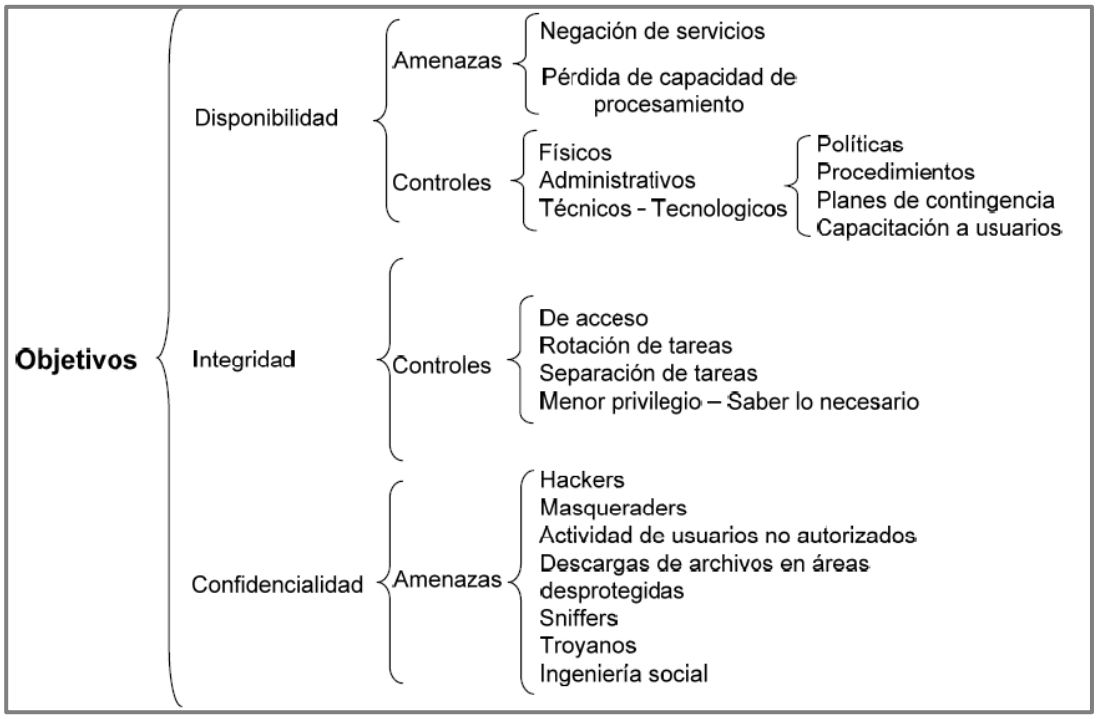


Figura N° 7. Objetivos de la seguridad de la información

Elaborado por: Flores, 2009

- **Identificación de activos de información**

Según **Gutiérres Camilo (2012)**, la identificación de activos de información está comprendida por "*todos aquellos recursos involucrados en la gestión de la información, que va desde datos y hardware hasta documentos escritos y el recurso humano*". Como se puede apreciar podría existir una diversidad de recursos que se involucren en las actividades y procesos diarios de las empresas.

Según los términos manejados por la **ISO27000 (2005)**. Se identifican ocho (8) activos de información vitales, entre los que se encuentran:

- Activos de información (datos, de manuales de usuario, entre otros)
- Documentos en papel (contratos)
- Activos de software (aplicación, software de sistemas, entre otros)
- Activos físicos (computadoras, servidores, medios magnéticos, enrutadores, entre otros)

- Personal (estudiantes, clientes, empleados, entre otros)
- Imagen de la compañía y reputación
- Servicios (comunicaciones, entre otros)

- **Incidente de seguridad**

Acurio (2009: 20), determina que "*un incidente de seguridad informática puede considerarse como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos*".

- **Mecanismos de prevención**

Con respeto a la mitigación de vulnerabilidades de un sistema informático como tal, podemos considerar varios mecanismos de prevención como los que hace referencia el **Ministerio de Educación, Cultura y Deporte del Gobierno de España (s.f.)**, contemplado en sus conceptos y fundamentos de seguridad informática se representan en la siguiente figura los mecanismos de prevención:

Figura N° 8. Mecanismos de Prevención

Elaborado por: Investigadora

- **Seguridad de Base de Datos**

Según **Villalobos (2012),** describe los principios básicos y siete (7) recomendaciones o actividades de seguridad en base de datos:

1) Identificar la sensibilidad. - Para lograr identificar la sensibilidad o riesgos de una base de datos, se debe empezar por realizar un catálogo de tablas o datos sensibles de sus instancias de base de datos, el proceso de identificación debe automatizarse, en caso de existir cambios en los datos y su ubicación. Se puede desarrollar o adquirir herramientas para identificación; asegurando éstas contra el malware, colocado en la base de datos el resultado de los ataques de inyección SQL, pues aparte de exponer información confidencial a vulnerabilidades, como la inyección SQL, también facilita a los atacantes incorporar otros ataques en el interior de la base de datos.

2) Evaluación de la vulnerabilidad y la configuración. - La evaluación de la configuración de la base de datos se realiza para confirmar que no se tiene huecos de seguridad, la evaluación implica la verificación del proceso de instalación y el sistema operativo, además se debe comprobar los privilegios de grupos de los archivos lectura, escritura y ejecución de la base de datos y las bitácoras de transacciones.

Los archivos con parámetros de configuración y programas ejecutables deben ser verificados, así como la versión de la base de datos, ya que cuando se trabaja con versiones inferiores a las versiones estables conocidas, estas pueden ser vulnerables, también se deber restringir que las aplicaciones o capa de usuario ejecuten consultas SQL.

El administrador de la base de datos debe limitar el acceso a los procedimientos de ciertos usuarios, delimitar los accesos de los datos por parte de los usuarios, procedimientos y/o datos y declinar las coincidencias de horarios entre usuarios que coincidan.

3) Endurecimiento. - El endurecimiento y/o fortalecimiento de seguridad regularmente se pueden establecer luego de una evaluación de vulnerabilidades que determinan las respectivas recomendaciones específicas, otros elementos de fortalecimiento involucra la eliminación y/o desactivación de todas las funciones, configuraciones y opciones que no se consideren necesarias. Además, se puede aplicar políticas que determinen lo que está permitido o no.

4) Auditoría. - Después de creada una configuración y controles de endurecimiento/fortalecimiento, se debe realizar auto evaluaciones y seguimiento a las recomendaciones de auditoría para lograr el mejoramiento de la seguridad. Es necesario automatizar el control de la configuración para registrar los cambios en la misma, además se debe implementar alertas para conocer cuando se realizan cambios a la configuración, ya que cada vez que se realizan cambios puede afectar a la seguridad de la base de datos.

5) Monitoreo. - El monitoreo en tiempo real de la base de datos es fundamental para tener el control de la seguridad y limitar su exposición, se puede aplicar o adquirir agentes inteligentes de monitoreo, detección de intrusiones y/o uso indebido.

El monitoreo puede emitir alertas sobre patrones inusuales de acceso, presencia de ataques de inyección SQL, cambios no autorizados a los datos, cambios de privilegios en las cuentas, cambios de configuraciones que se pueden ejecutar a través de comandos SQL, entre otros.

Un requisito para la gobernabilidad de datos y cumplimiento de regulaciones como SOX y regulaciones de privacidad, es el monitoreo a usuarios privilegiados que ayuda a detectar intrusiones o posibles ataques realizados con privilegios de usuario de alto nivel.

El monitoreo dinámico es también un elemento esencial de la evaluación de vulnerabilidades, que permite ir más allá de evaluaciones estáticas o forenses para casos como el de múltiples usuarios que comparten credenciales con privilegios o un número excesivo de inicios de sesión de base de datos.

6) Pistas de auditoría. - Un requisito de auditoría y de gran importancia para las investigaciones forenses es la aplicación de pistas de auditoría y la generación de trazabilidad de las actividades que afectan la integridad de los datos o la visualización de los datos sensibles.

7) Autenticación, control de acceso y gestión de derechos. - Es importante autenticar a los usuarios, garantizar la rendición de cuentas por usuario y administrar los privilegios de limitar el acceso a los datos, para lo que se debe implementar y revisar periódicamente los informes sobre de derechos de usuarios, como parte de un proceso de formal de auditoría.

El uso de cifrado para hacer ilegibles los datos confidenciales, complica el trabajo a los atacantes, esto incluye el cifrado de los datos en tránsito, de modo que un atacante no puede escuchar en la capa de red y tener acceso a los datos cuando se envía al cliente de base de datos.

- **Métodos de control para la Base de Datos**

Para profundizar un poco el presente proyecto dentro de los mecanismos o metodologías de mitigación de vulnerabilidades podemos citar los métodos de control de amenazas para las bases de datos, **Malik y Patel (s.f.: 6)** mencionan en su investigación que para eliminar las amenazas a la seguridad de cada organización, tiene que constar una o varias políticas de seguridad que deberían aplicarse en la organización con seguridad y efectividad. Por citar así una de las políticas más importantes es la política de seguridad de autenticación, ya que con una correcta autenticación se disminuiría las probabilidades de amenazas. Otra forma seria tener mecanismos de control de acceso a la base de datos, para controlar los diferentes usuarios tienen derechos de acceso a los objetos de la base de datos.

Los mecanismos de control de acceso se ocupan de la gestión de los derechos de acceso. Según Malik y Patel ésta es la técnica básica para proteger los objetos de datos en las bases de datos y es apoyado por la mayor parte del DBMS. En la *Figura*

N° 10 Métodos de control para la base de datos, se muestra la visión general de los métodos de control utilizado para la seguridad de la base de datos.

Figura N° 9. Métodos de control para la base de datos

Elaborado por: Malik y Patel (s.f.)

- **Tipos de Seguridad en Base de Datos**

Los tipos de seguridad **Juntamay y Macas (2011: 50)**, los describe en dos de mecanismos de seguridad existentes en las bases de datos; los *mecanismos de seguridad discrecionales* que se utilizan para otorgar privilegios es un modo determinado a los usuarios para tener acceso a archivos, registros o campos de datos y los *mecanismos de seguridad obligatorios* que sirven para imponer igualdad de múltiples niveles, catalogando los datos y los usuarios en varias clases (o niveles) de seguridad e implementando después la política de seguridad apropiada para la organización.

- **Sistema Gestor de Base de Datos**

Se cita a continuación varios conceptos sobre un Sistema Gestor de Base de Datos o en inglés Database Management System (DBMS).

Para **Álvarez (2007)**, un Sistema Gestor de Base de Datos, se describe como un conjunto de programas que administran y gestionan la información contenida en una base de datos. Un sistema gestor permite definir y realizar el mantenimiento de la integridad de los datos contenidos; además de controlar la seguridad, la privacidad y la manipulación de los mismos.

El portal web **EcuRed (2016),** publica un artículo donde se determina el concepto de un Sistema Gestor de Base de Datos, como un sistema de software que permite la definición de bases de datos, entiéndase como parte de esto la elección de las estructuras de datos necesarios para el almacenamiento y búsqueda de los mismos, ya sea de forma interactiva o a través de un lenguaje de programación. Un SGBD trabaja de forma relacional, es un modelo de datos que facilita a los usuarios las actividades para describir los datos que serán almacenados en la base de datos para que luego estos puedan ser manipulados con un grupo de operaciones.

- **Servicios de un SGBD**

El portal web **Mc Graw Hill Education (2015)**, describe que el SBGD es una aplicación que permite a los usuarios definir, crear y mantener la base de datos y proporciona un acceso controlado a la misma y debe prestar los siguientes servicios:

SERVICIOS DE UN SGBD

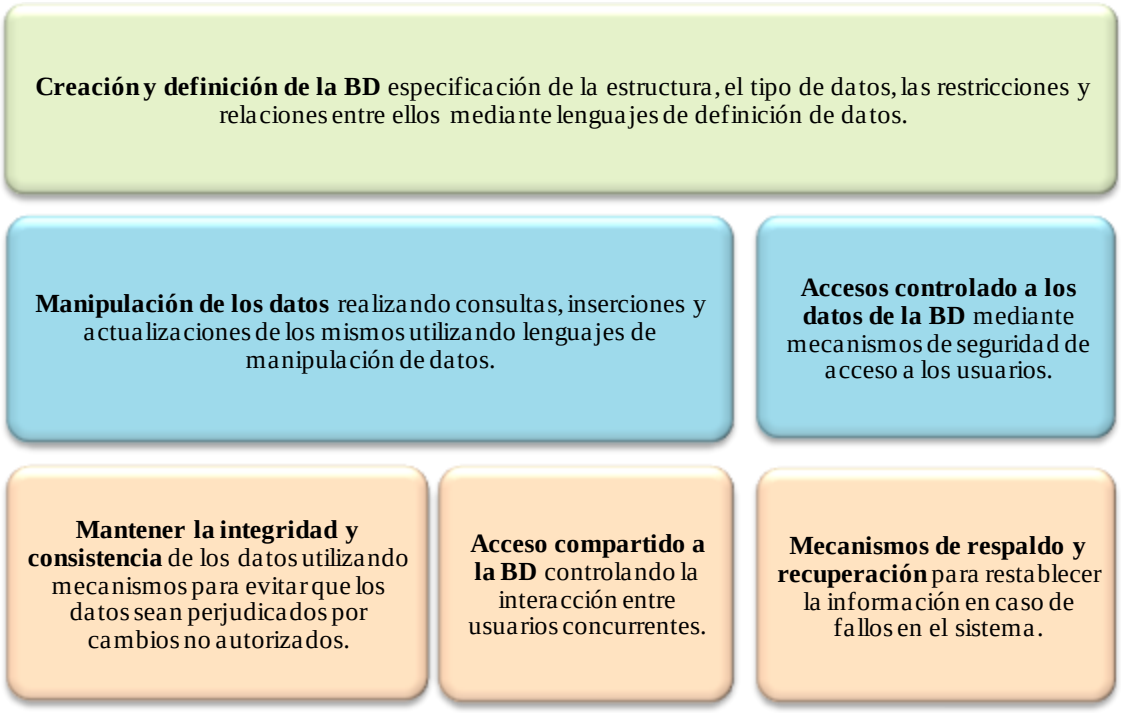


Figura N° 10. Servicios de un SGBD

Elaborado por: Investigadora

- **Componentes de los SGBD**

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. La documentación del portal web **Mc Graw Hill Education (2015)**, determina que los Sistemas Gestores de Base de Datos contienen los siguientes componentes principales:

A. Lenguajes de los SGBD

Todos los SGBD ofrecen lenguajes e interfaces apropiadas para cada tipo de usuarios: administradores, diseñadores, programadores de aplicaciones y usuarios finales. Además permiten al administrador de la base de datos realizar especificaciones de los datos que componen la base de datos, determinar la estructura, las relaciones que existen entre ellos, las reglas de integridad, los

controles, las características de tipo físico y las vistas externas de los usuarios. Los lenguajes del SGBD se clasifican en:

- **Lenguaje de definición de datos (LDD o DDL):** se utiliza para especificar el esquema de la base de datos, las vistas de los usuarios y las estructuras de almacenamiento.
- **Lenguaje de manipulación de datos (LMD o DML):** se utilizan para leer y actualizar los datos de la base de datos. Es el utilizado por los usuarios para realizar consultas, inserciones, eliminaciones y modificaciones.
- **Lenguajes de cuarta generación (4GL):** que permiten al usuario desarrollar aplicaciones de forma fácil y rápida, también se les llama *herramientas de desarrollo.*

B. Diccionario de datos

Se describe a este componente como el lugar donde se deposita información acerca de todos los datos que forman la base de datos, en sí es una guía en la que se describe la base de datos y los objetos que la forman.

El diccionario contiene las características lógicas de los sitios donde se almacenan los datos del sistema incluyendo nombre, descripción, alias, contenido y organización. Identifica los procesos donde se emplean los datos y los sitios donde se necesita el acceso inmediato a la información.

C. Seguridad e integridad de datos

Un SGBD proporciona los siguientes mecanismos para garantizar la seguridad e integridad de los datos:

- ✓ Le corresponde garantizar la protección de los datos contra accesos no autorizados, tanto intencionados como accidentales. Además de controlar que sólo los usuarios autorizados accedan a la base de datos.

- ✓ Los SGBD ofrecen mecanismos para implantar restricciones de integridad en la base de datos las mismas que van a proteger la base de datos contra daños

accidentales. Los valores de los datos que se almacenan deben satisfacer ciertos tipos de restricciones de consistencia y reglas de integridad, que especificará el administrador de la base de datos. El SGBD tiene la capacidad para determinar si se produce una violación de la restricción.

- ✓ Proporciona herramientas y mecanismos para la planificación y realización de copias de seguridad y restauración.

- ✓ El SGBD debe ser capaz de recuperar la base de datos llevándola a un estado consistente en caso de ocurrir algún suceso que la dañe.

- ✓ Debe asegurar el acceso concurrente y ofrecer mecanismos para conservar la consistencia de los datos en el caso de que varios usuarios actualicen la base de datos de forma concurrente.

D. Administrador de la base de datos

El DBA tiene una gran responsabilidad ya que posee el máximo nivel de privilegios y es el encargado de crear los usuarios que se conectarán a la base de datos. En la administración de una base de datos siempre hay que procurar que haya el menor número de administradores, de ser posible una sola persona.

En los sistemas de gestión de base de datos existen diferentes categorías de usuarios que se caracterizan porque cada una de ellas tiene una serie de privilegios o permisos sobre los objetos que forman la base de datos.

En los sistemas como por ejemplo Oracle las categorías más importantes son:

- **Los usuarios de la categoría DBA** (*Database Administrator*), cuya función es precisamente administrar la base y que tienen el nivel más alto de privilegios.
- **Los usuarios de la categoría RESOURCE,** que pueden crear sus propios objetos y tienen acceso a los objetos para los que se les ha concedido permiso.
- **Los usuarios del tipo CONNECT,** que solamente pueden utilizar aquellos objetos para los que se les ha concedido permiso de acceso.

2.5. Hipótesis

La elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos incide en la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

2.6. Señalamiento de variables

- **Variable Independiente:** Metodología de detección y mitigación de vulnerabilidades de base de datos.

- **Variable Dependiente:** Seguridad de la Información de la empresa Automekano Cía. Ltda.

CAPÍTULO III

METODOLOGÍA

3.1. Modalidad básica de la investigación

- ***Predominante cualitativo***, en el presente trabajo de investigación se tiene una realidad única e irrepetible en el marco de estudio de la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato, además está orientado a la formación de hipótesis y asume una realidad dinámica.

- ***Predominante cuantitativo***, el presente trabajo de investigación permitirá la búsqueda de las causas de los hechos que estudia, con una perspectiva desde afuera, que se orienta a la comprobación y dará énfasis en el resultado final.

- ***Investigación de campo***, debido a que se realizará para recabar la información necesaria que permitirá la elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

- ***Investigación Bibliográfica - Documental***, ya que se utilizará para el análisis e investigación los aportes de libros, trabajos de investigación, revistas, publicaciones, documentos oficiales, leyes, entre otros (documentación física y electrónica). Fuentes de investigación de carácter primarias debido a su importancia, aporte investigativo efectivo y validez legal.

3.2. Nivel o tipo de investigación

- **Exploratorio,** la presente investigación generará hipótesis y reconocerá las variables de interés investigativo a nivel de la elaboración de la metodología de detección y mitigación de vulnerabilidades de base de datos y se explorará un problema desconocido en el contexto particular de la empresa Automekano Cía. Ltda.

- **Descriptivo,** debido a que será posible realizar una detección de vulnerabilidades de base de datos de la empresa y será factible establecer y documentar recomendaciones para la mitigación de las vulnerabilidades de base de datos, además se podrá documentar la metodología que permitirá detectar y mitigar vulnerabilidades de base de datos para la seguridad de la información de la empresa Automekano Cía. Ltda.

- **Asociación de variables,** porque buscará medir el grado de relación entre la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos y la incidencia en la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

- **Explicativo,** ya que se encargará de buscar el porqué de los hechos mediante los establecimientos de relaciones causa-efecto. En este sentido, la investigación podría ocuparse tanto de la determinación de las causas de la ausencia de una metodología para la detección y mitigación de vulnerabilidades y la inseguridad de la base de datos de la empresa; así como los efectos que podrían ser incremento de vulnerabilidades en la base de datos, posibles riesgos de información almacenada y el aumento de las brechas de seguridad de información en la empresa Automekano Cía. Ltda.

- **Correlacional,** ya que busca la relación entre la variable independiente que es la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos y la incidencia sobre la variable dependiente que es la Seguridad de la Información de la empresa Automekano Cía. Ltda.

3.3. Población y muestra

La población considerada será el Jefe de Sistemas y el personal que realiza diferentes actividades en el Departamento de Sistemas de la empresa Automekano Cía. Ltda., de la ciudad de Ambato y sus sucursales en la ciudad de Quito y Guayaquil; población que está conformado por un total de siete (7) personas.

DESCRIPCIÓN	POBLACIÓN	PORCENTAJE (%)
Jefe de Sistemas (Administrador de la Base de Datos)	1	14%
Analistas de Sistemas (Ambato)	4	57%
Analista de Sistemas (Quito)	1	14%
Analista de Sistemas (Guayaquil)	1	14%
TOTAL	**7**	**100%**

Tabla N° 3. Descripción de la población

Elaborado por: Investigadora

3.4. Operacionalización de variables

- **Variable Independiente:** Metodología de detección y mitigación de vulnerabilidades de base de datos.

CONCEPTO	DIMENSIONES	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS
Metodología de detección y mitigación Metodología de testeo de seguridad.	Amenazas y Vulnerabilidades (motor de Base de Datos)	- Procesos - Plataforma - Autenticación - Programación - Acceso a los datos	¿Con que tiempo se realiza un análisis de seguridad de base de datos en busca de vulnerabilidades?	Entrevista a través de un cuestionario aplicado al Departamento de Sistemas de la empresa.
Es un conjunto de reglas y lineamientos que permite saber CUÁNDO, QUÉ y CUÁLES eventos serán testeados.	Metodologías recomendadas para análisis y mitigación de vulnerabilidades	- Entendimiento de la infraestructura - Pruebas - Medidas preventivas - Realización de las pruebas - Pruebas de explotación - Análisis de resultados - Plan de remediación	¿Han existido ataques hacia el servidor de la base de datos de la empresa? ¿Se realizan acciones para la detección y mitigación de vulnerabilidades en base de datos?	Entrevista a través de un cuestionario aplicado al Departamento de Sistemas de la empresa.

Tabla N° 4. Operacionalización de variable independiente

Elaborado por: Investigadora

- **Variable Dependiente:** Seguridad de la información de la empresa Automekano Cía. Ltda.

CONCEPTO	DIMENSIONES	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS
Seguridad de la información se define como: La protección de la información y los sistemas que soportan para evitar el acceso no autorizado, uso, divulgación, alteración, modificación o destrucción, con el fin de proporcionar: Confidencialidad, Integridad y Autenticidad, objetivos que permiten implementar controles, y detectar amenazas.	Seguridad de la base de datos Sistema Gestor de Base de Datos. Componentes de un SGBD	- Identificar sensibilidad - Evaluación de vulnerabilidades y la configuración - Endurecimiento - Auditoria - Monitoreo - Pistas de auditoria - Autenticación, control de acceso y gestión de derechos. - Lenguajes - Diccionario de Datos - Seguridad e integridad de datos - Administrador de base de datos	¿Cuál es el nivel de importancia de la información de la base de datos que maneja la empresa? ¿Qué nivel se seguridad tiene el servidor de la base de datos de la empresa? ¿Qué software de seguridad se encuentran instalados en la empresa? ¿Qué usuarios pueden acceder al a información confidencial de la base de datos de la empresa?	Entrevista a través de un cuestionario aplicado al Departamento de Sistemas de la empresa. Entrevista a través de un cuestionario aplicado al Departamento de Sistemas de la empresa.

Tabla N° 5. Operacionalización de variable dependiente

Elaborado por: Investigadora

3.5. Plan de recolección de información

En el presente proyecto se ha planteado entrevistas a través de cuestionarios aplicados al Jefe de Sistemas y al personal que realiza diferentes actividades en el Departamento de Sistemas de la empresa Automekano Cía. Ltda., para concretar la obtención de información se han debido contestar las siguientes preguntas:

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Para qué?	Para recolectar información primaria para comprobar la hipótesis.
¿A qué personas u sujetos?	Al Jefe de Sistemas y al personal que realiza diferentes actividades en el Departamento de Sistemas de la empresa Automekano Cía. Ltda.
¿Sobre qué aspectos?	**V.I.** Metodología de detección y mitigación de vulnerabilidades de base de datos. **V.D.** Seguridad de la información de la empresa Automekano Cía. Ltda.
¿Quién? ¿Quiénes?	La investigadora Carolina Anabel Bonilla Vaca
¿A quiénes?	Al Jefe de Sistemas y a los Analistas de Sistemas de la empresa Automekano Cía. Ltda.
¿Cuándo?	Segundo cuatrimestre del 2016, de acuerdo al cronograma establecido.
¿Dónde?	Empresa Automekano Cía. Ltda., de la ciudad de Ambato.
¿Cuántas veces?	Una vez para la obtención de la información de la investigación.
¿Qué técnicas de recolección?	Encuesta
¿Con que?	Cuestionario
¿En qué situación?	En condiciones de respeto, profesionalismo investigativo y absoluta confidencialidad y reserva.

Tabla N° 6. Recolección de información

Elaborado por: Investigadora

3.6. Plan de procesamiento de la información

Los datos e información obtenida con las técnicas e instrumentos empelados, serán procesados siguiendo ciertos procedimientos que ayuden a que los resultados obtenidos se acerquen a la realidad lo más que fuere posible. Los procedimientos que se seguirán son:

- Observación crítica de la información recogida;
- Revisión y codificación de la información;
- Categorización y tabulación de la información;
    - Tabulación manual
- Análisis de los datos;
- Interpretación de los resultados;
    - La presentación de los datos se realizará a través de gráficos y cuadros para analizar e interpretarlos.
    - La redacción de una síntesis general de los resultados.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis de los resultados

En la presente investigación la información fue recopilada utilizando como técnicas la entrevista y la encuesta. En base a los datos recolectados en la entrevista realizada al Jefe de Sistemas que es el encargado de la administración de la base de datos empresarial y en base a la encuesta realizada al personal que realiza diferentes actividades en el Departamento de Sistemas de la empresa Automekano Cía. Ltda., de la ciudad de Ambato y sus diferentes sucursales en la ciudad de Quito y Guayaquil. Los modelos de la entrevista y la encuesta se desarrollaron de acuerdo a los modelos de los Anexos 1 y Anexo 2 respectivamente, donde se plantean las siguientes preguntas para la entrevista:

- **Entrevista al Jefe de Sistemas de la empresa Automekano Cía. Ltda.**

Para llevar a cabo la entrevista al Jefe de Sistemas quien es el que realiza las actividades de administración de la base de datos, se planteó varios criterios en base al análisis de las diferentes actividades y tareas que realizan los administradores de base de datos y administradores de los sistemas de información de las empresas de similar índole. A continuación se presenta el esquema de la Entrevista al Jefe de Sistemas para lo cual se trabajó con el modelo de entrevista que se presenta en el Anexo 1.

ENTREVISTA AL JEFE DE SISTEMAS

N°	PREGUNTAS	RESPUESTAS
1	¿Qué activos de la información podría ser testeados?	Los principales activos de la información que deberían ser testeados en temas de Seguridad de la Información son los servidores de producción, la base de datos, la infraestructura de red y los usuarios de red.
2	¿Por qué realizaría un testeo de seguridad a los activos antes descritos?	Para prevenir posibles riesgos o amenazas que pudiesen provenir de ataques informáticos y de esta forma evitar el daño o pérdida de los activos de mayor valor para la empresa.
3	¿Conoce usted si existen o no vulnerabilidades en la base de datos de la empresa?	Técnicamente no, pero considero como una amenaza principal que podría ser origen de vulnerabilidades el desconocimiento del usuario de la base de datos independientemente del rol o los privilegios que tenga sobre la base de datos de la empresa.
4	¿Cuál sería el posible origen de las amenazas que podría presentarse?	El origen podría principalmente ser el desconocimiento de los usuarios de los posibles riesgos y amenazas a los que puede estar expuesto el sistema de información y la base de datos, además podría presentarse otras amenazas más tangibles como accesos no autorizado externo ya sea por IP pública o por la red LAN.
5	¿Qué funciones principales realiza el sistema de información?	Procesa las transacciones principales de las actividades propias de la empresa y proveer la información para la toma de decisiones.
6	¿Qué funciones se deberían asegurar en el sistema de información?	Las funciones de integridad de la información, el aislamiento de accesos no autorizados, que permita la auditabilidad y el control, que permita recuperarse ante posibles pérdidas de disponibilidad, que permita la administración y custodia de la información.

7	¿Qué tipo de ataque informático ha sufrido la base de datos?	Hasta el momento se ha tenido ataques a la base de datos sin tener pérdida de disponibilidad del servicio y ataques a la IP pública sin llegar a la denegación del servicio.
8	¿Qué tipo de ataques relacionados con base de datos se podría presentar?	Algún ataque que permita la extracción de la información de referencia de las marcas representadas o de la base de datos de los clientes de la empresa.
9	¿Se cuenta con una metodología para la detección de vulnerabilidades en base de datos?	No existe una metodología para detectar vulnerabilidades en base de datos, lo único que se realizan son actividades de monitoreo y análisis de los logs de las herramientas de seguridad perimetral que tiene la red de comunicación de la empresa.
10	¿Se cuenta con una metodología para la mitigación de vulnerabilidades en base de datos?	No existe una metodología a seguir que permita mitigar vulnerabilidades, lo único que se hacen es actividades que permitan de uno u otro modo mejorar la seguridad sobre los equipos de seguridad de redes.

Tabla N° 7. Entrevista al Jefe de Sistemas

Elaborado por: Investigadora

En la presente investigación la información fue recopilada utilizando como técnica la encuesta, la misma que fue aplicada al personal que realiza diferentes actividades en el Departamento de Sistemas de la empresa; de acuerdo al modelo presentado en el Anexo 2, donde se plantearon las siguientes preguntas:

ENCUESTA AL PERSONAL DEL DEPARTAMENTO DE SISTEMAS

N°	PREGUNTAS
1	¿Cuál es el nivel de importancia de la información de la base de datos que maneja la empresa?

2	¿Con que tiempo se realiza un análisis de seguridad de base de datos en busca de vulnerabilidades?
3	¿Qué nivel se seguridad tiene el servidor de la base de datos de la empresa?
4	¿Qué software de seguridad se encuentra instalado en la empresa?
5	¿Qué usuarios pueden acceder a la información confidencial de la base de datos de la empresa?
6	¿Han existido ataques hacia el servidor de la base de datos de la empresa?
7	¿Se realizan acciones para la detección y mitigación de vulnerabilidades en base de datos?

Tabla N° 8. Encuesta al personal del Departamento de Sistemas

Elaborado por: Investigadora

4.2. Interpretación de datos

- **Análisis e interpretación de la entrevista al Jefe de Sistemas**

En base a las responsabilidades, funciones y experiencia que tiene el Jefe de Sistemas de la empresa Automekano Cía. Ltda., se realizó la entrevista en la que se puede poner en manifiesto la siguiente información:

Pregunta N° 1	**¿Qué activos de la información podría ser testeados?**
Respuesta:	Los principales activos de la información que deberían ser testeados en temas de seguridad de la información son los servidores de producción, la base de datos, la infraestructura de red y los usuarios de red.
Análisis:	El entrevistado manifiesta de la existencia de activos de

	información principales que considera deberían realizarse un testeo de Seguridad de la Información.
Interpretación:	Es importante que se tenga la apertura y conocimientos de la importancia y los beneficios de los testeos de seguridad de información por parte del Jefe de Sistemas de la empresa, debido a que muchos jefes de departamentos de sistemas de varias empresas no consideran importante este tipo de análisis, ya a que no han tenido hasta la presente fecha sospechas de posibles ataques y presencia de amenazas contra los activos de la información.

Tabla N° 9. Pregunta N° 1

Elaborado por: Investigadora

Pregunta N° 2	**¿Por qué realizaría un testeo de seguridad a los activos antes descritos?**
Respuesta:	Para evitar el daño o pérdida de los activos de mayor valor para la empresa y para prevenir posibles riesgos o amenazas que pudiesen provenir de ataques informáticos.
Análisis:	El Jefe de Sistemas de la empresa Automekano Cía. Ltda., pone en manifiesto que posibles riesgos y amenazas a la seguridad de la información podrían suscitarse, así como también no deja pasar por alto el hecho de que la metodología resultado de la presente investigación podría facilitar las futuras detecciones de vulnerabilidades ante la presencia de posibles amenazas y riesgos a la base de datos de la empresa.
Interpretación:	Los activos de información de la empresa Automekano Cía. Ltda., son activos altamente valorados dentro de los activos empresariales; debido a que se tiene el conocimiento y la experiencia por parte del Jefe de Sistemas de los problemas que se podría presentar y los mismos que podría ser prevenidos de manera temprana y evitar mayores inconvenientes que podría causar pérdidas a la empresa.

Tabla N° 10. Pregunta N° 2

Elaborado por: Investigadora

Pregunta N° 3	**¿Conoce usted si existen o no vulnerabilidades en la base de datos de la empresa?**
Respuesta:	Técnicamente no, pero considero como una amenaza principal que podría ser origen de vulnerabilidades el desconocimiento del usuario de la base de datos independientemente del rol o los privilegios que tenga sobre la base de datos de la empresa.
Análisis:	Al confirmarse que técnicamente no se tiene algún proceso o método que permita conoce con exactitud si existen o no vulnerabilidades a nivel de base de datos, esto es un problema ya que el desconocimiento podría significar un problema para la seguridad de la información que se procesa y almacena en la base de datos.
Interpretación:	Es preocupante que se tenga un desconocimiento de que si se tiene o no vulnerabilidades a nivel de base de datos, esto podría traer problemas de seguridad en los cuales no se pueda prevenir o plantear un plan de contingencia que permita contemplar un alcance más real de los posibles riesgos a que los que se expone la base de datos y por ende la información que se procesa y almacena en la misma.

Tabla N° 11. Pregunta N° 3

Elaborado por: Investigadora

Pregunta N° 4	**¿Cuál sería el posible origen de las amenazas que podría presentarse?**
Respuesta:	El origen podría principalmente ser el desconocimiento de los usuarios de los posibles riesgos y amenazas a los que se puede estar expuesto el sistema de información y la base de datos, además podría presentarse otras amenazas más tangibles como accesos no autorizados de tipo externo ya sea por IP pública o por la red LAN.
Análisis:	Muchas de las amenazas y riesgos que atentan contra la seguridad se ha podido evidenciar que es el desconocimiento de los mismos

	usuarios de los Sistemas de Información, la falta de concientización y de interés por acoger una cultura en el ámbito de la seguridad de la información; hablando de amenazas y riesgos que son de conocimiento avanzado para su ejecución, el entrevistado manifiesta que los accesos no autorizados que provienen del exterior por IP pública y por la red LAN, como se manifiesta ya se ha tenido evidencias de amenazas a las que se ha enfrentado la bases de datos de la empresa.
Interpretación:	La falta de interés de los usuarios de conocer los riesgos y amenazas que se pueden presentar en el sistema de información y en la base de datos, es lo que puede hacer que los mismos usuarios se conviertan en amenazas para la seguridad de la información. Además de la innovación que se tiene en el medio de las amenazas, riesgos y vulnerabilidades de seguridad por parte de personas que poseen conocimientos necesarios para llevarlas a cabo, hace que cada vez se vuelva más necesario la detección de vulnerabilidades, así como la mitigación y el fortalecimiento de la seguridad en los activos de información de la empresa.

Tabla N° 12. Pregunta N° 4

Elaborado por: Investigadora

Pregunta N° 5	**¿Qué funciones principales realiza el sistema de información?**
Respuesta:	Procesar las transacciones principales de las actividades propias de la empresa y proveer la información para la toma de decisiones.
Análisis:	Según la concepción breve y primordial que manifiesta el entrevistado, el procesamiento de la información a través de las diferentes transacciones provenientes de las actividades propias de la empresa es una de las funciones principales de sus sistemas de información, además de que dicho sistema provea información integra, la mantenga confidencial y siempre disponible para la toma de decisiones de la empresa.
Interpretación:	Todo sistema de información empresarial está realizado y adaptado a las necesidades de procesamiento de la información, el resultado de las actividades del día a día de la empresa es automatizado en los procesos del sistema de información lo que

	agilita los procesos y ayuda con la información necesaria para la toma de decisiones.

Tabla N° 13. Pregunta N° 5

Elaborado por: Investigadora

Pregunta N° 6	**¿Qué funciones se deberían asegurar en el sistema de información?**
Respuesta:	Las funciones de integridad de la información, el aislamiento de accesos no autorizados, que permita la auditabilidad y el control, que ayude a recuperarse ante posibles pérdidas de disponibilidad, que facilite la administración y custodia de la información.
Análisis:	Las funciones que pone en manifiesto el entrevistado son en su mayoría las que toda base de datos segura, debería contemplar para evitar cualquier riesgo o amenaza a la información que se considera el activo más valioso para la empresa Automekano Cía. Ltda.
Interpretación:	Toda base de datos empresarial debería contar con funciones que permitan obtener las características principales de la seguridad de información que puedan garantizar la confidencialidad, integridad y la disponibilidad.

Tabla N° 14. Pregunta N° 6

Elaborado por: Investigadora

Pregunta N° 7	**¿Qué tipo de ataque informático ha sufrido la base de datos?**
Respuesta:	Hasta el momento se ha tenido ataques a la base de datos sin tener pérdida de disponibilidad del servicio y ataques a la IP pública sin llegar a la denegación del servicio.

Análisis:	Como manifiesta el Jefe de Sistemas, hasta la presente fecha si se han manifestado intentos de ataques informáticos hacia la base de datos y ataques a la IP pública, ninguno de estos tuvo éxito y no se presentó pérdida de disponibilidad de los servicios tecnológicos.
Interpretación:	Se tiene la preexistencia de evidencia de ataques sufridos a los recursos tecnológicos de la empresa Automekano Cía. Ltda., esto hace que se tenga mayor interese por la realización de la presente investigación y se pueda contar con todas las facilidades por parte del Jefe de Sistemas y la Gerencia de la empresa.

Tabla N° 15. Pregunta N° 7

Elaborado por: Investigadora

Pregunta N° 8	**¿Qué tipo de ataques relacionados con base de datos se podría presentar?**
Respuesta:	Algún ataque que permita la extracción de la información de referencia de las marcas representadas o de la base de datos de los clientes de la empresa.
Análisis:	Según se manifiesta por parte del entrevistado, se puede considerar como un posible riesgo cualquier tipo de ataque que tenga como objetivos la extracción de información de la empresa, que se puede evidenciar y que podría ocasionar pérdidas incalculables para la empresa Automekano Cía. Ltda.
Interpretación:	Cuando se ha tenido la evidencia de amenazas y riesgos a los activos de la empresa, no se puede descartar cuales podría ser los posibles escenarios de originarse nuevos problemas de seguridad de información que atenten contra la base de datos de la empresa Automekano Cía. Ltda.

Tabla N° 16. Pregunta N° 8

Elaborado por: Investigadora

Pregunta N° 9	**¿Se cuenta con una metodología para la detección de vulnerabilidades en base de datos?**
Respuesta:	No existe una metodología para detectar vulnerabilidades en base de datos, lo único que se realizan son actividades de monitoreo y análisis de los logs de las herramientas de seguridad perimetral que tiene la red de comunicación de la empresa.
Análisis:	Como se manifiesta por parte del Jefe de Sistemas no se cuenta con una metodología que permita detectar vulnerabilidades de base de datos, al realizar monitoreos y análisis de los logs (registros de conexiones aceptadas o rechazadas de la red de comunicaciones) de las herramientas de seguridad perimetral de la red de comunicaciones, no se puede determinar ciertamente lo que una metodología de análisis de vulnerabilidades de base de datos si lograría este objetivo.
Interpretación:	Con los datos que revela esta pregunta de la entrevista se podría entender que el área de sistemas de la empresa, necesita comprender que los monitoreos y análisis de la información de registros de conexión aceptados o rechazados de la red de comunicaciones de los equipos de seguridad perimetral, no permiten determinar con exactitud si existen o no vulnerabilidades en la base de datos. Al desconocerse con puntualidad la existencia o no de vulnerabilidades de base de datos también se pone en riesgo la información de la empresa.

Tabla N° 17. Pregunta N° 9

Elaborado por: Investigadora

Pregunta N° 10	**¿Se cuenta con una metodología para la mitigación de vulnerabilidades en base de datos?**
Respuesta:	No existe una metodología a seguir que permita mitigar vulnerabilidades, lo único que se hacen es actividades que permitan de uno u otro modo mejorar la seguridad sobre los equipos de seguridad de redes.
Análisis:	Se pone en manifiesto por parte del Jefe de Sistemas la

	inexistencia de una metodología de mitigación de vulnerabilidades de base de datos, y aunque no es justificable es bastante comprensible ya que al no existir una metodología para detectar las vulnerabilidades de base de datos, consecuentemente no tendría relación la existencia de una sola metodología que necesita implícitamente de la otra.
Interpretación:	Si no se cuenta con una metodología para detección de vulnerabilidades de base de datos que permita descubrir las posibles amenazas y riesgos de seguridad de la base de datos, no tendría mucho sentido que se tenga una metodología de mitigación sin tener la información precedente a esta etapa que permita establecer la mitigación a amenazas, riesgos y vulnerabilidades desconocidas.

Tabla N° 18. Pregunta N° 10

Elaborado por: Investigadora

- **Análisis e interpretación de la Encuesta al personal del Departamento de Sistemas**

A continuación, se presentan los resultados de cada una de las preguntas:

Pregunta N° 1.- ¿Cuál es el nivel de importancia de la información de la base de datos que maneja la empresa?

NOTA: *Indicador Normal, representa la información que puede ser visualizada por cualquier usurario. Indicador Alto, representa la información que solo puede acceder personal autorizado.*

Análisis:

LITERAL	INDICADOR	VALORES	PORCENTAJE (%)
A	NORMAL	3	43%
B	ALTA	4	57%
	TOTAL	**7**	**100%**

Tabla N° 19. Pregunta N° 1

Elaborado por: Investigadora

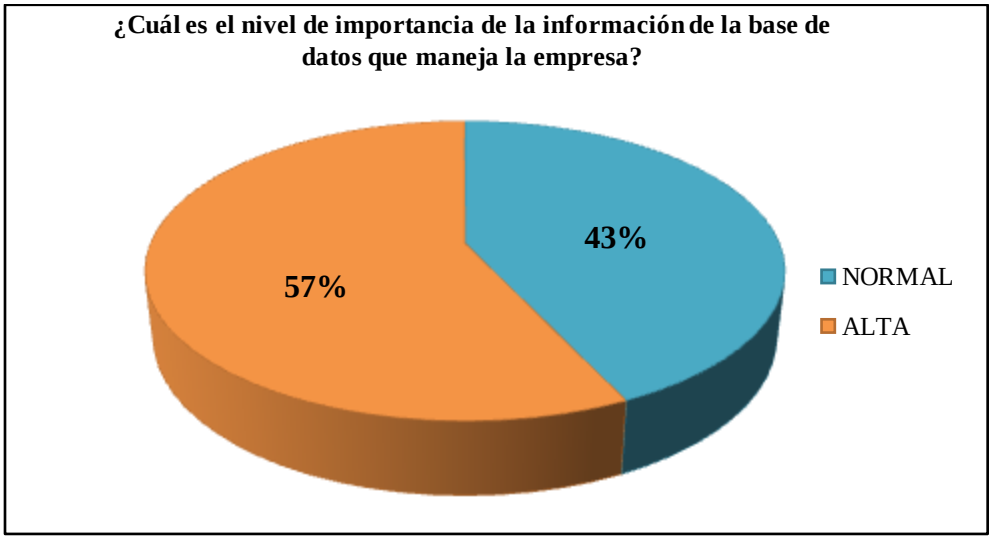


Figura N° 11. Pregunta N° 1

Elaborado por: Investigadora

Interpretación:

De los 7 encuestados que forman parte del Departamento de Sistemas de la empresa, 3 encuestados que representan el 43%, indica que el nivel de importancia de la información es considerado como normal, mientras que 4 encuestados que representan el 57% manifiestan que el nivel de importancia es alto.

Pregunta N° 2.- ¿Con qué tiempo se realiza un análisis de seguridad de base de datos en busca de vulnerabilidades?

Análisis:

LITERAL	INDICADOR	VALORES	PORCENTAJE (%)
A	SEMANAL	0	0%
B	MENSUAL	0	0%
C	SEMESTRAL	4	57%
D	ANUAL	0	0%
E	NUNCA	3	43%
	TOTAL	**7**	**100%**

Tabla N° 20. Pregunta N° 2

Elaborado por: Investigadora

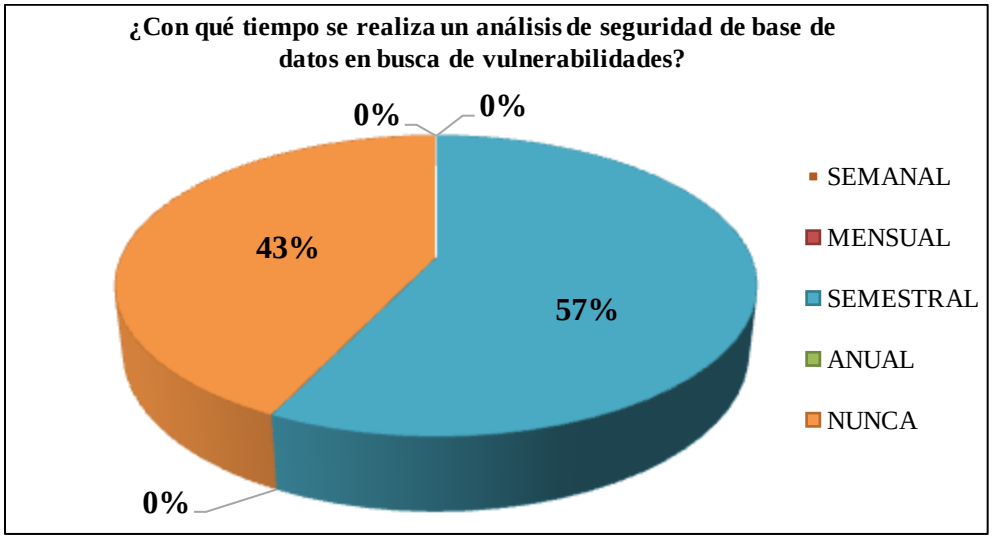


Figura N° 12. Pregunta N° 2

Elaborado por: Investigadora

Interpretación:

De los 7 encuestados que forman parte del Departamento de Sistemas de la Empresa, 4 encuestados que representan el 57%, indica que se realiza un análisis de seguridad de base de datos en busca de vulnerabilidades semestralmente, mientras que 3 encuestados que representan el 43% manifiestan que nunca se ha realizado un análisis de seguridad de base de datos.

Pregunta N° 3.- ¿Qué nivel de seguridad tiene el servidor de la base de datos de la empresa?

Análisis:

LITERAL	INDICADOR	VALORES	PORCENTAJE (%)
A	BAJO	0	0%
B	MEDIO	6	86%
C	ALTO	1	14%
	TOTAL	**7**	**100%**

Tabla N° 21. Pregunta N° 3

Elaborado por: Investigadora

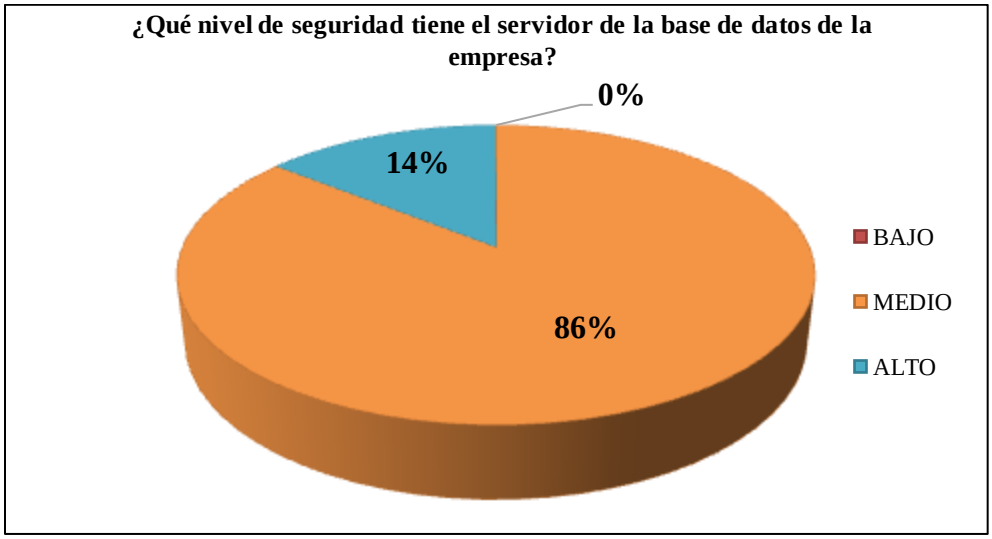


Figura N° 13. Pregunta N° 3

Elaborado por: Investigadora

Interpretación:

De los 7 encuestados que forman parte del Departamento de Sistemas de la empresa, 6 encuestados que representan el 86%, indica que el nivel de seguridad que poseen el servidor de la base de datos es medio, mientras que 1 encuestado que representa el 14% manifiestan que la seguridad es alto.

Pregunta N° 4.- ¿Qué software de seguridad se encuentra instalado en la empresa?

Análisis:

LITERAL	INDICADOR	VALOR	PORCENTAJE (%)
A	ANTIVIRUS	5	42%
B	FIREWALL	6	50%
C	DETECCIÓN DE MALWARE	0	0%
D	IDPS	0	0%
E	IDS	1	8%
	TOTAL	**12**	**100%**

Tabla N° 22. Pregunta N° 4

Elaborado por: Investigadora

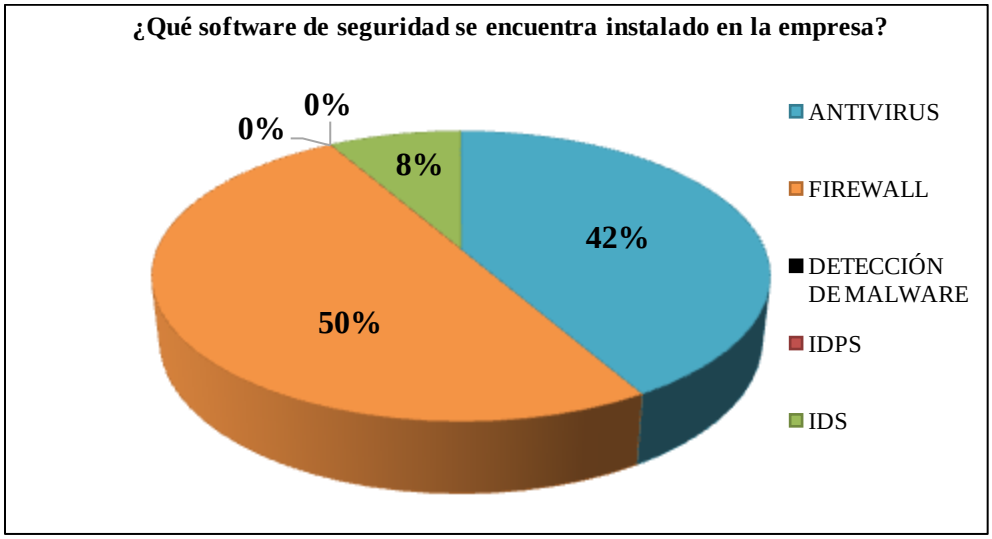


Figura N° 14. Pregunta N° 4

Elaborado por: Investigadora

Interpretación:

De los 7 encuestados que forman parte del Departamento de Sistemas de la Empresa, la pregunta 4 de opción múltiple, los encuestados señalaron la opción A) Antivirus, por 5 ocasiones que representan el 42%. Señalaron la opción B) Firewall, por 6 ocasiones que representan el 50%, y señalaron la opción C) Otros, por 1 ocasión que representa el 8%.

Pregunta N° 5.- ¿Qué usuarios pueden acceder a la información confidencial de la base de datos de la empresa?

Análisis:

LITERAL	INDICADOR	VALORES	PORCENTAJE (%)
A	ADMINISTRADORES	5	42%
B	ANALISTAS DE SISTEMAS	6	50%
C	OTROS	1	8%
	TOTAL	**12**	**100%**

Tabla N° 23. Pregunta N° 5

Elaborado por: Investigadora

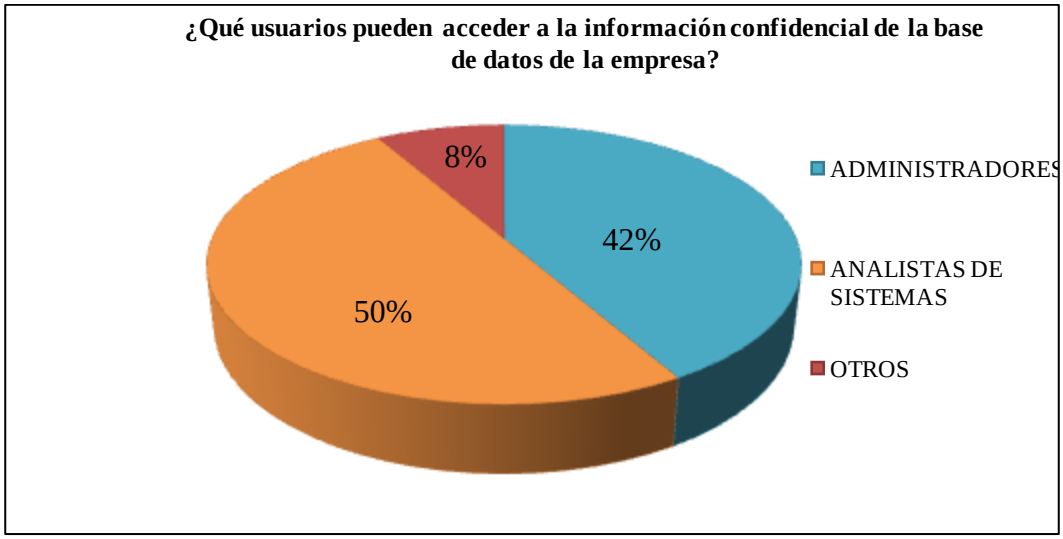


Figura N° 15. Pregunta N° 5

Elaborado por: Investigadora

Interpretación:

De los 7 encuestados que forman parte del Departamento de Sistemas de la empresa, en la pregunta 5 de opción múltiple, los encuestados señalaron la opción A) Administradores, por 5 ocasiones que representan el 42%. Señalaron la opción B) Analistas de Sistemas, por 6 ocasiones que representan el 50%, y señalaron la opción C) Otros, por 1 ocasión que representan el 8%.

Pregunta N° 6.- ¿Han existido ataques hacia el servidor de la base de datos de la empresa?

Análisis:

LITERAL	INDICADOR	VALORES	PORCENTAJE (%)
A	SI	1	14%
B	NO	2	29%
C	NO LO SABE	4	57%
	TOTAL	**7**	**100%**

Tabla N° 24. Pregunta N° 6

Elaborado por: Investigadora

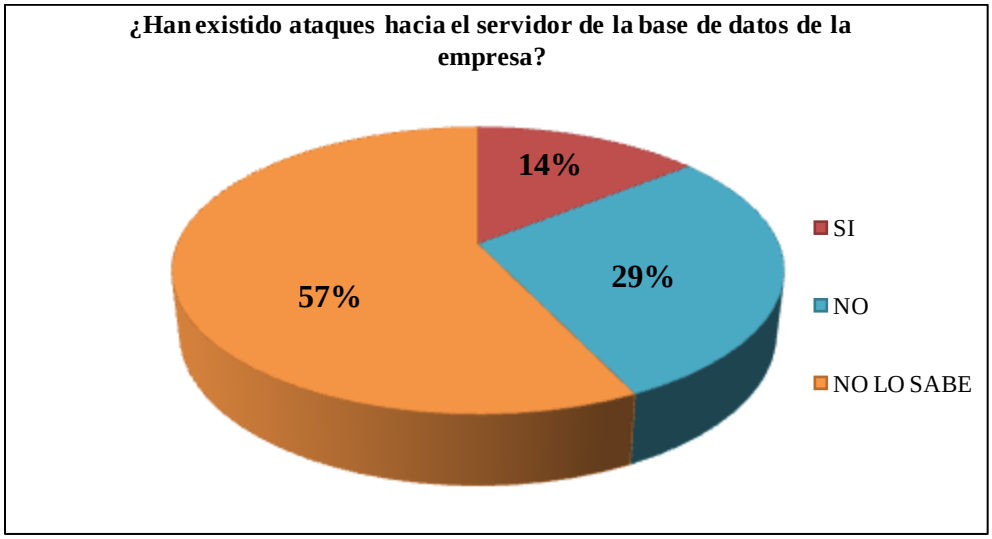


Figura N° 16. Pregunta N° 6

Elaborado por: Investigadora

Interpretación:

De los 7 encuestados que forman parte del Departamento de Sistemas de la Empresa, 4 encuestados que representan el 57%, indica que No saben si han existido ataques hacia el servidor de base de datos, mientras que 2 encuestados que representan el 29% manifiestan que No han existido ataques, mientras que 1 encuestado que representa el 14%, indica que Si han existido ataques hacia el servidor de base de datos.

Pregunta N° 7.- ¿Se realizan acciones para la detección y mitigación de vulnerabilidades en base de datos?

Análisis:

LITERAL	INDICADOR	VALORES	PORCENTAJE (%)
A	SI	3	43%
B	NO	4	57%
	TOTAL	**7**	**100%**

Tabla N° 25. Pregunta N° 7

Elaborado por: Investigadora

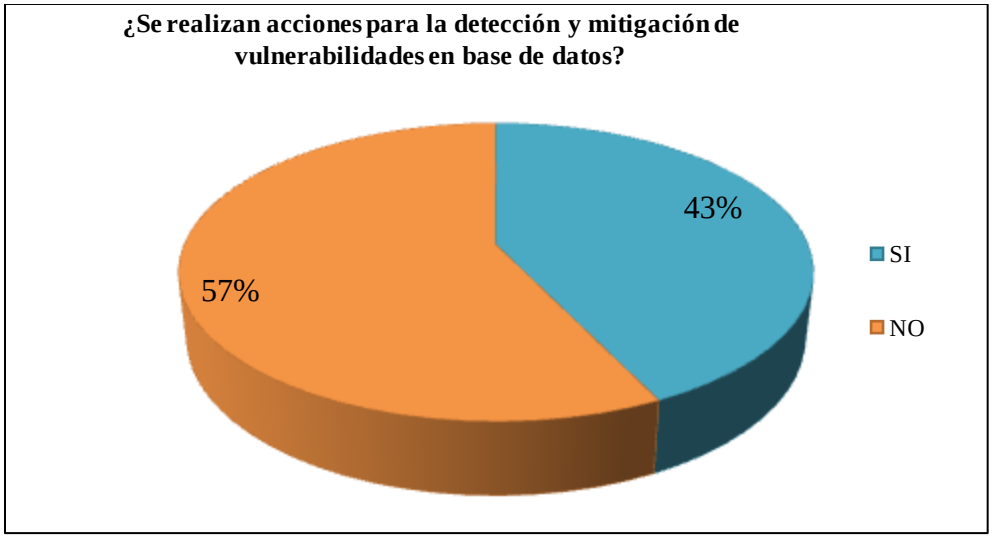


Figura N° 17. Pregunta N° 7

Elaborado por: Investigadora

Interpretación:

De los 7 encuestados que forman parte del Departamento de Sistemas de la empresa, 4 encuestados que representan el 57%, indica que No realizan acciones de detección de vulnerabilidades, mientras que 3 encuestados que representan el 43% manifiestan que Si realizan acciones de detección de vulnerabilidades de base de datos.

4.3. Verificación de la Hipótesis

Para verificar la hipótesis se tratará la información utilizando el método estadístico conocido como t-student, que permitirá determinar si se aplica o no la propuesta en poblaciones pequeñas.

Se ha tomado en cuenta las dos preguntas determinantes de la Encuesta al personal del Departamento de Sistemas, la número 2 y la número 6; debido a que los resultados arrojados, dicen que base de datos de la empresa necesita tener mayor control y mayores tipos de seguridades, ya que no se realizan análisis de seguridad de base de datos de manera más frecuente, lo cual puede provocar que existan vulnerabilidades y además existe desconocimiento por parte de las personas que

conforman el Departamento de Sistemas de la empresa sobre los niveles de seguridad que existen en los equipos.

- **Modelo Lógico**

La implementación de un sistema de detección y prevención de intrusos influirá en la seguridad de la información interna y confidencial de la empresa.

a) **Hipótesis Nula (H_0) =** La elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos **si** incidirá en la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

b) **Hipótesis Alterna (H_1) =** La elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos **si** incidirá en la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

Se calcula el intervalo de confianza en 95%, asumiendo que para:

$$\boldsymbol{H_0 = \mu 1 - \mu 2 = 0}$$
$$\boldsymbol{H_1 = \mu 1 - \mu 2 \neq 0}$$

- **Nivel de significancia y regla de decisión**

Se trabajará con un intervalo de confianza de IC 95%, para lo que se necesita calcular la varianza y el error estándar.

- **Elección de la prueba estadística**

$$\boldsymbol{t = \frac{\bar{x}_1 - \bar{x}_2}{EE(\bar{x}_1 - \bar{x}_2)} = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{S^2\left(\frac{1}{n1} + \frac{1}{n2}\right)}}}$$

Dónde:

$\boldsymbol{t} = t\ student$

$\boldsymbol{EE} = Error\ standar$

$\boldsymbol{\bar{X}} = Media$

$\boldsymbol{n} = Número\ de\ observaciones$

$\boldsymbol{S} = Desviación\ estandar$

- **Combinación de Frecuencias**

Se combina dos preguntas de la encuesta con el fin de comprobar la hipótesis y representar gráficamente dicha combinación.

Se trabajará con las preguntas 6 y 7 de la encuesta, se tratará de establecer la relación que permita verificar la hipótesis según el grado de significancia.

Frecuencias observadas

N°	PREGUNTAS	SI	NO	NO SABE	TOTAL
6	¿Han existido ataques hacia el servidor de la base de datos de la empresa?	1	2	4	7
7	¿Se realizan acciones para la detección y mitigación de vulnerabilidades en base de datos?	3	4	0	7
	TOTALES	**4**	**6**	**4**	**14**

Tabla N° 26. Frecuencias observadas

Elaborado por: Investigadora

Con los datos de las frecuencias observadas se procede a calcular la medida para cada pregunta seleccionada partiendo de la fórmula

$$\bar{x} = \frac{\sum x}{n}$$

De aquí según los tamaños muestrales n1 = 2 y n2 = 3 para la medida se tendría:

$$\bar{x}_1 = \frac{7}{2} \qquad \bar{x}_2 = \frac{7}{3}$$

$$\boldsymbol{\bar{x}_1 = 3.5} \qquad \boldsymbol{\bar{x}_2 = 2.33}$$

Una vez obtenidos estos datos se calcula la desviación típica para cada grupo de respuestas aplicando la fórmula:

$$\boldsymbol{S = \sqrt{\frac{1}{n-1}\sum (x - \bar{x})^2}}$$

A partir de esta fórmula tendremos los valores en las desviaciones típicas para los grupos como S1 y S2

Desviación estándar para S1:

$$\boldsymbol{S1 = \sqrt{\frac{1}{n_1 - 1}\sum (x_1 - \bar{x}_1)^2}}$$

$$S1 = \sqrt{\frac{1}{2-1}\left[(3-3.5)^2 + (4-3.5)^2\right]}$$

$$S1 = \sqrt{\frac{1}{1}\left[(-0.5)^2 + (0.5)^2\right]}$$

$$S1 = \sqrt{\frac{1}{1}\left[0.25 + 0.25\right]}$$

$$\boldsymbol{S1 = 0.71}$$

Desviación estándar para S2:

$$\boldsymbol{S2 = \sqrt{\frac{1}{n_2 - 1}\sum (x_2 - \bar{x}_2)^2}}$$

$$S2 = \sqrt{\frac{1}{3-1}\left[(1-2.33)^2 + (2-2.33)^2 + (4-2.33)^2\right]}$$

$$S2 = \sqrt{\frac{1}{2}\left[(-1.33)^2 + (-0.33)^2 + (1.67)^2\right]}$$

$$S2 = \sqrt{\frac{1}{2}\left[1.77 + 0.11 + 2.79\right]}$$

$$\boldsymbol{S2 = 1.53}$$

Se calculará la desviación típica o desviación estándar:

$$\mathbf{S2} = \frac{(\mathbf{n_1 - 1})\mathbf{S_2^1} + (\mathbf{n_2 - 1})\mathbf{S_2^2}}{\mathbf{n_1 + n_2 - 2}}$$

$$S2 = \frac{(2-1)0.71^2 + (3-1)0.1.53^2}{2 + 3 - 2}$$

$$S2 = \frac{(2-1)0.5041 + (3-1)2.3409}{2 + 3 - 2}$$

$$\boldsymbol{S2 = 1.729}$$

Con esto podemos calcular el error estándar:

$$\boldsymbol{EE = \sqrt{S^2\left(\frac{1}{n_1} + \frac{1}{n_2}\right)}}$$

$$EE = \sqrt{1.729\left(\frac{1}{2} + \frac{1}{3}\right)}$$

$$\boldsymbol{EE = 1.2}$$

Grados de libertad:

$$\boldsymbol{G_1 = (n_1 - 1)(n_2 - 1)}$$

Dónde:

$\boldsymbol{G_1} = Grados\ de\ libertad$
$\boldsymbol{n} = Núero\ de\ observación$

Remplazando se tiene:

$$\boldsymbol{G_1} = (2 - 1)(3 - 1)$$
$$\boldsymbol{G_1} = 2$$

De donde basándose en la tabla de distribución F para la distribución t tiene que el grado de significancia es:

$$\infty = \mathbf{2.92}$$

Con este resultado se procede a buscar el intervalo de confianza IC 95% y se tiene:

$$\boldsymbol{IC} = \ [(\bar{\boldsymbol{x}}_{\boldsymbol{1}} - \bar{\boldsymbol{x}}_{\boldsymbol{2}}) \pm \infty \boldsymbol{EE}\ (\bar{\boldsymbol{x}}_{\boldsymbol{1}} - \bar{\boldsymbol{x}}_{\boldsymbol{2}})]$$

$$IC95\% = \ [(3.5 - 2.33) \pm (2.95)(1.2)\ (3.5 - 2.33)]$$

$$IC95\% = \ 1.17 \pm 4.1$$

$$\boldsymbol{IC95\%} = \ (\mathbf{5.27}; \mathbf{-2.93})$$

- **Cálculo matemático**

Se busca que no exista asociación entre variables comprobando valores esperados a través de t-student. De donde se tiene según la graduación de niveles de las desviaciones estándar y la varianza para la distribución se tiene que:

$\boldsymbol{G_1 = 2}$ $\boldsymbol{\infty = 2.92}$

$\boldsymbol{\bar{x}_1 = 3.5}$ $\boldsymbol{\bar{x}_2 = 2.33}$

$\boldsymbol{n_1 = 2}$ $\boldsymbol{n_2 = 3}$

$\boldsymbol{EE = 1.2}$ $\boldsymbol{S2 = 1.53}$

Entonces aplicando la fórmula de t student:

$$\boldsymbol{t = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{S^2\left(\frac{1}{n1} + \frac{1}{n2}\right)}}}$$

$$t = \frac{3.5 - 2.33}{\sqrt{1.53\left(\frac{1}{2} + \frac{1}{3}\right)}}$$

$\boldsymbol{t = 1.04}$

- **Regla de decisión:**

Dado que para $H_0 = \mu 1 - \mu 2 = 0$ y para $H_0 = \mu 1 - \mu 2 \neq 0$, se hace referencia al grado de significancia de 2,92 según el resultado de t = 1,04, se avalúa según la regla general de aceptación dentro del intervalo de confianza IC (5,27: -2,93), si el valor se encuentra dentro del intervalo de confianza y el resultado t es menor al grado de significancia al referente a la hipótesis, esta es aceptada caso contrario esta deberá rechazarse, en tal virtud la regla se cumple y **la hipótesis se acepta**.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- El planteamiento del problema revela el riesgo de pérdida de seguridad de la información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato, que según la teoría investigada plantea y describe que los posibles efectos podrían ser la presencia de las vulnerabilidades en la base de datos empresarial, además de una factible presencia de amenazas y riesgos de la información que incrementarían significativamente las brechas de seguridad de información en la empresa.

- La información recabada con la técnica instrumental de investigación que se utilizó es una entrevista al Jefe de Sistemas y un cuestionario realizado al personal del Departamento de Sistemas de la empresa, permitió focalizar uno de los objetivos específicos que determina la realización de un análisis de los métodos actuales que se utilizan para detectar vulnerabilidades de base de datos.

- Los resultados de la entrevista ayudaron a determinar que el Departamento de Sistemas de la empresa no cuenta actualmente con una metodología para detectar vulnerabilidades de base de datos, así como tampoco se cuenta con la etapa complementaria que contempla una metodología de mitigación de

vulnerabilidades, por lo que se concluye que es importante el que se desarrolle la propuesta.

- Se detectó que 15% del personal del Departamento de Sistemas afirman que si han existido ataques de seguridad al servidor de la base de datos de la empresa, mientras que el 57% restante desconoce si han ocurrido o no este tipo de eventos. Además se descubrió con la investigación que más el 50% de la población establecida para esta fase investigativa afirma que no se realizan acciones parta la detecciones y mitigación de vulnerabilidades de base de datos.

5.2. Recomendaciones

- Se recomienda acoger la información que revela el planteamiento del problema y que la teoría investigada plantea y describe sobre las metodologías de detección y mitigación de vulnerabilidades de base de datos existentes, además de plantear una perspectiva amplia sobre las amenazas y riesgos de la información que podría afectar la seguridad de información en la empresa.

- Aceptar la información recabada con las técnicas instrumentales de investigación utilizadas, que ayudó a determinar la inexistencia de una metodología de detección y mitigación de vulnerabilidad, además de evidenciar el desconocimiento de la existencia o no de vulnerabilidades en la base de datos de la empresa.

- Desarrollar la propuesta de manera que permita establecer y desarrollar una metodología para detectar y mitigar las vulnerabilidades de base de datos de la empresa, con la finalidad de lograr prevenir posibles amenazas y riesgos de seguridad, además de obtener el aseguramiento y fortalecimiento de la seguridad de la base de datos de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

- Se recomienda la realización de la investigación, ya que la hipótesis se cumple sustentada en la investigación y resultados del estudio de probabilidad y estadística que se realizó aplicando la distribución t-Student, en el cual se obtuvieron resultados que se encuentra dentro del intervalo de confianza por lo tanto se fundamentó con esta etapa de la investigación que la hipótesis es aceptada.

CAPÍTULO VI

LA PROPUESTA

6.1. Datos informativos

La Empresa Automekano Cía. Ltda., constituida legalmente en el Ecuador en el año 2005, con la alianza estratégica de dos grupos empresariales importantes como son Ambacar y Automotores Carlos Larrea; caracterizados por su confiabilidad, rectitud y tradición en el negocio automotriz de la zona central del país.

Con décadas de experiencia en el sector automotriz, demostrada a través del manejo de varias marcas importantes de autos, brindado un respaldo total, tanto en atención al cliente, como en servicio técnico especializado y disponibilidad de repuestos; deciden asumir la responsabilidad de la distribución exclusiva en el Ecuador de las siguientes marcas importantes:

- En la línea de Camiones y Volquetas UD TRUCKS fundada en 1935.
- Maquinaria pesada y compactación JCV y VIBROMAX fundada en 1945.
- Maquinaría para asfalto Lee Boy ADSCD fundada en 1964.

Estas Marcas han sido comercializadas en el Ecuador desde hace casi 40 años.

En el año 2012 llega un nuevo reto para esta empresa y asume la distribución de uno de los principales fabricantes de Autobuses de China HIGER.

Visión

Ser el socio ideal de sus clientes proveyendo soluciones innovadoras para el crecimiento de sus negocios.

Política de Calidad

Automekano comercializa maquinaria, camiones, vehículos y autobuses de alta calidad y con tecnología de vanguardia, que cumplen estándares internacionales de seguridad; brindando oportunamente productos y servicio técnico especializado, garantizando siempre la satisfacción de sus clientes, con la innovación y capacitación continua en la compañía.

6.1.1. Título

"ELABORACIÓN DE UNA METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE VULNERABILIDADES DE BASE DE DATOS Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AUTOMEKANO CÍA. LTDA., DE LA CIUDAD DE AMBATO".

6.1.2. Institución ejecutora

Empresa Automekano Cía. Ltda.

6.1.3. Beneficiarios

Departamento de Sistemas.

6.1.4. Ubicación

Provincia: Tungurahua
Cantón: Ambato
Dirección: Avenida Indoamerica Km 1.

6.1.5. Tiempo estimado para la ejecución

Inicio: abril 2016
Fin: diciembre 2016

6.1.6. Equipo técnico responsable

- Investigadora: Ing. Carolina Anabel Bonilla Vaca.
- Jefe del Departamento de Sistemas de la empresa.

6.1.7. Costo

Se planeó un costo de un valor de $2.200,00 (DOS MIL DOSCIENTOS CON 00/100 DÓLARES DE ESTADOS UNIDOS DE AMÉRICA), el mismo que se estableció considerando los materiales utilizados en la presente investigación:

COSTOS DEL PROYECTO		
ÍTEMS	**DESCRIPCIÓN**	**COSTO**
1	Suministros de oficina	$ 100,00
2	Fotocopias	$ 90,00
3	Anillados, empastados, impresiones	$ 220,00
4	Transporte	$ 200,00
5	Servicios Básicos (luz, agua, teléfono, internet)	$ 350,00
6	Creación Ambiente de test y seguridad	$ 900,00
7	Dispositivos de almacenamiento externo	$ 140,00
8	SUBTOTAL	$2.000,00
9	10% IMPREVISTOS	$ 200,00
	TOTAL	**$2.200,00**

Tabla N° 27. Costos del proyecto

Elaborado por: Investigadora

6.2. Antecedentes de la propuesta

La empresa Automekano Cía. Ltda., cuenta con un sistema de información y base de datos donde la información se almacena y se procesa focalizando todo en un solo repositorio centralizado de datos, factor que hace que la información tenga la posibilidad de estar expuesta a la presencia de potenciales amenazas y riesgos a la seguridad de información que podría ocasionar diversos daños y perjuicios como: robo de información, fraudes, espionaje, sabotaje, vandalismo, entre otros., problemas de seguridad de información a los que se les conoce también como ataques informáticos o vulnerabilidades tecnológicas.

Ante la evidencia de la falta de una metodología que permita detectar las vulnerabilidades de base de datos, así como de forma completaría permita la prevención y mitigación ante la posible presencia de amenazas y riesgos de seguridad de la información; para la presente investigación se obtuvo información importante sobre la infraestructura, recursos y servicios tecnológicos que son parte de los activos de información de la empresa.

Se pudo evidenciar que la empresa actualmente cuenta con una infraestructura que brinda servicios tecnológicos en la oficina matriz en la ciudad de Ambato y a sus sucursales en la ciudad de Quito y Guayaquil, además cuenta con un grupo de personal de postventas que trabaja por todo el país.

La empresa cuenta con un software de gestión web ideal para pymes conocido como ZEUS – ERP que automatiza los procesos macro/principales como son: Vehículos, Talleres y Repuestos; además los procesos de apoyo de la empresa como son: tecnologías de la información, importaciones, recursos humanos y gerencia.

En el proceso macro Vehículos se realiza las actividades de seguimiento desde la prospección del cliente/cotizaciones hasta la venta del vehículo; el proceso macro Talleres controla las actividades que va desde la generación del presupuesto que aprueba el cliente hasta la entrega/facturación del trabajo del cliente y el proceso macro Repuestos controla las actividades desde la emisión de proformas para el

cliente hasta la entrega de repuestos; todos los procesos macros requieren en cualquier tiempo del proceso de apoyo de Importaciones.

El Sistema de Información Gerencial es parte del Sistema ZEUS - ERP que ayuda a la toma de decisiones para el proceso de Vehículos en el momento de realizar la compra e importación de nuevos vehículos y apoya en el proceso de Talleres y Repuestos para la compra e importación de repuestos para el stock y abastecimiento respectivos.

Todo el sistema ZEUS - ERP que automatiza las actividades de la empresa, funciona utilizando una diversidad de bibliotecas y la información ingresada se compila en una extensa y organizada base de datos centralizada que actualmente tiene un número de 1.310 tablas. Por ello, la característica fundamental de este tipo de software reside en recopilar y mantener disponible y actualizada la información de la que podrán hacer uso todos los sectores de la empresa, en cualquier momento que se requiera. Para una mejor comprensión del funcionamiento de todo el sistema se describe el mismo en la *Figura N° 18. Diagrama Funcional del Sistema ZEUS – ERP*.

DIAGRAMA FUNCIONAL DEL SISTEMA ZEUS – ERP

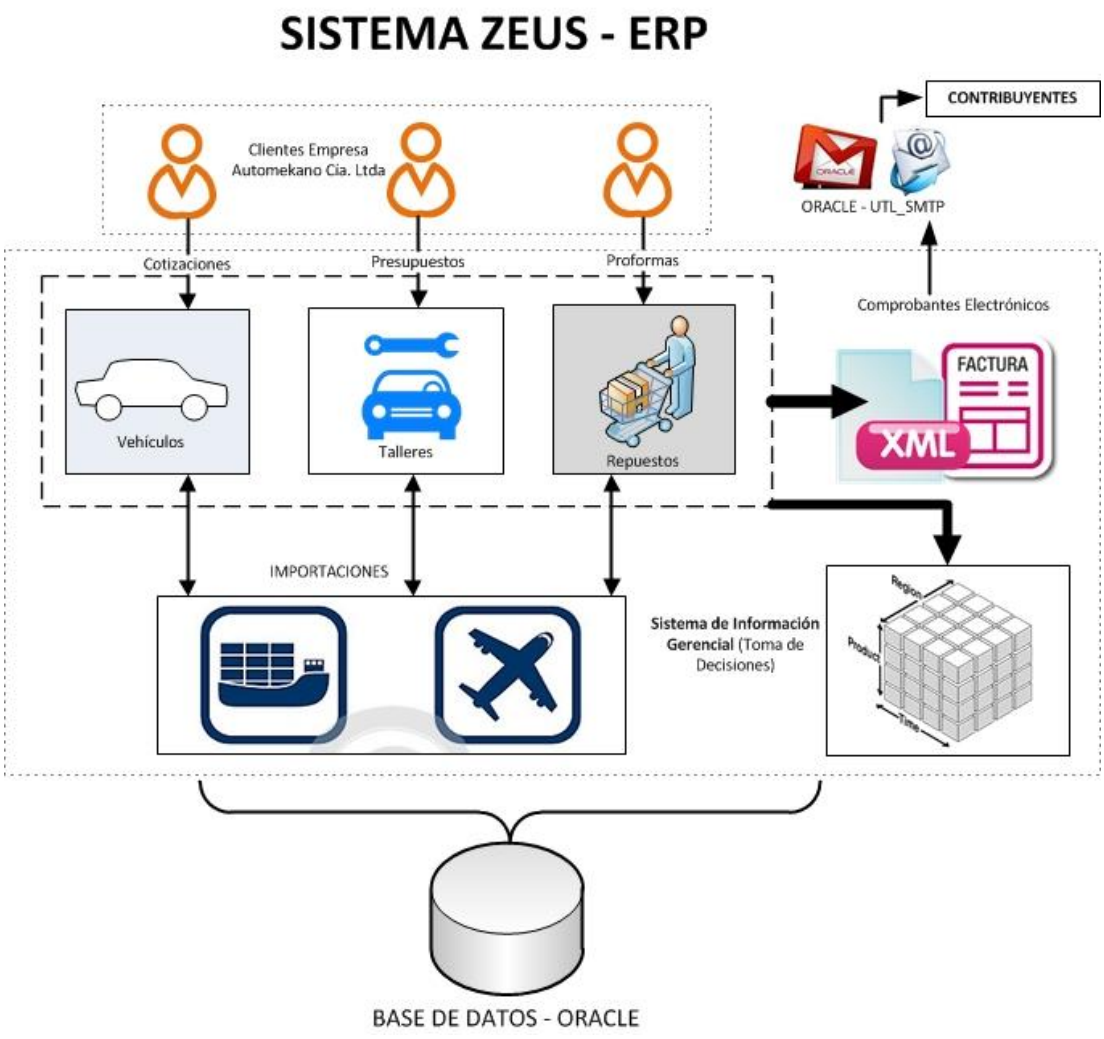


Figura N° 18. Diagrama Funcional del Sistema ZEUS - ERP

Elaborado por: Investigadora

La gestión de roles se realiza a través del Módulo de Seguridad tanto para usuarios del sistema ZEUS - ERP y para la los usuarios de base de datos.

ROLES DE USUARIOS DE LA BDD	
ROLE_ROL	ROLE_DESCRIPCION
1	GERENTE GENERAL
2	CONTADOR GENERAL
3	REPUESTOS

4	VENDEDOR VEHÍCULOS
5	JEFE DE TALLER
6	ADMINISTRADOR DEL SISTEMA
7	ASISTENTE CONTABLE 1
8	GERENTE REGIONAL
9	PASANTE
10	CAJA Y FACTURACION
11	IMPORTACIONES
12	GERENTE NACIONAL POSVENTA
13	POSTVENTAS REPUESTOS
14	ASISTENTE TALLER
15	BODEGA
16	COBRANZA
17	RECURSOS HUMANOS
18	PAGOS
19	GERENTE DE SERVICIOS
20	MARKETING

Tabla N° 28. Roles de usuarios de la Base de Datos.

Elaborado por: Investigador

El servidor principal en el que aloja la base de datos Oracle 10g posee un sistema operativo Oracle Linux.

La base de datos Oracle 10g cuenta con 35 usuarios, los mismos que están distribuidos de la siguiente forma:

- Ambato (matriz) 13 usuarios de BDD
- Quito 10 usuarios de BDD
- Guayaquil 8 usuarios de BDD
- Personal postventas 4 usuarios de BDD

En un segmento de red virtualizado aloja un servidor de escritorio remoto y el sistema de Comprobantes Electrónicos que cuenta actualmente con 90 tablas, este está implementado en la misma base de datos y actualmente no cuenta con acceso o publicación de servicios a través de IP pública.

6.3. Justificación

La empresa Automekano Cía. Ltda., cuenta con infraestructura y aplicaciones tecnológicas a través de las cuales se pueden realizar de forma automática muchas de sus actividades de gestión, administración y comercialización; parte fundamental de ello son los sistemas de información, las redes de comunicaciones y las bases de datos que permiten procesar, transportar y alojar la información de muchas actividades empresariales, razón por la que la información se convierte en el único activo de valor incalculable para la empresa, motivo fundamental para que los métodos, técnicas, procesos, estándares, normas o buenas prácticas que se empleen para lograr de cierta forma que dicho activo sea integro, disponible y confidencial es un reto constante de la empresa.

Al mismo tiempo que la empresa cuenta con servicios de tecnologías de información e incorporan medidas de seguridad, no se descarta la presencia de vulnerabilidades en las redes de comunicación, sistemas de información, base de datos, entre otros; las mismas que pueden facilitar que los atacantes cibernéticos que encuentren la manera de explotarlas. Esto representa un problema, ya que de lograrse romper alguna medida de seguridad perimetral, un hacker ilegal puede extender su ataque a toda la red y llegar a robar información importante de la base de datos, razones importantes para que la elaboración de una Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos que incida en la seguridad de la información sea prioritaria e importante para la empresa.

Debido a que se cuenta con las factibilidades investigativas, tecnológicas, económicas, legales y operativas; que hacen posible que el presente proyecto se desarrolle contemplando las distintas fases investigativas y aplicativas en la empresa, las mismas que permiten que se puedan realizar un análisis y testeos de seguridad para la búsqueda y detección de vulnerabilidades de base de datos; así como analizar y plantear las recomendaciones de mitigación a las mismas; con lo que la empresa podrá corregir, prevenir y fortalecer la seguridad de la base de datos y de esta forma mejorar e incrementar la seguridad de la información.

Finalmente se puede indicar que la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos contemplará características que le permiten ser un aporte investigativo a la comunidad, ya que se podría contar con un instrumento de investigación consistente y que puede repetirse, además de ser posible aplicarlo en empresas similares, ya que tiene una validez más allá del periodo de tiempo "actual"; la misma que para poder aplicarse, el investigador solo necesitará tener conocimientos básicos de seguridad de información y tener algunos méritos de analista y testeador de seguridad.

6.4. Objetivos

6.4.1. General

Desarrollar una Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos que incremente la Seguridad de la Información de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

6.4.2. Específicos

- Documentar la metodología que permite detectar y mitigar vulnerabilidades de base de datos de la empresa Automekano Cía. Ltda., de la ciudad de Ambato.

- Realizar la detección de vulnerabilidades de base de datos fundamentado en la metodología propuesta.

- Establecer las recomendaciones para la mitigación de las vulnerabilidades encontradas en la base de datos.

6.5. Análisis de factibilidad

6.5.1. Factibilidad tecnológica

a) Para realizar el análisis de detección de vulnerabilidades es necesario:

- Computador portátil marca DELL
  - Procesador Intel(R) Core (TM) i7 3612QM CPU @2.10GHz 2.10 GHz.
  - Memoria RAM 8 GB
  - Disco duro 500 GB
- Sistema Operativo Windows 7 ultimate 64 bits
- Conexión a la red empresarial
- Servicio de internet

b) El equipo donde se ejecutará el análisis de detección de vulnerabilidades de base de datos:

- Servidor HP ProLiant DL380 G6
  - Procesador Intel® Xeon® Quad-Core: E5530 (2.4GHz).
  - Memoria RAM de 32 GB
  - Disco duro SAS 500 GB
- Sistema Operativo Windows Oracle Linux 2.6.9
- Conectado en la red empresarial
- Servicio de internet

6.5.2. Factibilidad organizacional

Debido a que el desarrollo de la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos es un gran aporte a la seguridad de la información de la empresa Automekano Cía. Ltda., se cuenta con la autorización formal por parte de la Gerencia de la empresa y gracias al aporte del Departamento de Sistemas, se brinda la apertura necesaria para la realización del presente trabajo de investigación.

6.5.3. Factibilidad económica-financiera

La empresa Automekano Cía. Ltda., cuenta con los recursos tecnológicos necesarios sobre los cuales se ejecutará el análisis para la detección de vulnerabilidades, además de ello se trabajará con herramientas técnicas de código abierto (sin costo) y versiones de software Community, no se requiere de mayor inversión económica para el desarrollo del presente proyecto de investigación.

6.5.4. Factibilidad legal

Existe la autorización y aprobación a la solicitud para realizar el trabajo de investigación "ELABORACIÓN DE UNA METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE VULNERABILIDADES DE BASE DE DATOS Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AUTOMEKANO CÍA. LTDA., DE LA CIUDAD DE AMBATO", la misma que está legalmente formalizada y firmada por parte del Gerente Regional de la empresa. Revisar **Anexo 3.**

6.5.5. Factibilidad operativa

La metodología propuesta en el presente proyecto de investigación a más de presentar las etapas de detección que reúnen condiciones y prácticas funcionales del análisis de seguridad, se complementa con el análisis directo de los datos recopilados durante las etapas realizadas, a más de la etapa complementaria de análisis y documentación de la mitigación a los resultados encontrados. El esquema de la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos propuesta, consta de 8 etapas que se describen a continuación:

1) **Revisión de privacidad**
   - Inspección previa de la base de datos
   - Sistemas involucrados en la recolección de datos
   - Técnicas de obtención de datos

2) **Descripción de requisitos**

- Requisitos técnicos para el testeo de seguridad

3) **Sondeo de red**

- Análisis de configuración de red
- Análisis de DNS del dominio de internet
- Análisis de mapeo de red

4) **Identificación de los servicios y sistemas**

- Análisis de los servicios disponibles en los servidores y sus versiones
- Análisis de los servidores de nombres NetBIOS

5) **Búsqueda de información competitiva**

- Detección de vulnerabilidades en la base de datos
- Análisis de vulnerabilidades

6) **Búsqueda y verificación de vulnerabilidades**

- Informe de mitigación de vulnerabilidades de la base de datos

7) **Testeo de sistemas confiados**

- Sistemas dependientes de otros sistemas
- Tipo de vulnerabilidades que afectan los sistemas de confianza y aplicaciones

8) **Análisis de resultados**

- Recomendaciones de mitigación

La metodología cumple con las características que ISECOM (Institute for Security and Open Methodologies - Instituto para la Seguridad y las Metodologías Abiertas) plantea que se considere un test de seguridad, siempre que cumpla con las siguientes cualidades:

- Cuantificable
- Consistente y que se pueda repetir
- Válido más allá del período de tiempo "actual".
- Basado en el mérito del testeador y analista, y no en marcas comerciales.
- Exhaustivo.
- Concordante con leyes individuales y locales y el derecho humano a la privacidad.

6.6. Fundamentación

6.6.1. Metodologías de Análisis

El autor del e-book Hacking **(Benchimol, 2011)** plantea un capítulo de su obra para la investigación de Metodologías de Análisis, es así que prescribe que una metodología tiene una funcionalidad de una guía que implican una serie de métodos o técnicas para realizar determinados objetivos. Como se entiende que los métodos son en realidad procedimientos que permiten lograr los objetivos planteados. Si se aplica una metodología para el análisis de seguridad de información, se tendría que una metodología no es otra cosa que una o varias formas de conseguir los resultados de un testeos de seguridad estableciendo métodos organizados y en concordancia entre distintos profesionales.

6.6.2. Análisis comparativo de Metodologías de Análisis de Seguridad para Base de Datos

Para determinar el uso de la Metodología OSSTMM (Open Source Security Testing Methodology Manual - Manual de Metodología Abierta de Testeo de Seguridad), como base o fundamento para la determinación de la Metodología de Detección y Mitigación de Base de Datos que se propone en la presente investigación, se realizará un análisis comparativo de las metodologías más aplicadas para procesos de auditorías, testeos de seguridad, pentesting (prueba de penetración) y ethical hacking.

- **METODOLOGÍA OSSTMM**

La metodología OSSTMM 2.1 **(**Open Source Security Testing Methodology Manual - Manual de Metodología Abierta de Testeo de Seguridad), creada por **Herzog, (2003)** Director de ISECOM (Institute for Security and Open Methodologies - Instituto para la Seguridad y las Metodologías Abiertas), tiene una creciente aceptación en la comunidad de la Seguridad de Tecnologías de Información. La metodología representa un estándar de referencia en el área de testeo de seguridad en cualquier entorno desde el exterior al interior, incluye lineamientos de acción, la ética del testeador profesional, la legislación sobre el testeo de seguridad y un conjunto integral de testeo; OSSTMM pretende ser una guía referencial para el profesional.

El objetivo principal de OSSTMM es establecer un método aceptado que permita ejecutar un test de seguridad minucioso e íntegro, esta metodología no presenta ninguna recomendación a seguir como si se tratara de un manual técnico paso a paso. Lo más relevante de la metodología es que los diferentes test pueden ser evaluados y ejecutados en las áreas que sean aplicables, el que un testeador debe aplicar siempre una metodología estándar para que la calidad del resultado de un test de seguridad no sea difícil de juzgar. OSSTMM cubre únicamente el testeo de seguridad externo, que comprende acciones desde un entorno no privilegiado hacia un entorno privilegiado, para evadir los componentes de seguridad, procesos y alarmas para obtener el acceso privilegiado.

El alcance de la metodología es proveer un método estandarizado para realizar un exhaustivo test de seguridad en seis secciones de una organización y cada una determina sus respectivos módulos:

1) Seguridad de la información
2) Seguridad de los procesos
3) Seguridad en las tecnologías de internet
4) Seguridad en las comunicaciones
5) Seguridad inalámbrica
6) Seguridad física.

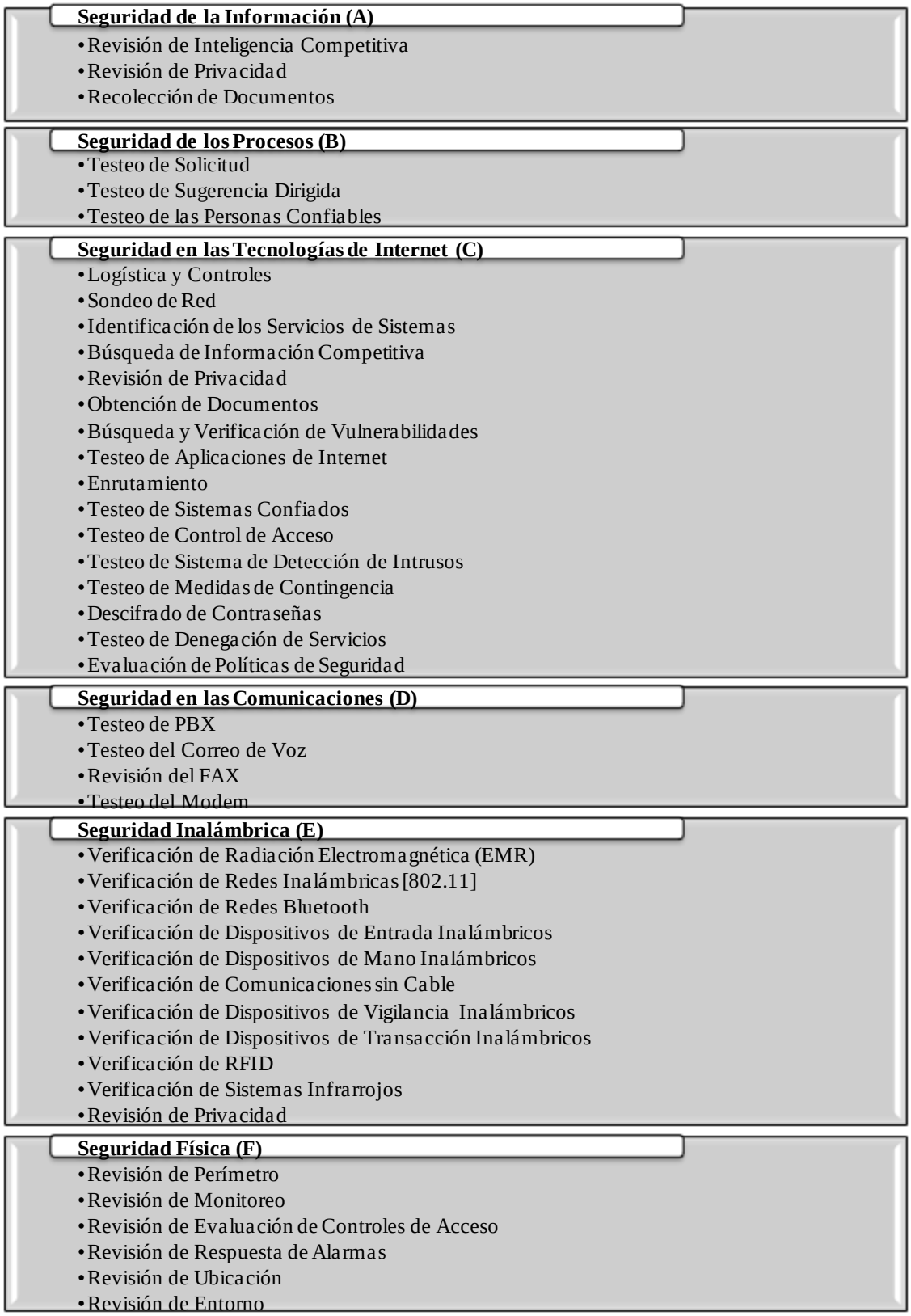


Figura N° 19. Metodología OSSTMM

Elaborado por: Investigadora

Se puede considerar un test OSSTMM si se cuenta con las características que exige el ISECOM:

- ✓ Cuantificable
- ✓ Consistente y que se pueda repetir
- ✓ Válido más allá del período de tiempo "actual"
- ✓ Basado en el mérito del testeador y analista, y no en marcas comerciales
- ✓ Exhaustivo
- ✓ Concordante con leyes individuales y locales y el derecho humano a la privacidad

El manual está dirigido para profesionales de testeo de seguridad, debido a que muchos de los términos, destrezas y procesos que presenta OSSTMM pueden no ser fáciles de comprender para aquellos que no están involucrados o con experiencia en testeos de seguridad.

- **METODOLOGÍA ISSAF**

En el sitio web oficial de **(OISSG, 2006)**, se da a conocer la metodología ISSAF (Información System Security Assessment Framework), sus siglas traducidas al español Marco de Evaluación de Seguridad de Sistemas de Información, es en sí, un marco metodológico de trabajo desarrollado por la OISSG (Open Information Systems Security Group) que permite evaluar las redes, los sistemas y las aplicaciones. La metodología apunta a 3 fases principales como son: la planeación y preparación, la evaluación y la presentación de informes.

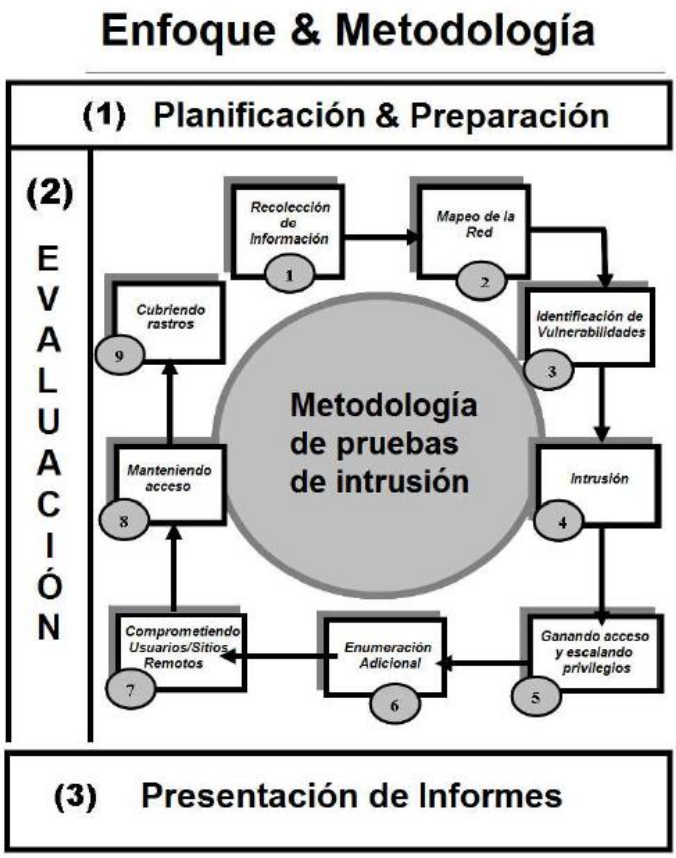


Figura N° 20. Metodología ISSAF

Elaborado por: ISSAF versión 0.2.1., 2006

FASE I: Planeación y preparación

Implica los pasos para el intercambio de información inicial, realizar la planificación y se prepara para la prueba; previo a realizar la prueba de intrusión debe existir un acuerdo formal entre las partes que provee un elemento básico de protección legal, el mismo que debe estar debidamente firmado por el representante de la empresa y el auditor, así mismo se debe determinar el grupo de trabajo, las fechas de la ejecución, los tiempos de la prueba, la ruta de escalamiento además de otras evaluaciones. Las actividades establecidas son:

- Identificar los contactos de parte y parte.
- Reuniones abiertas para confirmar el alcance, enfoque y metodología.
- Acordar los casos de prueba específicos y rutas de escalamiento.

FASE II: Evaluación

La evaluación es la fase en la que se ejecuta la prueba de intrusión, implica una perspectiva por capas, cada capa representa un mayor nivel de acceso a los activos de información, la evaluación comprende nueve capas:

1) **Recopilación de información:** Para recopilar la información se puede incluir el uso de internet para encontrar datos y conceptos sobre el objetivo que pueden ser empresas o personas, se puede usar métodos técnicos (DNS y Whois) y no técnicos como motores de búsqueda, grupos de noticias, listas de correo, entre otros.

2) **Mapeo de red:** Toda la información que compete a la red se toma de la recopilación de información y se expande para producir una metodología de red probable del objetivo. Se pueden utilizar para esta etapa varias herramientas y aplicaciones que permitan el descubrimiento de la información técnica de los host y redes involucrados en la prueba.

3) **Identificación de vulnerabilidades:** Para poder comenzar con esta parte, el auditor debe escoger los puntos específicos a probar y la forma de probarlos. Durante esta etapa el auditor tendrá que realizar varias actividades para detectar y explotar los puntos débiles.

4) **Intrusión:** Implica que el auditor intentará obtener acceso no autorizado, para evadir las medidas de seguridad y tratar de llegar al mayor nivel de acceso posible.

5) **Ganando acceso y escalando privilegios:** Estas actividades permiten a los auditores confirmar y documentar las intrusiones posibles y/o la propagación de ataques automatizados que ayudan a obtener una mejor evaluación del impacto para la empresa.

6) **Enumeración adicional:** Comprende: obtener contraseñas; rastrear tráfico y analizarlo; recoger las cookies y usarlas para explotar sesiones y para realizar ataques de contraseña; recolectar correos electrónicos; identificar rutas y redes además mapear redes internas.

7) **Comprometiendo usuarios/sitios remotos:** Basta que exista un solo agujero de seguridad en suficiente para exponer toda la red, sin importar que tan seguro puede ser el perímetro de red.

8) **Manteniendo acceso:** El software de túnel, las puestas traseras y los rootkits, además de otros, no se utilizan muy seguido debido al riesgo de que un atacante los descubra y obtenga acceso privilegiado al sistema.

9) **Cubriendo rastros:** Durante la prueba de intrusión es una práctica normal ocultar archivos y borrar registros, para actuar lo más abierto posible, la excepción a este es, si el cliente lo solicita. Para generar información en detalle y registro de todas las actividades.

FASE II: Presentación de informes

Se puede presentar un informe verbal para informar inmediatamente a la empresa, en caso que se halle alguna vulnerabilidad en el transcurso de las pruebas de intrusión. Una vez finalizado todos los casos de prueba definidos en el alcance, se debe presenta un informe final por escrito con los resultados de las pruebas y las recomendaciones de las mejoras respectivas. Finalmente se procede con la limpieza del sistema de las pruebas de instrucción realizada.

- **METODOLOGÍA OWASP**

Según su propio sitio web **(OWASP, 2000)** El Proyecto Abierto de Seguridad de Aplicaciones Web - OWASP (Open Web Application Security Project), es una organismo sin ánimo de lucro creada y formada por empresas, organizaciones educativas y particulares de todo el mundo liderada por Jess Williams y de total

independencia de fabricantes. La metodología comprende un marco de trabajo diseñado para apoyar en el proceso del ciclo de desarrollo de software (SDLC), es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro, contemplando desde un inicio la seguridad en la ingeniería de software. Uno de sus trabajos es la Guía de Pruebas que es un manual de referencia con vulnerabilidades, contramedidas y una completa metodología para la revisión y evaluación del estado de seguridad de nuestras aplicaciones.

El material de la comunidad OWASP está disponible licencias de software libre y abierto, la metodología recomienda enfocar la seguridad de aplicaciones informáticas poniendo atención en todas sus dimensiones: personas, procesos y tecnología.

(Benchimol, 2011) resume los proyectos OWASP que se dividen en dos categorías principales que son los proyectos de desarrollo y de documentación.

- **Proyectos de Documentación**

  - **Guía de desarrollo.-** Un documento que proporciona una guía detallada para construir aplicaciones web seguras.
  - **Guía de pruebas.-** Una guía centrada en las pruebas y listas de comprobación de seguridad sobre aplicaciones web.
  - **Top 10.-** un documento extracto sobre las vulnerabilidades críticas de las aplicaciones web.
  - **Legal.-** Un proyecto centrado en la contratación de servicios de software y sus aspectos de seguridad.
  - **AppSec FAQ.-** Es donde se encuentran respuestas a las preguntas más frecuentes sobre seguridad de aplicaciones web.

- **Proyectos de Desarrollo**

  - **WebScarab.-** Una aplicación para realizar pruebas de seguridad en aplicaciones y servicios web.

- **WebGoat.-** Un entorno de entrenamiento para que los usuarios aprendan sobre seguridad de aplicaciones web de forma segura y legal.

Para enfocar a OWASP a lo que contempla una metodología para la ejecución de test de seguridad, en este caso se orienta el estudio en la guía de pruebas. El framework se describe cinco fases que comprende:

1. Fase previa al desarrollo
2. Fase de definición y diseño
3. Fase del tiempo en que se realiza el desarrollo
4. Fase del tiempo de instalación y publicación
5. Fase de mantenimiento y operaciones

La guía de pruebas, se divide en:

- Obtención de información
- Pruebas de reglas de negocio
- Pruebas de autenticación
- Pruebas de manejo de sesión
- Pruebas de validación de datos
- Pruebas de denegación de servicio (DoS)
- Pruebas de servicios web
- Pruebas de AJAX.

a. Comparativa de las Metodologías de Análisis de Seguridad para Base de Datos

Para realizar la comparativa de las metodologías y poder determinar la que mejor se ajuste a los objetivos de la investigación, además que pueda presentar una línea de referencia para la elaboración de la Metodologías de Detección y Mitigación de Vulnerabilidades de Base de Datos que se propone en la presente investigación.

COMPARATIVA DE LAS METODOLOGÍAS DE ANÁLISIS			
CARACTERÍSTICAS	**OSSTMM**	**ISSAF**	**OWASP**
Ámbitos de aplicación	6	3	1
Metodología actual	✓		✓
Soporte de la comunidad	✓		✓
Plantillas para testeo	✓	✓	
Guía técnica paso a paso		✓	✓
Presentación de informes y reportes	✓	✓	
Valores de evaluación de riesgo	✓		
Permite medir el funcionamiento de la seguridad	✓		
Diseño y construcción de un plan de mitigación		✓	
Se adapta a la ISO 27000	✓		

Tabla N° 29. Comparativa de las Metodologías de Análisis

Elaborado por: Investigadora

Sin duda la metodología OSSTMM se elige de entre las demás porque cubre seis ámbitos de análisis como son: seguridad de la información, seguridad de los procesos, seguridad en las tecnologías de internet, seguridad en las comunicaciones, seguridad inalámbrica y seguridad física. Al ser una metodología que presenta más ámbitos que las demás, permite cubrir el propósito principal de la metodología propuesta que proyecta detectar vulnerabilidades de las bases de datos. La metodología ISSAF únicamente es aplicable en tres ámbitos: redes, sistemas y aplicaciones; mientras que la metodología OWASP cubre únicamente las aplicaciones web.

La metodología que se toma como fundamento o línea base de investigación para la elaboración de la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos, es la metodología OSSTMM principalmente porque es una metodología actual; al ser un manual de metodología abierta se puede plantear modificaciones, además que las plantillas que presenta OSSTMM ayudan al levantamiento de información para un mejor análisis y cuenta con métodos que permiten medir el funcionamiento de la seguridad y evaluación del riesgo.

OSSTMM al no presentar un diseño o método que permite la construcción de planes de mitigación, permite que se pueda plantear una metodología nueva que presente a más de un análisis de las vulnerabilidad, un método para las recomendaciones y mitigaciones a las vulnerabilidades, lo que ayuda a que la metodología propuesta presente a la empresa (cliente) un panorama más amplio que no solo muestre sus puntos débiles de seguridad sino también las posibles gestiones y acciones para la prevención, fortalecimiento y mejora.

6.7. Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos (DMV-BDD "Detección y Mitigación de Vulnerabilidades de Base de Datos")

Para el desarrollo y la implementación de la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos (DMV-BDD "*Detección y Mitigación de Vulnerabilidades de Base de Datos"*) se toma como referencia la Metodología de testeo de seguridad OSSTMM que presenta una línea de fundamento válido para todas las metodologías de testeo de seguridad tanto conocidas como inexploradas y no limita la creatividad del investigador al no contener estándares demasiado formales o rigurosos, dejando así ámbitos abiertos para que el investigador pueda encajar nuevos métodos de trabajo.

La metodología que se propone no cubre los testeos de seguridad externos que involucra testeos externo a interno como lo hace la metodología OSSTMM, la Metodología DMV-BDD que describe la propuesta cubre el tipo de testeo interno a interno que permite realizar análisis con la ejecución de pruebas de caja blanca o

pruebas de caja gris, donde el testeador tiene conocimiento previo de los elementos o del entorno a ser testeado.

Gracias a que la presente investigación cuenta con la aprobación y aval de la empresa Automekano Cía. Ltda., permite contar con privilegios de acceso como son las credenciales del usuario administrador de la base de datos, además de tener un entorno privilegiado donde no se tiene que hacer esfuerzos para evadir los componentes de seguridad para realizar el reconocimiento pasivo de red, el mismo que permite dejar libre de herramientas de seguridad perimetral al servidor que contiene la base de datos.

El alcance de la metodología propuesta fundamenta las etapas de la realización de los análisis exhaustivos y test de seguridad en dos de los seis métodos que contiene la metodología OSSTMM, los mismos que se describen a continuación:

- Seguridad de la información
- Seguridad en las Tecnologías de Internet

La metodología propuesta en la presente investigación no necesita ser implementada o seguida por profesionales del testeo de seguridad como OSSTMM requiere, ya que únicamente se necesita conocimientos básicos en seguridad de información para entender los términos y métodos utilizados, lo que si requiere es una capacidad de análisis de investigación bastante amplia para que permita al analista estudiar y examinar las vulnerabilidades y poder establecer las recomendaciones para su prevención y mitigación.

Para obtener un análisis más profundo y real, la metodología propuesta no se puede trabajar en ambientes de pruebas, debido a que podrían existir configuraciones especiales y procesos que la base de datos realiza como parte de su desempeño, que incluso el respaldo completo de un sistema de base de datos no podría restaurar en un ambiente de pruebas.

Los métodos utilizados para los testeo de seguridad en la metodología propuesta son pasivos, esto hace posible que se pueda realizar los análisis de testeo en el ambiente real de la base de datos sin la necesidad de detener los servicios en lo referente a la

base de datos como tal; aunque para realizarse pruebas iniciales de reconocimiento e identificación de servicio y sistemas se realiza con análisis pasivos de red, para esta etapa si es necesario que se habilite una ventada de mantenimiento en la empresa donde se aplica, para así no realizar este proceso en horas laborables y que esto asegure que nadie más hace uso de los servicios tecnológicos de la empresa para no confundir el ambiente de análisis.

La metodología propuesta a más de presentar las etapas de detección que reúne condiciones y prácticas funcionales del análisis de seguridad, se complementa con el análisis directo de los datos recopilados durante las etapas realizadas y la etapa de análisis y documentación de la mitigación a los resultados encontrados. A continuación se presenta el esquema de la metodología propuesta:

METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE VULNERABILIDADES DE BASE DE DATOS (DMV-BDD)

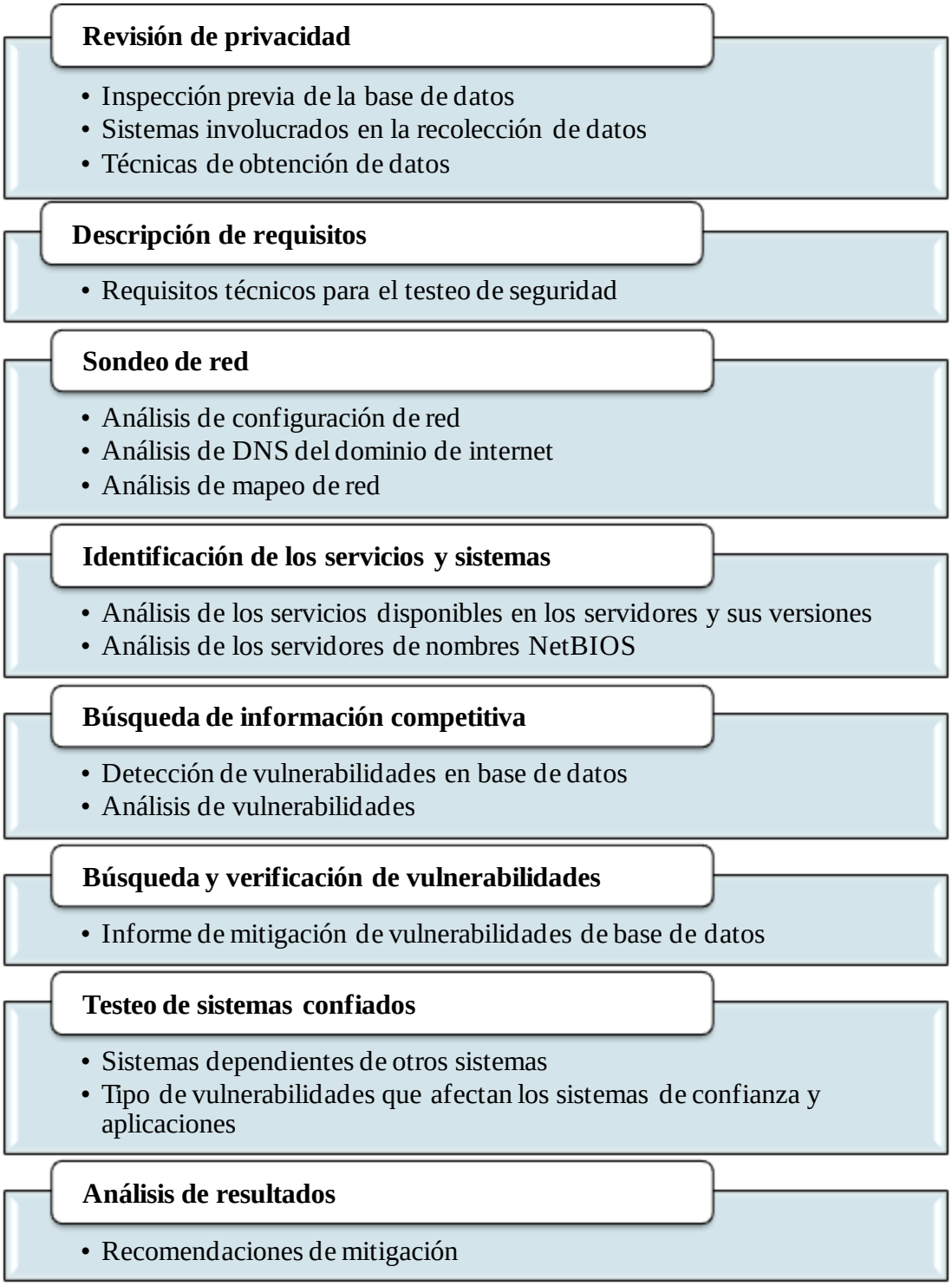


Figura N° 21. Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos (DMV-BDD)

Elaborado por: Investigadora

La Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos (DMV-BDD) propuesta, consta de 8 etapas las mismas que se describen a continuación:

1) Revisión de privacidad

Según describe (Herzog, 2003), en la metodología OSSTMM *"la privacidad implica que el proceso es conocido únicamente por los sistemas o partes involucradas".*

Para esta etapa se debe indicar que todos los análisis deben ejecutarse manteniendo el derecho a la privacidad personal sin importar la ley regional. La ética y el entendimiento de la privacidad son a menudo más avanzados que la legislación actual.

La revisión de la privacidad es el punto de vista global y ético del almacenamiento, transmisión y control de los datos basados en la privacidad del cliente y del empleado de una empresa. El uso de estos datos es la preocupación de muchas personas privadas y la legislación no da reglas específicas considerando la privacidad. Por lo que para esta etapa se podría contemplan el establecimiento de actas de confidencialidad de información entre la empresa y el investigador si así lo consideran necesarias las partes, también podría contemplarse el acta entrega de información que compete a esta etapa o al menos que el gerente general autorice formalmente la realización de los trabajos de investigación.

En esta etapa se recomienda que el investigador realice el levantamiento de la información que contemple:

a. Inspección previa de la base de datos: Es necesario realizar una inspección previa de la base de datos, la que puede consistir en el levantamiento de la información general de todo lo que relaciona a la base de datos, como en qué tipo de servidor está alojada, el sistema operativo del servidor donde se implementó la base de datos, qué sistema de base de datos poseen, qué sistemas consumen los recursos de la base de datos, cuántos usuarios posee, qué privilegios y roles tienen, entre otros datos que pueden servir de antecedente a la investigación.

b. Sistemas involucrados en la recolección de datos: Se refiere a los sistemas involucrados generalmente en los test de seguridad, en la búsqueda de vulnerabilidades y las comprobaciones automáticas que implican los testeos y análisis en un sistema de base de datos dentro de una red o redes.

c. Técnicas de obtención de datos: Son todas las técnicas que se utilizan a través de la aplicación de análisis profesional mediante escaneos de seguridad, donde se puede determinar si se realizará o no la intrusión que generalmente se usa para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

Siempre hay que dar a conocer a la empresa en qué consiste la instrucción, ya que cuando se trabaja en ambientes de producción, se omite por completo este tipo de comprobación de las vulnerabilidades.

El análisis de seguridad de base de datos, ubicaciones y procesos inestables y obviamente inseguros, están prohibidos hasta que hayan sido debidamente asegurados. Se espera que el analista use evidencia recopilada únicamente para proveer una revisión adecuada de la base de datos y procesos de seguridad.

2) Descripción de requisitos

La descripción de requisito implica detallar la información del equipo de cómputo, así como los requisitos de software que comprende aplicaciones o herramientas de software necesarias para la ejecución de los análisis y testeos de seguridad. No se determina si la empresa debe o no proveer de dichos requisitos, lo que si se debe contemplar es las características técnicas para que el proceso de análisis y detección de vulnerabilidades se desarrollen de forma efectiva y óptima.

a. Requisitos técnicos para el testeo de seguridad

- Requisitos de hardware
- Requisitos de software (aplicaciones – herramientas)

3) Sondeo de red

El autor del Manual de Metodología Abierta de Testeo de Seguridad OSSTMM 2.1., **Herzog, (2003: 47)** establece que, el sondeo de red sirve como introducción a los sistemas a ser analizados. Se podría definir mejor como una combinación de recolección de datos, obtención de información y política de control. A pesar que a menudo es recomendable desde un punto de vista legal el definir exactamente y contractualmente los sistemas a analizar, si el investigador es un auditor externo o aún si es el administrador de sistemas puede ser que no pueda empezar con los nombres de sistema o IPs en concreto, es mejor tener la certeza de ésta información por lo que es necesario sondear y analizar.

La clave es encontrar el número de sistemas alcanzables que deben ser analizados, para localizar de entre todos ellos al sistema de base de datos; el sondeo de red debe ejecutarse sin exceder los límites legales de lo que se quiere analizar. Por lo tanto, el sondeo de red es simplemente una forma de empezar un test; otra forma sería recibir el rango de direcciones IP y comprobar en qué equipo se aloja la base de datos. En este módulo no se realiza ningún tipo de intrusión directamente en los sistemas, excepto en los sitios considerados un dominio cuasi-público.

A continuación se presentan los análisis de sondeo de red con los que el investigador puede recolectar y confirmar información básica del entorno de la base de datos. Si el investigador conoce de otras formas de testeo de red puede aplicarlas, lo importante de esta etapa es conseguir información que permita tener un panorama completo y comprar el entorno de la base de datos.

a. Análisis de configuración de red: Este análisis permite verificar la configuración de las interfaces de red, la tabla de enrutamiento de red IP, permite conocer la máscara de red, broadcast de red, dirección gateway, dirección IP de destino y servidores DNS. Es decir todo lo que implica las conexiones de comunicaciones de red que se relacionan con el servidor de la base de datos.

b. Análisis de DNS del dominio de internet: El propósito de este análisis es reunir la mayor cantidad de información posible del segmento de red donde se

aloja el servidor de la base de datos, el investigador podrá ejecutar en la herramienta de testeo las acciones necesarias para detallar la información del dominio de internet.

c. Análisis de mapeo de red: Toda la información que compete al segmento de red donde se conecta el servidor de base de datos, se toma de la recopilación de información y se expande para producir una metodología de red probable del objetivo. Se pueden utilizar para esta etapa varias herramientas y aplicaciones que permitan el descubrimiento de la información técnica de los host y redes involucrados en la prueba.

4) Identificación de los servicios y sistemas

El autor de la metodología OSSTMM **Herzog, (2003: 47)** determina que el escaneo de puertos es la prueba invasiva de los puertos del sistema en los niveles de transporte y red. También se incluye aquí la validación de la recepción del sistema a protocolos tunelizados, encapsulados o de enrutamiento. En este módulo se deben enumerar los servicios de Internet activos o accesibles así como traspasar al cortafuegos (herramienta de seguridad perimetral – firewall) con el objetivo de encontrar más máquinas activas. La pequeña cantidad de protocolos empleados aquí tiene el objetivo de resultar en una definición clara de los objetivos. Es por esto que algunos de los protocolos no aparecen.

El testeo de diferentes protocolos dependerá del tipo de sistema y servicios que ofrecen los sistemas, cada base de datos utiliza protocolos de puerto escucha por defectos y si el servidor de la base de datos tiene configuraciones por defecto, podría detectarse puertos abiertos innecesariamente. Cada servidor activo en Internet dispone de 65.536 puertos TCP y UDP posibles (incluido el Puerto 0). En cualquier caso, no siempre es necesario comprobar todos estos puertos en cada sistema. Esto se deja a la libre elección del equipo que realiza los tests. Una vez los puertos abiertos han sido identificados, es necesario llevar adelante un análisis de la aplicación que escucha tras dicho servicio. En algunos casos, más de una aplicación puede encontrarse detrás de un servicio donde una aplicación es la que realmente escucha

en dicho puerto y las otras se consideran componentes de la aplicación que escucha. Tras la identificación de los servicios, el siguiente paso es identificar el sistema mediante las pruebas sobre el sistema con el fin de obtener respuestas que puedan distinguir su sistema operativo y su versión.

a. Análisis de los servicios disponibles en los servidores y sus versiones: Para realizar el escaneo de todos los puertos es necesario no tener la presencia de herramientas de seguridad perimetral (cortafuegos), el análisis permite diferenciar el estado de los puertos, además la revisión de versiones para cada puerto abierto encontrado, para tratar de identificar el tipo y la versión de los servicios descubiertos.

b. Análisis de los servidores de nombres NetBIOS: El escaneo que permite realizar la exploración de la capa de software NetBIOS que facilita la comunicación entre la red y los servidores. El resultado de dicho escaneo sobre los servidores que ejecutan el servicio NetBIOS en la red, permite identificar los servidores dentro de la red local, los servidores con la información de la dirección IP, nombre NetBIOS, nombre del usuario con la sesión iniciada en el equipo y la dirección MAC.

5) Búsqueda de información competitiva

Comprende la búsqueda de información útil a partir del análisis y testeo de seguridad realizado y que puede ser tratada como información relevante. La información competitiva tiende a ser no invasiva y mucho más sutil debido a que un test no intrusivo permite dar un valor añadido a sus diferentes componentes y puede ayudar para encontrar las vulnerabilidades.

a. Detección de vulnerabilidades en base de datos: La detección de vulnerabilidades en base de datos, es una parte fundamental del análisis de seguridad, para efectos de la investigación se puede trabajar con distintas herramientas (aplicaciones de software), tomando en cuenta las características de

detección, búsqueda y análisis para la base de datos que la herramienta posea, además se debe contemplar factores de costos e inversión como si se tratará de herramientas que impliquen costos económicos para su adquisición y licenciamiento.

b. Análisis de vulnerabilidades: El alcance de la etapa de búsqueda de información competitiva incluye el análisis directo de los datos recopilados. Tal análisis es el resultado que surge de la comprensión de las vulnerabilidades encontradas; las necesidades y perspectivas de investigación de cada analista o investigador, y las prácticas recomendadas y reglamentaciones de seguridad y privacidad relativas al nivel del análisis que el investigador le pueda dar. Sin embargo, el análisis de datos está implícito en la utilización de los "Resultados Esperados" contenidos en la metodología. Es por ello que algunos análisis deben ser llevados a cabo para asegurar como mínimo que los resultados esperados sean satisfechos.

6) Búsqueda y verificación de vulnerabilidades

La búsqueda y verificación vulnerabilidades, está encaminada en poder identificar y comprender cada una de las debilidades y posibles errores en configuraciones, presencia de amenazas y riesgos de seguridad que previo a la realización de los análisis de detección de vulnerabilidades son desconocidos en el servidor de base de datos de la empresa.

a) Informe de mitigación de vulnerabilidades de base de datos: Comprende describir los posibles impactos de seguridad de información que pueden suscitarse y establecer a través de soluciones técnicas y buenas prácticas la prevención y mitigación a cada una de las vulnerabilidades halladas; estos resultados deben presentarse a través de informes, los mismos que permitan la descripción del nombre de la vulnerabilidad, referencia técnica (ejemplo base de datos CVE [Common Vulnerabilities and Exposures / Vulnerabilidades y Exposiciones Comunes]), la descripción o impacto de la misma, así como la recomendación de prevención y mitigación.

7) Testeo de sistemas confiados

El propósito de los testeos de sistemas confiados es analizar la presencia de entidades de confianza, que en el escenario de testeo a veces demuestran ser en realidad amenazas y riesgos de seguridad; que después de realizarse el análisis de seguridad pueden resultar ser sistemas de alto riesgo que conviven en el mismo servidor de la base de datos o que al pesar de ser sistemas totalmente independientes de la base de datos, pueden influir de forma negativa en la seguridad de la misma.

a. Sistemas dependientes de otros sistemas: Debido a que en muchos sistemas dependen unos de otros, en necesario analizar también a estos sistemas o componentes que por convivir en interfaces de red o equipos de hardware cercanos a la base de datos pueden influir en la seguridad de la misma.

b. Tipo de vulnerabilidades que afectan los sistemas de confianza y aplicaciones: Si el análisis y búsqueda de vulnerabilidades se realizó no solo al objetivo principal que es la base de datos sino los sistemas dependientes de la misma, es necesario a más de buscar vulnerabilidades en dichos sistemas realizar el respectico análisis y mitigación de los mismos.

8) Análisis de resultados

Toda la información que se desprende de los procesos de detección de vulnerabilidades, cuando balanceamos de forma detallada y eficiente los tests de seguridad, los resultados van a hablar por sí mismos una y otra vez. En empresas u organizaciones se mira a los resultados de los testeos de seguridad como un arma de costo justificado en su actitud defensiva de seguridad de información, razón por la que esta fase debe ser muy bien elaborada ya que pondrá en manifiesto los resultados de las etapas anteriores de la metodología.

a. Recomendaciones de mitigación: Desde el punto del analista, se pueden determinar recomendaciones que permitan tener una visión sobre las acciones preventivas y correctivas que deberá contemplar para fortalecer la seguridad de la base de datos, así como de los sistemas de confianza que pueden influir en la seguridad de la base de datos.

6.7.1. Implementación de la Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos (DMV-BDD)

1) Revisión de privacidad

La revisión de privacidad es el punto de vista legal y ético que la empresa necesita establecer y que se debe conservar durante el desarrollo de los métodos que se realizan en la metodología implementada.

Para el desarrollo de actividades y análisis de la metodología propuesta, se formalizó la solicitud para realizar en trabajo de investigación en la empresa Automekano Cía. Ltda., de la ciudad de Ambato, en la que el Gerente Regional autorizó y aprobó la investigación. Revisar documentación en el **Anexo 3.**

a. Inspección previa de la base de datos

La base de datos que será analizada se encuentra en un segmento de la red de comunicaciones de la empresa.

El Sistema Gestor de Base de Datos de esquema entidad relación que se utiliza en la empresa es Oracle 10g, que tiene un tamaño de 15 GB, la misma que está implementada sobre un sistema Operativo Linux Oracle. La base de datos empresarial tiene soporte de transacciones, estabilidad, escalabilidad y soporte multiplataforma.

El desarrollo de la metodología propuesta, implica únicamente aspectos de seguridad del sistema de base de datos de la empresa, por lo que no es necesario

conocer esquemas de la base datos, las transacciones que realiza ni el tipo de datos que contiene.

b. Sistemas involucrados en la recolección de datos

Para las etapas de Sondeo de Red e Identificación de Servicios de Sistemas, así como las etapas de Búsqueda de Información Competitiva y Búsqueda y Verificación de vulnerabilidades, es necesario analizar las características de cada herramienta, el alcance de las mismas, además de la facilidad o conocimientos que se tenga para realizar los diferentes análisis y un factor no menos importante es tener presente los costos que implican el uso de las mismas.

- **Herramienta de software para las etapas de Sondeo de Red e Identificación de Servicios de Sistemas**

  ✓ **Kali Linux**

  La herramienta utilizada para las etapas de sondeo de red y la de identificación de servicios de sistemas, es la herramienta de análisis Kali Linux (aplicación de software), la misma que presenta un ambiente usuario root (raíz), ya que está diseñada para trabajar en un ambiente privilegiado de usuario único raíz, lo que facilita empezar el análisis, pues no se necesita escalar privilegios de usuarios para poder trabajar con los comandos de la herramienta.

- **Herramienta de software para las etapas de Búsqueda de Información Competitiva y Búsqueda y Verificación de Vulnerabilidades**

  Para la etapa de testeo de vulnerabilidades de base de datos se pueden utilizar varias herramientas, a continuación describimos algunas:

  ✓ **McAfee Data Center Security Suite for Databases**: Esta herramienta permite la realización de más de 4.700 comprobaciones de vulnerabilidad contra los sistemas principales de bases de datos como Oracle, Microsoft SQL Server, IBM DB2 y bases de datos MySQL. McAfee Vulnerability Manager

para bases de datos, evalúa el riesgo de prácticamente todos los vectores de amenazas con exploración de frecuencia con la que puede detectar amenazas. También es una herramienta que tiene costos de licencias y las versiones de pruebas no están disponibles con las mismas características de análisis.

✓ **Nessus Professional:** Es la solución más usada para las evaluaciones de vulnerabilidad, configuración y compatibilidad. Previene ataques a la red mediante la identificación de vulnerabilidades y problemas de configuración que los piratas informáticos utilizan para penetrar la red. Nessus Professional ayuda a consultores y encargados de analizar intrusiones a:

- Escaneo del rango más amplio de dispositivos de red, sistemas operativos, bases de datos y aplicaciones;
- Detección de amenazas como virus, malware, puertas traseras y servidores que se comunican con sistemas infectados con botnets;
- Informar y comunicar problemas de seguridad en toda la organización mediante informes de solución.

Nessus profesional es una herramienta que tiene costos elevados de licencias anuales y su versión de prueba tiene varias restricciones con las que no se puede realizar búsquedas exhaustivas ni permite analizas los controles de configuración en las bases de datos.

✓ **NeXpose Rapid 7 version Community Edition:** Esta herramienta ayuda a los profesionales a reducir su superficie de ataque al proporcionar información procesable sobre las amenazas reales de vulnerabilidades en toda su infraestructura de TI; evalúa la vulnerabilidad y marca la verificación, además ofrece una gestión unificada de la vulnerabilidad a nivel de empresa, evalúa los riesgos y los informes de cumplimiento de políticas.

El objetivo principal del enfoque global de Rapid7 en la detección de vulnerabilidades con NeXpose, tiene énfasis en la flexibilidad y la facilidad de uso, mientras que la función principal del producto es el control de los sistemas

operativos, servidores, dispositivos de red, bases de datos y aplicaciones web para conocidas o potenciales amenazas de vulnerabilidad.

Además es una de solución de inteligencia frente a riesgos para la seguridad diseñada para particulares y pequeñas empresas, su versión Community permite realizar análisis para empresas pequeñas en las que se contemplen hasta 30 personas que utilizan los servicios de sistemas y aplicaciones tecnológicas. NeXpose es un escáner de vulnerabilidades muy destacado que permite comprender los riesgos para la seguridad presentes en todo el entorno informático, revela amenazas a la seguridad y prioriza las vulnerabilidades que analiza en categorías críticas, severas y moderadas para que se pueda dar solución a las vulnerabilidades según la criticidad de las mismas.

c. Técnicas de obtención de datos

- Testeo de seguridad interno a interno, que permite realizar análisis con la ejecución de pruebas de caja blanca y pruebas de caja gris donde el testeador tiene conocimiento previo de los elementos o del entorno a ser analizado.

- Se cuenta con privilegios de acceso como son las credenciales del usuario administrador de la base de datos, además de tener un entorno privilegiado donde no se tiene que hacer esfuerzos para evadir los componentes de seguridad para realizar el reconocimiento pasivo de red, que permite dejar libre de herramientas de seguridad perimetral el equipo que contiene la base de datos.

- Los métodos utilizados para los testeo de seguridad son pasivos, esto hace posible que se pueda realizar los análisis de testeo en el ambiente real de la base de datos sin la necesidad de detener los servicios en lo referente a la base de datos.

- Las pruebas iniciales de reconocimiento e identificación de servicios y sistemas se realiza con análisis pasivos de red, para esta etapa es necesario que se habilite una ventada de mantenimiento en la empresa.

- No se realizan procesos de análisis en horas laborables, para que se asegure que no nadie más hace uso de los servicios tecnológicos de la empresa para no confundir el ambiente de análisis.

2) Descripción de requisitos

a. Requisitos técnicos para el testeo de seguridad

✓ **Requisitos de hardware (Equipos)**

- Para realizar el análisis de detección de vulnerabilidades
  - Computador portátil marca DELL
    - Procesador Intel(R) Core(TM) i7 3612QM CPU @2.10GHz 2.10 GHz.
    - Memoria RAM 8 GB
    - Disco duro 500 GB
  - Sistema Operativo Windows 7 ultimate 64 bits
  - Conexión a la red empresarial
  - Servicio de internet

- Equipo sobre el que se ejecutará el análisis de detección de vulnerabilidades y hospeda el servidor de base de datos.

  - Servidor HP ProLiant DL380 G6
    - Procesador Intel® Xeon® Quad-Core: E5530 (2.4GHz).
    - Memoria RAM de 32 GB
    - Disco duro SAS 500 GB

  - Sistema Operativo Windows Oracle Linux 2.6.9
  - Conectado en la red empresarial
  - Servicio de internet

- ✓ **Requisitos de Software (Herramientas)**

  Para evitar la adquisición e implementación de recursos e infraestructura tecnológica, se procede a implementar una máquina virtual (Oracle VM Virtual Box) con lo que se puede tener a través de software/hardware una versión virtual de un equipo de cómputo con el sistema Operativo GNU/Linux, interfaz de red, dispositivo de almacenamiento y todos los recursos tecnológicos requeridos para la implementación de las herramientas necesarias (aplicaciones de software) para el sondeo de red e identificación de servicios de sistemas. Previo a un análisis de varias herramientas de testeos y búsqueda, se determina que se trabajaran con dos herramientas de uso libre (Open Source) Kali Linux y NeXpose.

3) Sondeo de red

La primera acción técnica, es realizar un sondeo de la red de comunicaciones que será una actividad principal del método de análisis de seguridad interno a interno; es necesario realizar un reconocimiento pasivo de red en un entorno privilegiado, donde no se tiene que hacer esfuerzos para evadir los componentes de seguridad que permite dejar libre de herramientas de seguridad perimetral al servidor que contiene la base de datos. En esta parte de la investigación no se realizará ningún tipo de intrusión directamente al sistema.

El sondeo de red no es una parte de la Metodología OSSTMM 2.1. (Manual de Metodología Abierta de Testeo de Seguridad), pero para efectos de la investigación y tomando en cuenta el aporte investigativo que brinda, será uno de los punto de partida en la metodología propuesta.

Se realizan varias actividades de testeo de red con la herramienta (aplicación de software) Kali Linux y el uso de varios comandos, por lo que a continuación se describen las actividades realizadas:

a. Análisis de configuración de red

El análisis permite verificar la configuración de las interfaces de red, la tabla de enrutamiento de red IP, la máscara de red, la dirección de broadcast de red, la dirección gateway, la dirección IP de destino y los servidores de DNS.

La revisión del archivo resolv.conf del servidor permite tener acceso al sistema de nombres de dominio de internet (DNS).

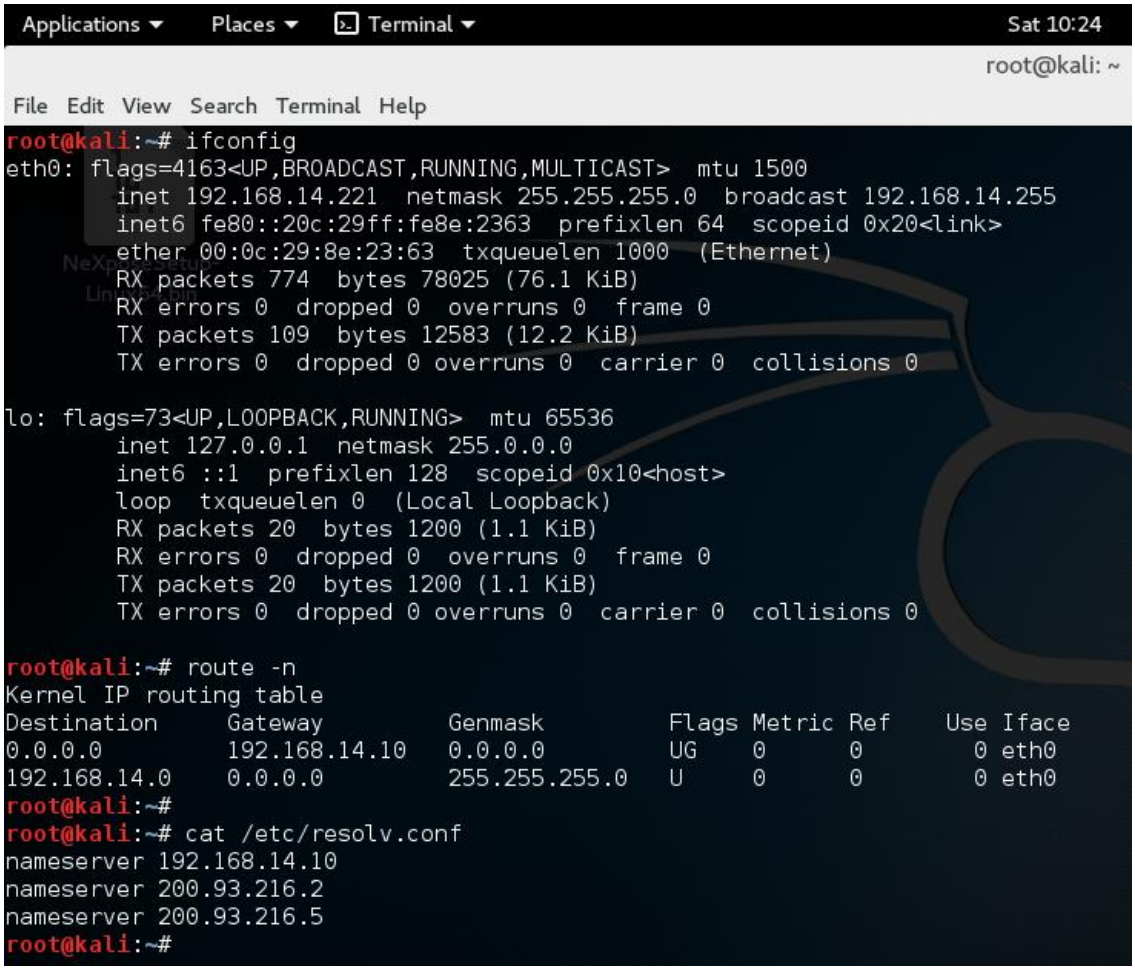


Figura N° 22. Análisis configuración de red

Elaborado por: Investigadora

El análisis de la configuración de red con el uso de los siguientes comandos:

- **ifconfig**.- Permite revisar la configuración de red;
- **route –n**.- Permite visualizar la tabla de enrutamiento de red
- **cat /etc/resolv.conf**.- Proporciona acceso a la información del Sistema de Nombres de Dominio de internet (DNS).

A continuación se describe la información de la configuración de red analizada:

INFORMACIÓN DE CONFIGURACIÓN DE RED			
DATOS	**DIRECCIÓN IP**	**COMANDO**	**ACCIÓN**
IP de red	192.168.14.221	Ifconfig	Permite visualizar y cambiar la configuración de las interfaces de red en su sistema.
Mascara de red	255.255.255.0		
Broadcast de red	192.168.14.255		
Gateway	192.168.14.10	route –n	Permite el acceso a la tabla de enrutamiento de red en formato de direcciones IP.
Destino	192.168.14.0		
Servidores DNS	192.168.14.10	cat /etc/resolv.conf	**cat:** Concatena archivos y los muestra en la salida estándar. **resolv.conf**: Proporciona acceso al Sistema de Nombres de Dominio de internet (DNS).
	200.93.216.2		
	200.93.216.5		

Tabla N° 30. Información de configuración de red

Elaborado por: Investigadora

b. Análisis del DNS del dominio de internet

Con el propósito de reunir la mayor información posible de la red, se ejecutan en la herramienta Kali Linux comandos necesarios para detallar la información del dominio de internet automekano.com, además se ejecuta comandos para descubrir todos los subdominios que apuntan a la misma dirección IP y la información sobre los registros de intercambio de correo.

Figura N° 23. Análisis del DNS del dominio de internet

Elaborado por: Investigadora

Para detallar la información de la Dirección IP del hosts que realiza la función de DNS del dominio de internet de la empresa, se utiliza el comando **dnsenum** automekano.com, comando que además permite enlistar todos los subdominios que apuntan a la misma dirección IP, omitiendo los resultados con 174.142.242.141. El comando dnsenum, permite además visualizar la información del registro de intercambio de correo. A continuación se detalla la información obtenida del análisis:

DNS DE DOMINIOS DE INTERNET			
DATOS	**DIRECCIÓN IP**	**COMANDO**	**ACCIÓN**
IP del host (Registro Dominio)	174.142.242.141	dnsenum automekano.com	Permite detallar la información de un dominio.
DATOS	**DNS**	**DIRECCIÓN IP**	**ACCIÓN**
Nombre de Servidores	dns2.name.services.com	98.124.197.1	Todos los subdominios se apuntan a la misma dirección IP Omitiendo resultados con 174.142.242.141 puede que esté utilizando servidores de OpenDNS.
	dns4.name.services.com	98.124.194.1	
	dns1.name.services.com	98.124.192.1	
	dns5.name.services.com	98.124.196.1	
	dns3.name.services.com	98.124.193.1	
DATOS	**MAIL MX SERVER (Registro de Intercambio de Correo)**	**DIRECCIÓN IP**	**ACCIÓN**
Nombre de Servidores	aspmx4.googlemail.com	74.125.24.26	Información sobre qué servidor de correo usa ese dominio para recibir el correo.
	alt2.aspmx.l.google.com	64.233.190.26	
	aspmx3.googlemail.com	64.233.190.26	
	aspmx5.googlemail.com	74.125.140.26	
	alt1.aspmx.l.google.com	74.125.141.26	
	aspmx2.googlemail.com	74.125.141.26	
	aspmx.l.google.com	74.125.138.27	

Tabla N° 31. DNS del Dominio de Internet

Elaborado por: Investigadora

c. Análisis de mapeo de red

Se realiza una exploración de red para determinar el inventario de servidores que se encuentran habilitados en la red por el puerto SSH (puerto 22), se utiliza el comando NMAP de la herramienta Kali Linux.

SSH por defecto utiliza el puerto 22, por lo que cuando un hacker lanza un ataque lo suele hacer sobre este puerto. Si se procede a cambiar el número del puerto, el servicio no responderá al puerto por defecto y habremos puesto una nueva traba a quien intente conseguir la información de los equipos que se describen en el análisis. En el fichero de configuración se debe cambiar el valor del puerto por el valor de algún otro puerto no muy común, por ejemplo el puerto 10589.

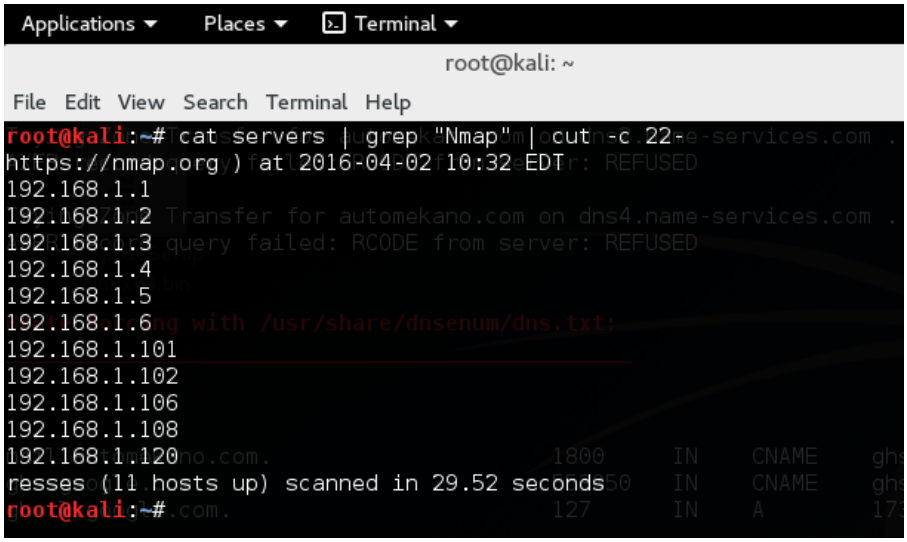


Figura N° 24. Análisis de mapeo de red

Elaborado por: Investigadora

El comando Nmap, permite mapear en la red de la empresa todos los equipos o servidores que tengan configurado el puerto 22 SSH por defecto. Esta información es bastante importante para el Jefe de Sistema de la empresa, ya que estas configuraciones por defecto pueden ser utilizadas para realizar ataques conocidos como el ataque de fuerza bruta que se ejecuta a través del puerto 22. Como se observa en la *Tabla N° 32. Resultados de mapeo de red*, el servidor con la IP

192.168.1.4 que contiene la base de datos también tiene habilitado el puerto 22, lo que representa una posible brecha del seguridad para el mismo. A continuación se describen todos los equipos y servidores de la red de la empresa que se encuentran habilitados el puerto 22.

RESULTADOS DE MAPEO DE RED (PUERTO SSH 22)			
DATOS	**DIRECCIÓN IP**	**COMANDO**	**ACCIÓN**
Dirección de IP Servidores activos a través de SSH	192.168.1.1	cat servers | grep "Nmap" | cut -c 22-	**cat:** Concatena archivos y los muestra en la salida estándar. **grep "Nmap":** Permite buscar, dentro de los archivos, las líneas que concuerdan con el comando Nmap. **cut -c 22-:** Selecciona únicamente las direcciones IP hacia el puerto 22
	192.168.1.2		
	192.168.1.3		
	192.168.1.4		
	192.168.1.5		
	192.168.1.6		
	192.168.1.101		
	192.168.1.102		
	192.168.1.106		
	192.168.1.108		
	192.168.1.120		

Tabla N° 32. Resultados de mapeo de red

Elaborado por: Investigadora

4) Identificación de los Servicios de Sistemas

a. Análisis de los servicios disponibles en los servidores y sus versiones

Para realizar el escaneo de todos los puertos, es necesario no tener la presencia de herramientas de seguridad perimetral (cortafuegos), el análisis permite diferenciar el estado de los puertos, además la revisión de versiones para cada puerto abierto encontrado para tratar de identificar el tipo y la versión de los servicios descubiertos.

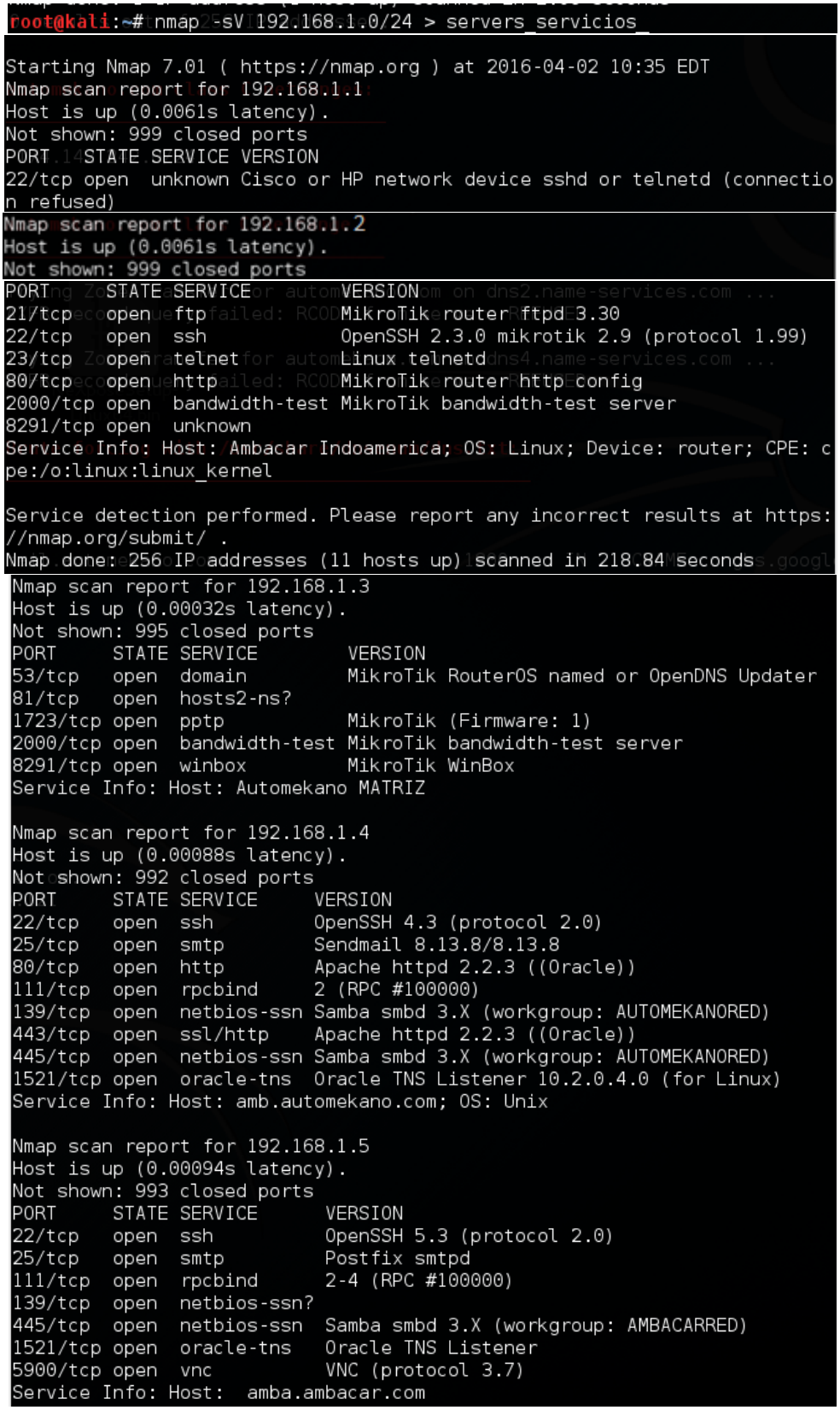


Figura N° 25. Servicios disponibles en los servidores y sus versiones

Elaborado por: Investigadora

La información más relevante del segmento de red analizado 192.168.1.0/24. La información que más se debe poner atención es la que describe el servidor 192.168.1.4 que contiene la base de datos empresarial.

Se puede observar en este análisis que el servidor de la base de datos tiene configurado por defecto el puerto TCP 1521. En las bases de datos Oracle es posible crear una librería y paquetes Procedural Language/Structured Query Language (PL/SQL) que efectúen llamadas a las funciones de cualquier librería del sistema de archivos. De forma remota, un atacante podría efectuar una llamada a system() y pasar el nombre de un programa a ejecutar. Para conseguir sus fines, el usuario malicioso debería ser capaz de conectar con el servidor de bases de datos Oracle y acceder con una cuenta que tenga permisos de CREATE LIBRARY. Sin embargo, es posible engañar al servidor Oracle para que se produzca la carga de librerías arbitrarias y se ejecuten funciones sin necesidad de autenticarse.

Para evitar el mencionado problema se recomienda la creación de una regla en las políticas de seguridad de la herramienta se seguridad perimetral de red (cortafuego), que permita bloquear el puerto 1521 desde Internet.

Los demás puertos que se encuentran habilitados en el servidor 192.168.1.4 que contiene la base de datos también deben ser analizados por parte del personal de Sistemas de la empresa y establecer las reglas de restricción en las política de la herramienta se seguridad perimetral de red (cortafuego), que permita los bloqueos a esos puertos desde internet o contemplar cambios de configuraciones de dichos puertos a unos menos conocidos.

SERVICIOS DISPONIBLES EN LOS SERVIDORES Y SUS VERSIONES					
DATOS	**DIRECCIÓN IP / HOST**	**PUERTO**	**ESTADO**	**SERVICIO**	**VERSIÓN**
Servicios disponibles en los servidores y sus versiones	192.168.1.1	22/tcp	Open	Desconocido	Cisco o HP dispositivo de red sshd o telnetd (conexión denegada)
	192.168.1.2 / Ambacar Indoamerica	21/tcp	Open	ftp	Mikrotik router ftpd 3.30
		22/tcp	Open	Ssh	OpenSSH 2.3.0 mikrotik 2.9
		23/tcp	Open	telnet	Linux telnetd

		80/tcp	Open	http	Mikrotik router http config
		2000/tcp	Open	bandwidth-test	Mikrotik router bandwidth-test server
		8291/tcp	Open	Desconocido	
	192.168.1.3 / Automekano MATRIZ	53/tcp	Open	Domain	Mikrotik RouterOS named or OpenDNS Updater
		81/tcp	Open	hosts2-ns?	
		1723/tcp	Open	Pptp	Mikrotik (Firmware: 1)
		2000/tcp	Open	bandwidth-test	Mikrotik bandwidth-test server
		8291/tcp	Open	Winbox	Mikrotik WinBox
	SERVIDOR DE BASE DE DATOS 192.168.1.4 / amb.automekano.com	22/tcp	Open	Ssh	OpenSHH 4.3 (protocol 2.0)
		25/tcp	Open	Smtp	Sendmail 8.13.8/8.13.8
		80/tcp	Open	http	Apache httpd 2.2.3 ((Oracle))
		111/tcp	Open	Rpcbind	2 (RPC #100000)
		139/tcp	Open	netbios-ssn	Samba smbd 3.X (workgroup: AUTOMEKANORED)
		443/tcp	Open	ssl/http	Apache httpd 2.2.3 ((Oracle))
		445/tcp	Open	netbios-ssn	Samba smbd 3.X (workgroup: AUTOMEKANORED)
		1521/tcp	Open	oracle-tns	Oracle TNS Listener 10.2.0.4.0 (for Linux)
	192.168.1.5 / amba.ambacar.com	22/tcp	Open	Ssh	OpenSHH 5.3 (protocol 2.0)
		25/tcp	Open	Smtp	Postfix smtpd
		111/tcp	Open	Rpcbind	2-4 (RPC #100000)
		139/tcp	Open	netbios-ssn	Samba smbd 3.X (workgroup: AUTOMEKANORED)
		445/tcp	Open	netbios-ssn	Oracle TNS Listener
		1521/tcp	Open	oracle-tns	Oracle TNS Listener
		5900/tcp	Open	Vnc	VNC (protocolo 3.7)

Tabla N° 33. Servicios disponibles en los servidores y sus versiones

Elaborado por: Investigadora

b. Análisis de servidores de nombres de NetBIOS

Se realiza la exploración de la capa de software NetBIOS que permite la comunicación entre la red y los servidores. La dirección de los servidores que ejecutan el servicio NetBIOS en la red y permite identificar los servidores dentro de la red local. Los servidores detectados presentan la información de la dirección IP, nombre NetBIOS, nombre del usuario con la sesión iniciada en el equipo y la dirección MAC.

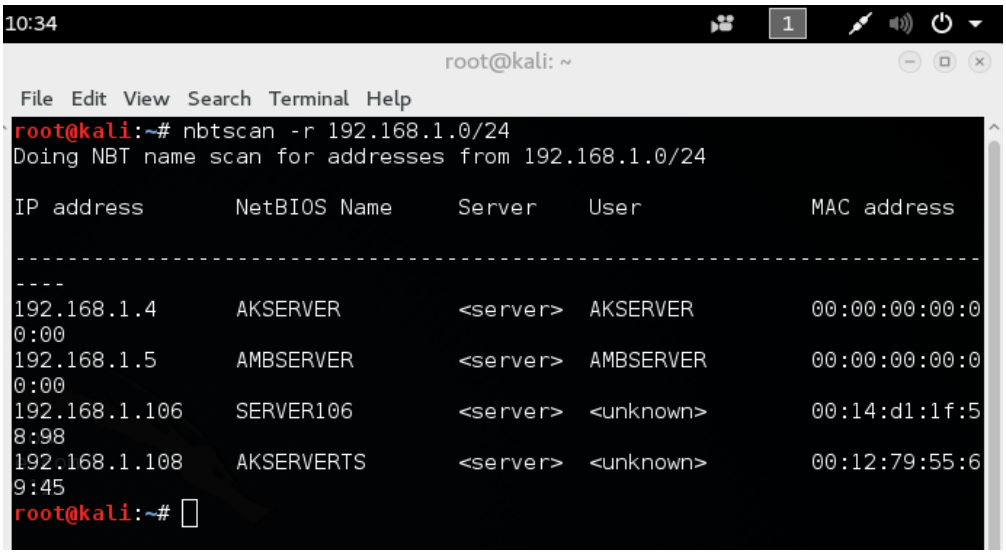


Figura N° 26. Análisis de servidores de nombres de NetBIOS

Elaborado por: Investigadora

El comando nbtscan permite dar a conocer los nombres de NetBIOS, de todos los servidores del segmento de red 192.168.1.0/24. La información que permite conocer el análisis es: las direcciones IP de los servidores, los nombres de host, nombres de usuario y la dirección MAC de los servidores.

NetBIOS sobre TCP/IP (NetBT) es un servicio de red del nivel de sesión que se encarga de asociar los nombres a direcciones IP.

SERVIDORES DE NOMBRES DE NETBIOS					
DATOS	**DIRECCIÓN IP**	**NOMBRE NETBIOS**	**USUARIO**	**DIRECCIÓN MAC**	**COMANDO**
Dirección de IP - Servidores de Nombres de NetBIOS	192.168.1.4	AKSERVER	AKSERVER	00:00:00:00:00	nbtscan -r 192.168.1.0/24
	192.168.1.5	AMBSERVER	AMBSERVER	00:00:00:00:00	
	192.168.1.106	SERVER106	desconocido	00:14:d1:lf:50	
	192.168.1.108	AKSERVERTS	desconocido	00:12:79:55:60	

Tabla N° 34. Servidores de nombres de NetBIOS

Elaborado por: Investigadora

5) Búsqueda de información competitiva

a. Detección de vulnerabilidades de base de datos

La detección de vulnerabilidades de base de datos es una parte fundamental del análisis de seguridad, para efectos de la investigación se trabaja con la herramienta (aplicaciones de software) NeXpose y tomando en cuenta el aporte investigativo que se puede obtener para la base de datos de la empresa Automekano Cía. Ltda.

La instalación de la herramienta de detección de vulnerabilidades en base de datos NeXpose no es parte de la metodología a seguir para la presente investigación.

El análisis de la base de datos está automatizado en la herramienta de análisis NeXpose, para este análisis se necesita la información básica del servidor de la base de datos, para realizar de forma automática la detección de vulnerabilidades de base de datos que comprende un elemento fundamental de la metodología propuesta.

Los *Datos de autenticación de la base de datos* en la herramienta de análisis de seguridad NeXpose, se describen en la siguiente tabla:

CREDENCIALES BASE DE DATOS	
Servicio	Oracle
SID	ORCL
Nombre Usuario	Zeus
Dirección IP	192.168.1.4
Puerto	1521

Tabla N° 35. Credenciales de base datos

Elaborado por: Investigadora

Para iniciar el análisis de seguridad en la herramienta NeXpose, se necesita ingresar la información de la base de datos como: nombre del servicio, el SID (instancia de la base de datos mediante la cual se conecta a esta), el nombre del usuario administrador y la contraseña.

Las demás credenciales para el testeo de seguridad es la Dirección IP del servidor donde está alojada la base de datos (192.168.1.4) y el puerto escucha Oracle Listener 1521/TCP. Cabe indicar que se dio a conocer el puerto 1521 en la etapa Identificación de los Servicios de Sistemas de la metodología propuesta.

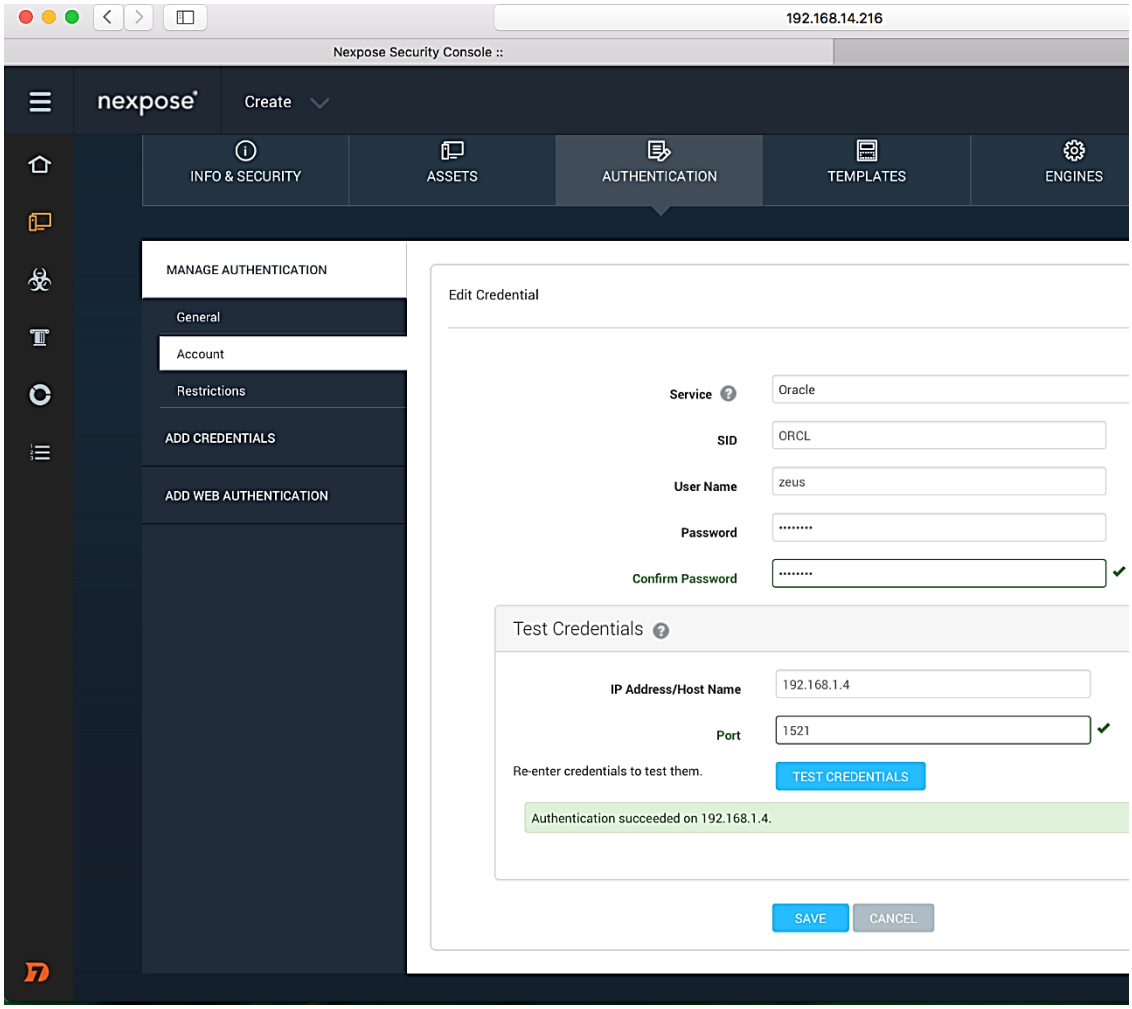


Figura N° 27. Autenticación a la base de datos

Elaborado por: Investigadora

La *Información y seguridad – General* de la herramienta de análisis de seguridad NeXpose, requiere que se identifique con un nombre al análisis a realizar.

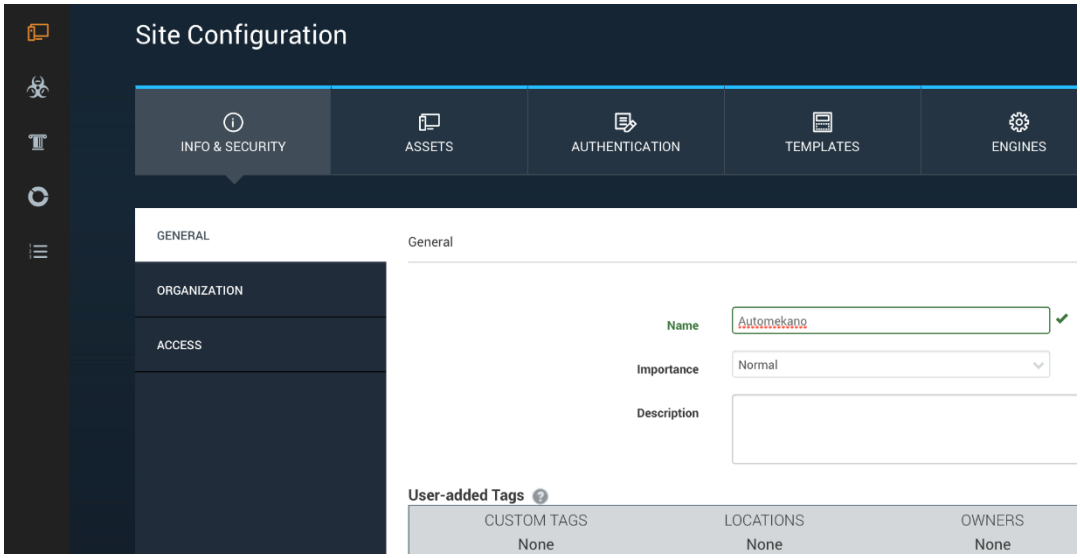


Figura N° 28. Información y seguridad – General

Elaborado por: Investigadora

Otra etapa de la configuración inicial para establecer el análisis de seguridad es la identificación de Activos. El activo a analizar en este caso es el servidor de la base de datos, por lo que es necesario que se ingrese la dirección IP del servidor de la base de datos 192.168.1.4

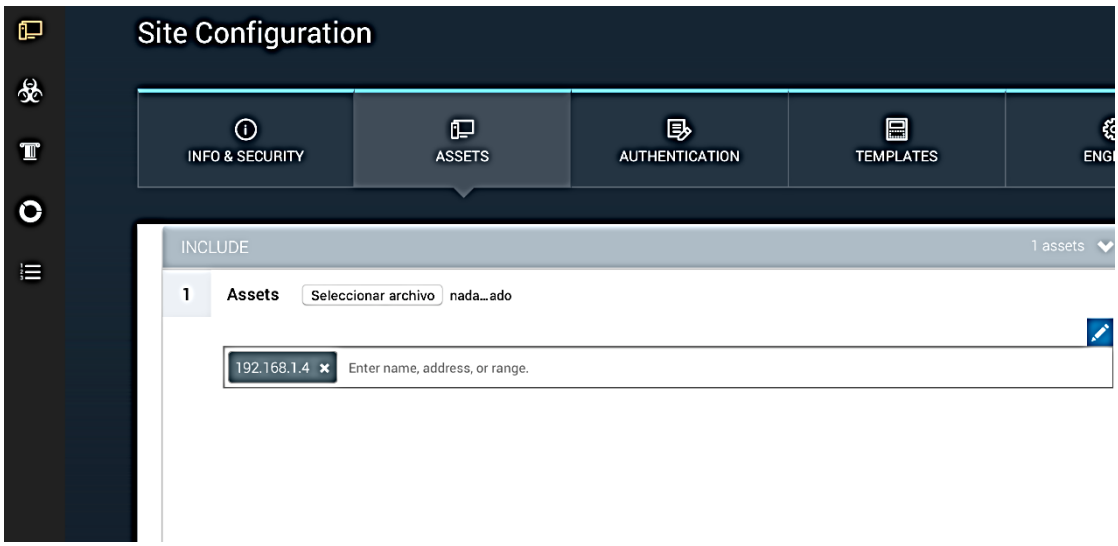


Figura N° 29. Identificación de Activos

Elaborado por: Investigadora

La *Administración de autenticación*, de forma automática establece el nombre de la base de datos que se encuentra alojada en el servidor antes especificado (192.168.1.4). A continuación se describe en la tabla y en la figura la información respectiva.

CREDENCIALES DE ESCANEO	
Habilitado	Si
Nombre	DB_Credential
Servicio	Oracle
Rango	Sitio especifico
Nombre de usuario	Zeus

Tabla N° 36. Administración de autenticación

Elaborado por: Investigadora

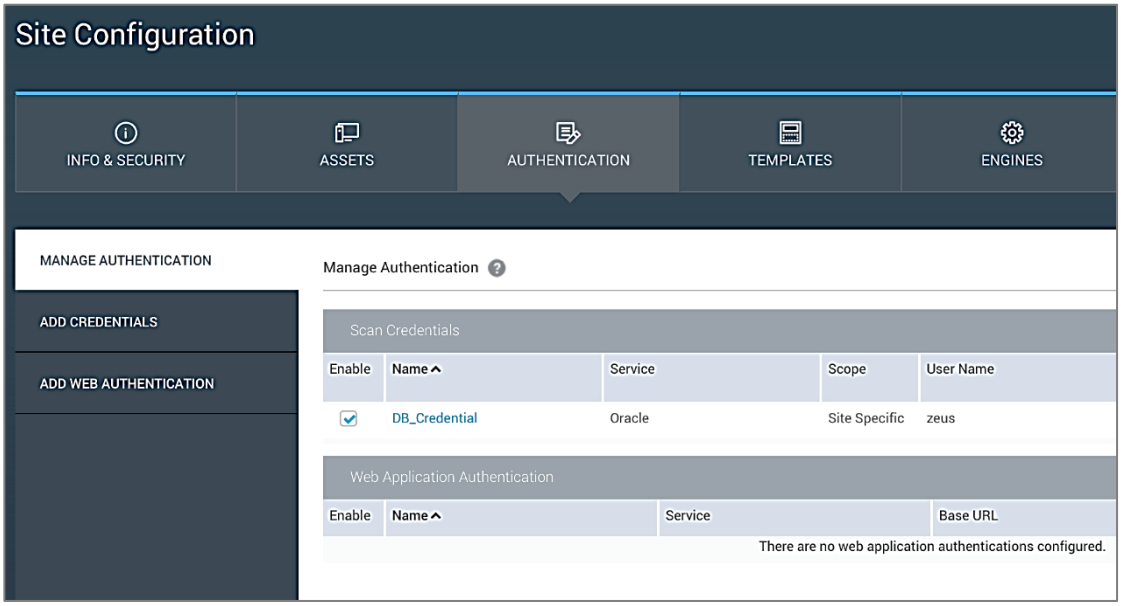


Figura N° 30. Administración de autenticación

Elaborado por: Investigadora

Se establece la platilla de auditoría completa para contar con la mayor información posible del análisis de la base de datos. Se determina la plantilla Full Audit.

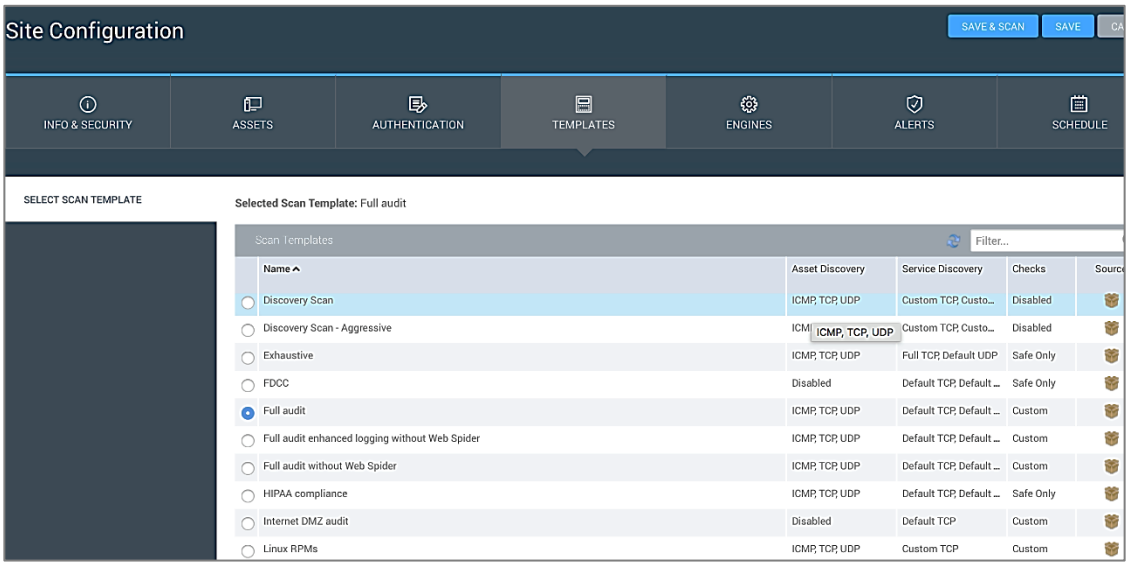


Figura N° 31. Selección de planilla de escaneo

Elaborado por: Investigadora

Se selecciona el motor de análisis local para que se inicie el análisis del activo ya antes configurado, para obtener los resultados de la etapa de detección de vulnerabilidades de base de datos.

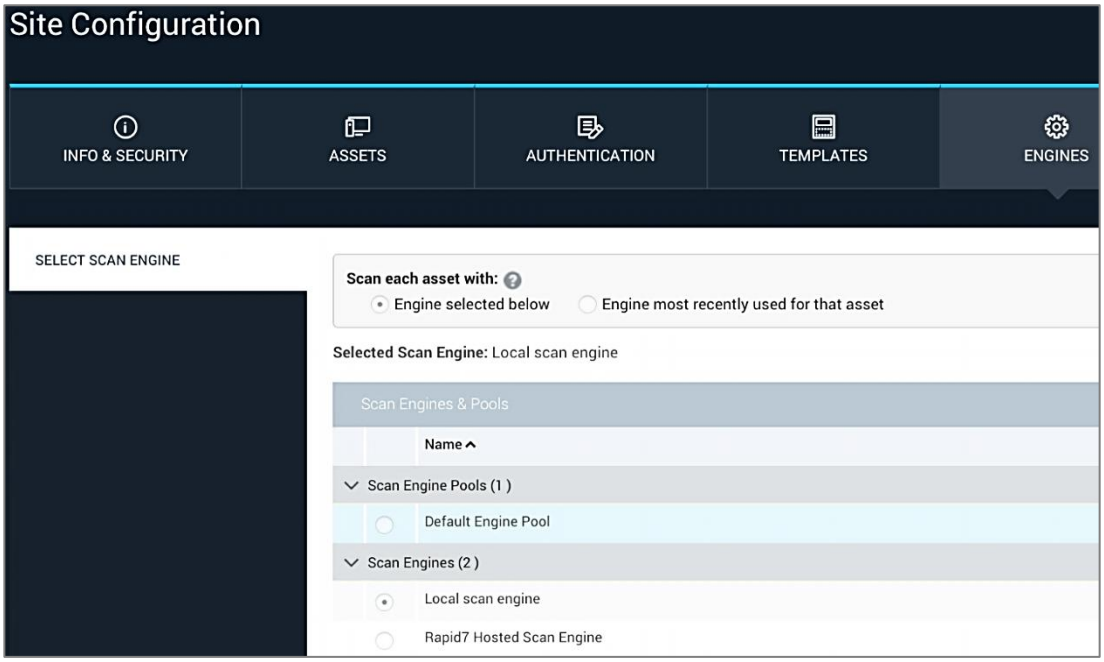


Figura N° 32. Selección de motor de análisis

Elaborado por: Investigadora

La *Visualización de los procesos de análisis*, permite visualizar todos los escaneos y se visualiza todas las vistas para procesar los resultados de la detección de vulnerabilidades de base de datos.

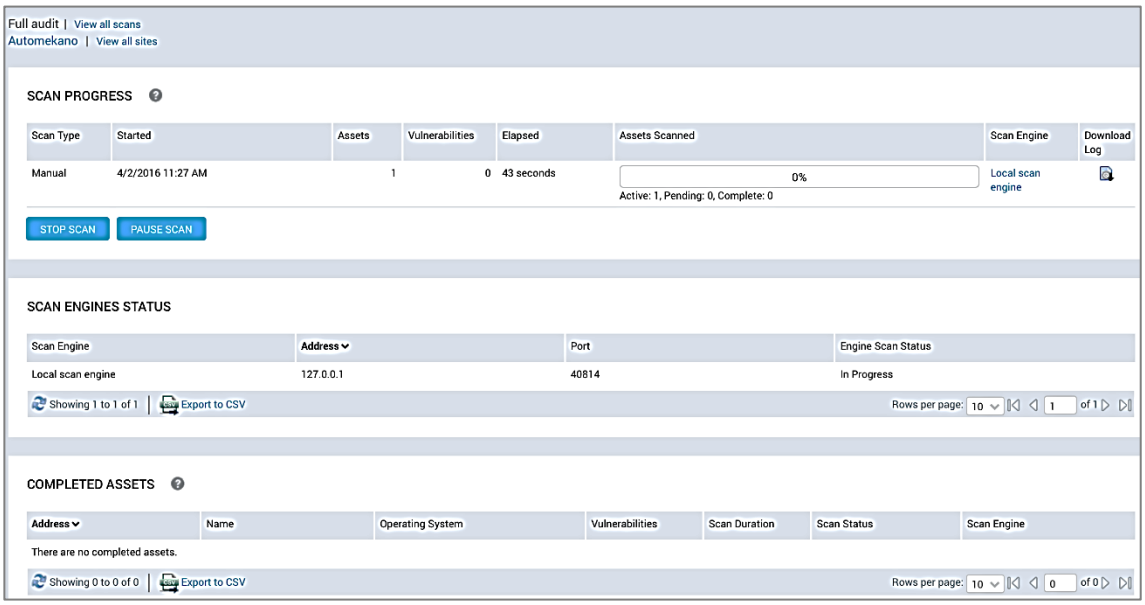


Figura N° 33. Visualización de los procesos de análisis

Elaborado por: Investigadora

La herramienta (aplicación de software) NeXpose permite crear el reporte de los resultados del testeo de vulnerabilidades, para lo que se elige el tipo de reporte Audit Report, el mismo que proporciona información completa sobre activos descubiertos con sus vulnerabilidades, para posteriormente realizar el análisis y verificación de la gran cantidad de información probada y que pertenece a muchos de los niveles de lo que se considera seguridad de la información. La cantidad de información obtenida, no siempre significa ser la información clave del rompecabezas que es el análisis mitigación de las vulnerabilidades halladas.

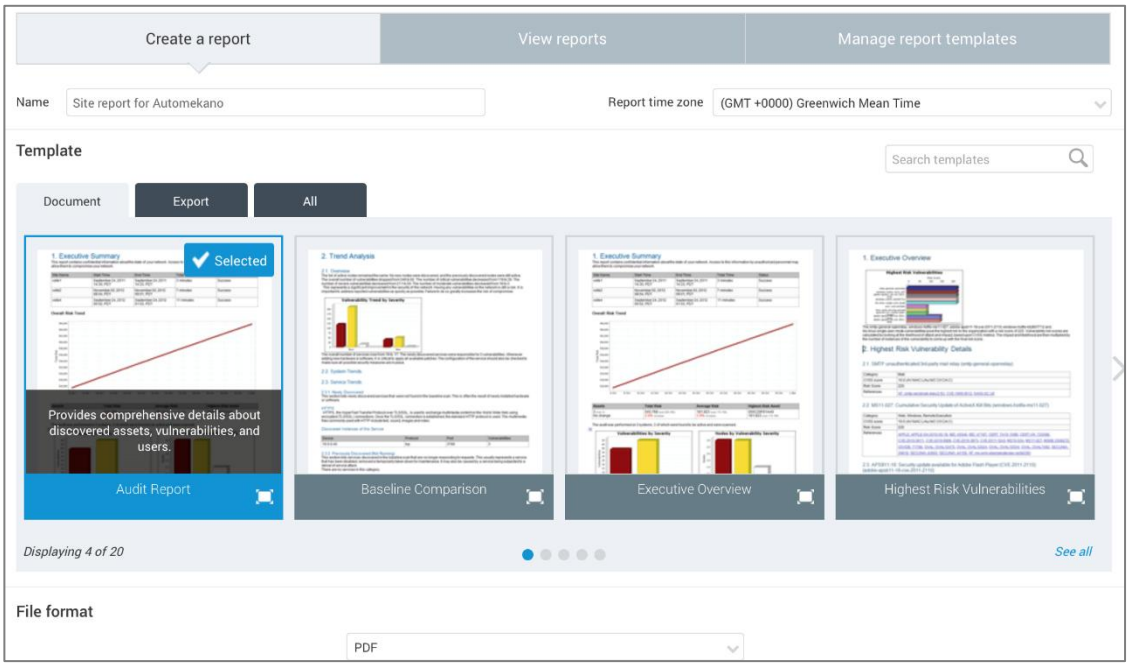


Figura N° 34. Creación de un reporte

Elaborado por: Investigadora

El informe de auditoría para el activo 192.168.1.4 (Dirección IP de servidor de base de datos) que se genera en archivo digital en formato PDF, contiene el detalle de cada una de las vulnerabilidades detectadas con la herramienta de análisis NeXpose, el archivo generado contiene 210 páginas, para optimizar la presente investigación se presentará únicamente el Resumen Ejecutivo y los Sistemas Descubiertos en el **Anexo 4**, las demás paginas serán analizadas y descritas en el Informe de Análisis y Mitigación de Vulnerabilidades de Base de Datos.

b. Análisis de Vulnerabilidades

El informe representa una auditoría de seguridad realizada por NeXpose de Rapid7, la misma que revela que no hay suficientes datos históricos para mostrar la tendencia de riesgo puesto que la auditoría se llevó a cabo en un sistema que se encuentra activo.

Según el resumen ejecutivo la figura principal de Vulnerabilidades de Severidad que detallan la siguiente información:

Existen 83 vulnerabilidades encontradas durante la exploración las mismas que se detallan a continuación:

- **7 resultaron vulnerabilidades críticas:** Las vulnerabilidades críticas requieren inmediata atención, estas hacen que sea relativamente fácil para los atacantes explotar una vulnerabilidad crítica y pueden proporcionarles el control total de los sistemas afectados.
- **61 vulnerabilidades fueron graves:** Las vulnerabilidades graves son a menudo más difíciles de explotar y no pueden proporcionar el mismo acceso a los sistemas afectados.
- **15 vulnerabilidades moderadas descubiertas:** Estas a menudo proporcionan información a los atacantes que pueden ayudar en el montaje ataques posteriores en la red.

Las vulnerabilidades críticas y graves serán tratadas en la presente investigación, a pesar que las vulnerabilidades moderadas también deben fijarse de manera oportuna, pero no son tan urgentes como las otras vulnerabilidades; ya que son vulnerabilidades que los posibles ataques podrían realizarse posteriores a la red de comunicaciones.

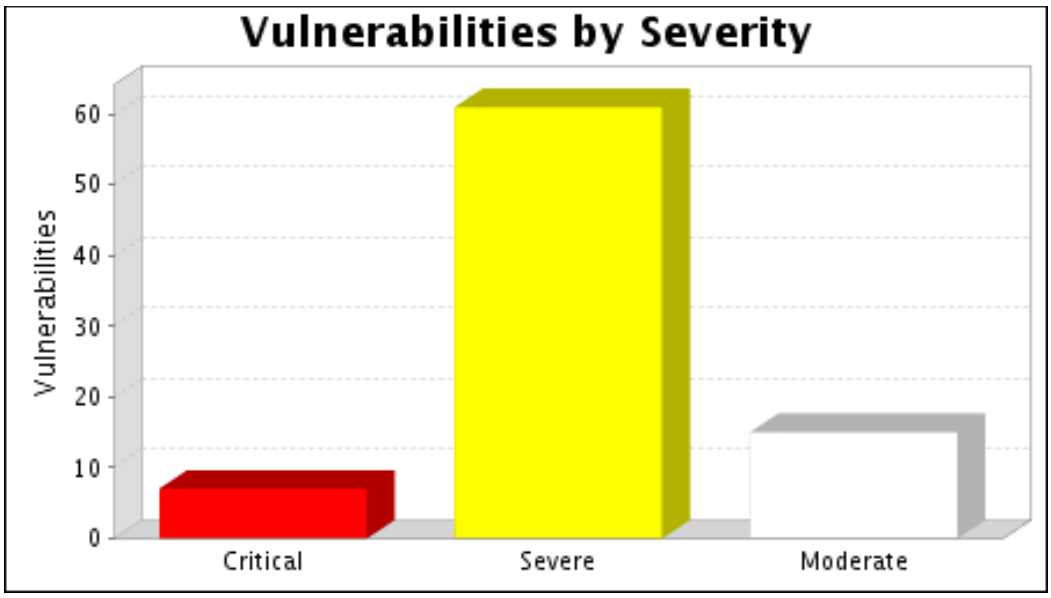


Figura N° 35. Vulnerabilidades Severas

Elaborado por: Investigadora

a. Vulnerabilidades Críticas

Las vulnerabilidades críticas que se hallaron en el análisis al servidor de la base de datos (dirección IP 192.168.1.4) son las que se describen detalladamente en el **Anexo 5.** *Informe de Mitigación de Vulnerabilidades Críticas*, las mismas que requieren inmediata atención, ya que este tipo de vulnerabilidades hacen que sea relativamente fácil para los atacantes explotarse y de no realizarse las acciones de prevención y mitigación posiblemente se podría presentar las siguientes consecuencias:

- Interrupción del servicio;
- Divulgación no autorizada de información;
- Modificación no autorizada de información;
- Versiones obsoletas de Oracle pueden ser vulnerables.
- Proporcionar acceso no autorizado;
- Posible pérdida parcial de la confidencialidad;
- Posible violación de integridad y disponibilidad;
- Proporcionar acceso a cuentas de usuario.

Se realiza un análisis estadístico de las vulnerabilidades críticas detectadas el 29% corresponden a vulnerabilidades en el sistema operativo Linux, el mismo que contiene la base de datos empresarial; el 14% corresponde a vulnerabilidades de la base de datos Oracle; el 43% son las vulnerabilidades que se encontró el servidor Apache HTTPD que se encuentra implementado en el mismo servidor donde reside la base de datos y finalmente el 14% determinan las vulnerabilidades del servidor de correo Sendmail SMTP que también ha sido implementado en el servidor que tiene la implementación del Sistema de Base de datos.

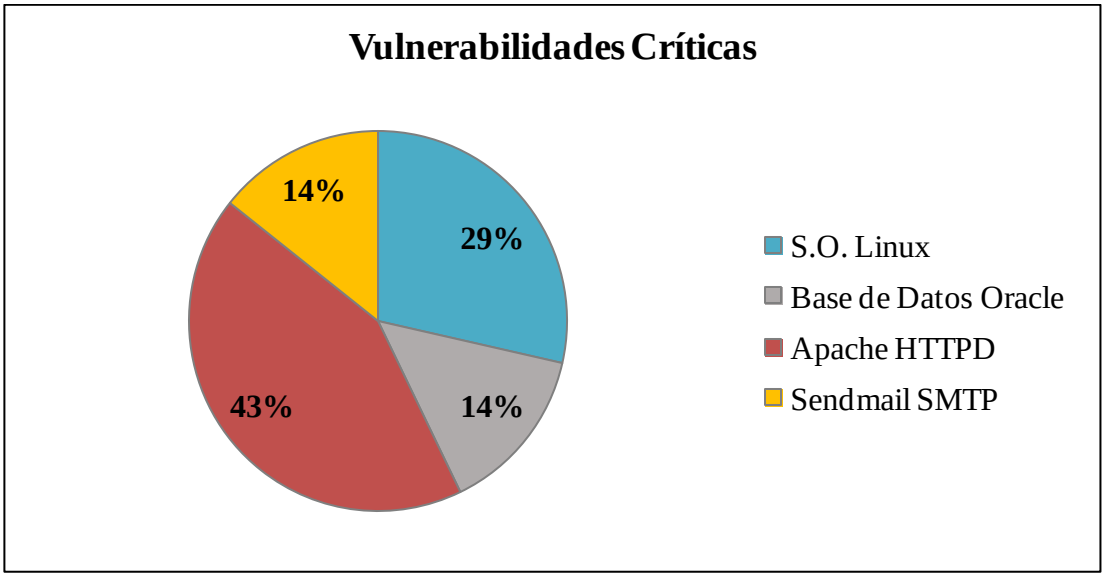


Figura N° 36. Vulnerabilidades Críticas

Elaborado por: Investigadora

b. Vulnerabilidades Graves

Las vulnerabilidades graves son a menudo más difíciles de explotar y no pueden proporcionar el mismo acceso a los sistemas afectados. A continuación, se analiza y se presenta las vulnerabilidades graves con sus impactos, referencias, descripciones y acciones de mitigación, las mismas que se han agrupado por tipo de servicio e impacto, además por tipo de mitigación ya que muchas se solucionan aplicando una acción de mitigación específica. La revisión de las vulnerabilidades detectadas que se consideran graves se describe a detalle en el **Anexo 6** *Informe de Mitigación de Vulnerabilidades Graves.*

Se realiza un estudio estadístico para determinar los porcentajes de las vulnerabilidades graves, es así que el Sistema Operativo Linux donde reside el Sistema de la Base de Datos tiene un 6% de vulnerabilidades detectadas; el 2% determina las vulnerabilidades que se detectaron a nivel de base de datos; el porcentaje más amplio es el que determina las vulnerabilidades detectadas en el Servidor de Apache HTTPD y un porcentaje de menos de 1% pertenece a al servidor de Sendmail SMTP. Los servicios de Apache HTTPD y Sendmail SMTP son servicios que residen en el servidor que contiene la base de datos.

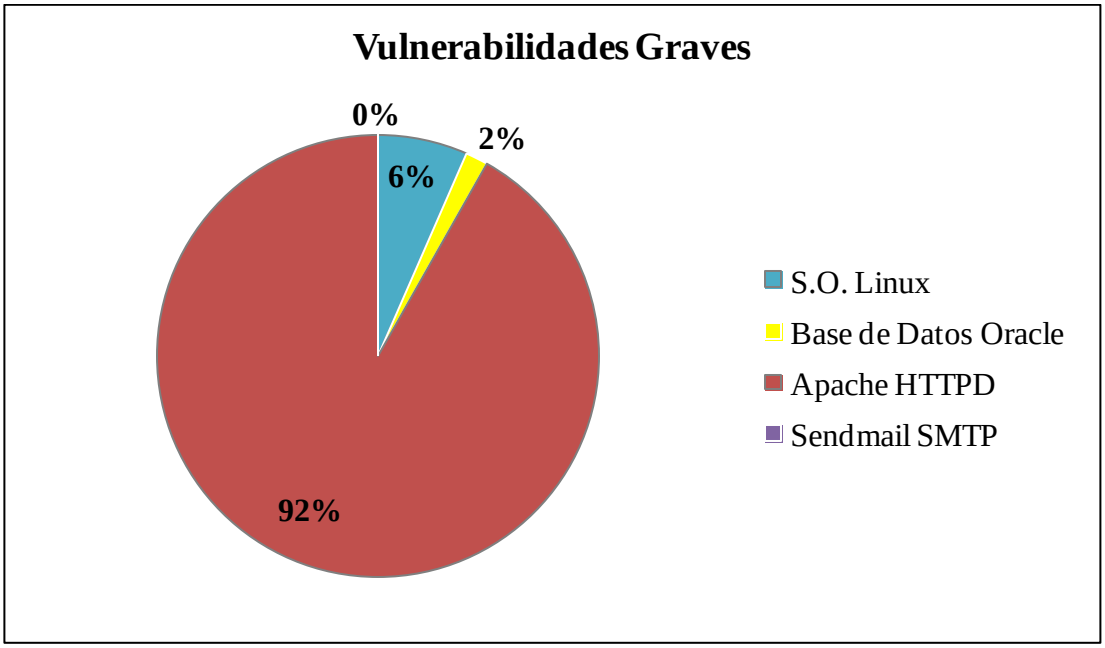


Figura N° 37. Vulnerabilidades Graves

Elaborado por: Investigadora

6) Búsqueda y verificación de vulnerabilidades

a. Informe de mitigación de vulnerabilidades de base de datos

La búsqueda y verificación vulnerabilidades identifica y comprende cada una de las debilidades y errores que eran desconocidos en el servidor de base de datos de la empresa Automekano Cía. Ltda.; el objetivo principal es la descripción de los posibles impactos de seguridad de información que pueden suscitarse y establecer a través de soluciones técnicas y prácticas la prevención y mitigación a cada una de las vulnerabilidades halladas; además de presentar los resultados a través de los informes de mitigación de vulnerabilidades críticas y graves.

- **Base de Datos Oracle (Versión obsoleta)**

El servidor de base de datos Oracle se ejecuta sobre una version obsoleta. Oracle sólo produce correcciones correspondientes a los últimos niveles de parches dentro de cada versión del producto. Por lo tanto, si el servidor se ejecuta en un conjunto de

modificaciones mayores, los parches de seguridad críticos no pueden aplicarse sin primero actualizar a un conjunto de parches más reciente. La versión de la Base de Datos Oracle 10.2.0.4, puede presentar vulnerabilidades, las mismas que se describen y se presenta las respectivas recomendaciones de prevención y mitigación.

INFORME DE MITIGACIÓN DE VULNERABILIDADES DE BASE DE DATOS	
DATOS TÉCNICOS	**Host y puerto afectado:** 192.168.1.4:1521 Ejecutar Oracle TNS Listener de la Base de datos Oracle 10.2.0.4 (versión vulnerable)
TIPO DE IMPACTO	**CRÍTICO:** Las versiones obsoletas de Oracle pueden ser vulnerables.
DESCRIPCIÓN	La Base de Datos de Oracle podría ser vulnerables a los ataques de desbordamiento de búfer, inyección SQL, ataques TNS Listener, ataques de cross-site scripting, y los ataques de recorrido de directorio (directory traversal).
REFERENCIA	http://www.oracle.com/support/library/brochure/lifetime-support-technology.pdf#page=6 http://www.oracle.com/us/support/lifetime-support/index.html
MITIGACIÓN	Es muy recomendable que actualice un parche o una instalación de Base de Datos Oracle con las últimas actualizaciones disponibles.
DATOS TÉCNICOS	Vulnerabilidad fue encontrada en Oracle Database 10.2.0.3/10.2.0.4/10.2.0.5/11.1.0.7/11.2.0.1 Función **mdsys.reset_inprog_index() SQL INJECTION**
TIPO DE IMPACTO	**CRÍTICO**
DESCRIPCIÓN	La Base de Datos de Oracle podría ser vulnerables a los ataques de desbordamiento de búfer, inyección SQL, ataques TNS Listener, ataques de cross-site scripting, y los ataques de recorrido de directorio (directory traversal).
REFERENCIA	https://vuldb.com/es/?id.4247 SecurityFocus (BID 45855), X-Force (64760), Secunia (SA42895), SecurityTracker (ID 1024972) y Vulnerability Center (SBV-29225)
MITIGACIÓN	Una actualización elimina esta vulnerabilidad. Aplicando un parche es posible eliminar el problema. El parche puede ser descargado de oracle.com. El mejor modo sugerido para mitigar el problema es actualizar a la última versión.
DATOS TÉCNICOS	Oracle Database 10.2.0.3/10.2.0.4/10.2.0.5/11.1.0.7/11.2.0.2 **Enterprise Manager Base Platform vulnerabilidad desconocida.**
TIPO DE IMPACTO	**CRÍTICO:** Las versiones obsoletas de Oracle pueden ser vulnerables.
DESCRIPCIÓN	La vulnerabilidad es identificada como CVE-2012-0520. El ataque se puede hacer desde la red. La explotación no necesita ninguna autentificación específica. No se conoce los detalles técnicos ni hay ningún exploit disponible. Permite a atacantes remotos afectar la integridad a través de vectores desconocidos relacionados con el Framework.
REFERENCIA	https://vuldb.com/es/?id.5093 SecurityFocus (BID 53081), Secunia (SA48855) y SecurityTracker (ID 1026929).

MITIGACIÓN	Aplicando un parche es posible eliminar el problema. El parche puede ser descargado de oracle.com. Una solución posible ha sido publicada inmediatamente después de la publicación de la vulnerabilidad.
DATOS TÉCNICOS	Base de Datos Oracle 10.2.0.3/10.2.0.4/10.2.0.5/11.1.0.7 **Enterprise Manager Base Platform /em/console/logon/logon autenticación débil**
TIPO DE IMPACTO	**CRÍTICO**
DESCRIPCIÓN	Una función desconocida del archivo */em/console/logon/logon* del componente *Enterprise Manager Base Platform* es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase autenticación débil. Esto tiene repercusión sobre la confidencialidad e integridad. La vulnerabilidad es identificada como CVE-2012-0528. El ataque se puede hacer desde la red. La explotación no necesita ninguna autentificación específica. Los detalles técnicos así como un exploit privado son conocidos.
REFERENCIA	https://vuldb.com/es/?id.5105 Secunia (SA 48855) y SecurityTracker (ID 1026929).
MITIGACIÓN	Aplicando un parche es posible eliminar el problema. El parche puede ser descargado de oracle.com. Una solución posible ha sido publicada inmediatamente después de la publicación de la vulnerabilidad.
DATOS TÉCNICOS	**Oracle Database 10.2.0.4/11.1.0.7 OCIPasswordChange API escalada de privilegios**
TIPO DE IMPACTO	**CRÍTICO**
DESCRIPCIÓN	Una función desconocida del componente *OCIPasswordChange API* es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase escalada de privilegios. Esto tiene repercusión sobre la confidencialidad e integridad. La vulnerabilidad es identificada como CVE-2012-0511. Se considera fácil de explotar. El ataque puede ser iniciado desde la red. La explotación no requiere ninguna forma de autentificación. No son conocidos los detalles técnicos, pero hay un exploit privado disponible.
REFERENCIA	https://vuldb.com/es/?id.5084 Secunia (SA 48855) y SecurityTracker (ID 1026929).
MITIGACIÓN	Aplicando un parche es posible eliminar el problema. El parche puede ser descargado de oracle.com. Una solución posible ha sido publicada inmediatamente después de la publicación de la vulnerabilidad.

Tabla N° 37. Informe de Mitigación de Vulnerabilidades de Base de Datos

Elaborado por: Investigadora

Oracle corrige 86 vulnerabilidades en su actualización de seguridad de enero 2013.

El primer boletín de seguridad para Oracle, de los cuatro de frecuencia trimestral que tiene planificado para 2013, contiene **parches para 86 vulnerabilidades** diferentes en múltiples productos.

A continuación se describen las 86 vulnerabilidades que pueden ser corregidas con la actualización:

	CORRECCIÓN DE VULNERABILIDADES CON LA ACTUALIZACION	
#	VULNERABILIDAD	DESCRIPCIÓN
6	**Oracle Database**	La primera de ellas afecta a Database Server y permite al atacante tomar el control del sistema. Aunque es explotable de forma remota y la complejidad de explotación es baja, la necesidad de autenticación simple y de poseer privilegios para la creación de tablas reduce su puntuación CVSS a 9 en sistemas Windows. Para sistemas *NIX, esta puntuación es menor (6,5), ya que el compromiso del sistema es sólo parcial.
7	**Fusion Middleware**	Existen 5 de las 7 vulnerabilidades de ese tipo que son explotables remotamente sin autenticación. Entre estas, 3 comprometen la disponibilidad y 2 la integridad del sistema. Las otras 2 son denegaciones de servicio solo explotables de manera local. Todas comprometen el sistema solo parcialmente.
13	**Enterprise Manager Grid Control**	Todas afectan al protocolo http y son explotables de forma remota sin necesidad de autenticación. Se debe poner especial atención a la vulnerabilidad CVE-2013-0359, que puede provocar el compromiso parcial de la confidencialidad, integridad y disponibilidad del sistema. El resto solo afectan también parcialmente a la integridad.
9	**E-Business Suite**	Existen 4 vulnerabilidades relacionadas con la disponibilidad del sistema y 2 de ellas explotables de forma remota.
1	**Oracle Supply Chain**	Esta se aloja en el componente Oracle Agile PLM Framework, en el protocolo HTTP y con baja puntuación CVSS (2,1) en parte debido a su alta complejidad de acceso, su necesidad de autenticación y su bajo impacto (parcial para la confidencialidad).
12	**PeopleSoft**	Todas relacionadas con el protocolo HTTP y 7 de ellas pueden

		explotarse de forma remota sin necesidad de credenciales, suponiendo estas en su mayoría un compromiso parcial de la integridad del sistema.
1	**Oracle JD Edwards**	De importancia baja y no explotable remotamente, supone solo un compromiso parcial de la confidencialidad.
10	**Siebel CRM (10)**	Todas relacionadas con el protocolo HTTP y la mitad de ellas explotables remotamente sin autenticación. Principalmente del tipo denegación de servicio o revelación de información.
8	**Oracle Sun Products**	Siendo 7 para Solaris, explotables solo de manera local. De estas, tres implican un compromiso total del sistema. La restante afecta al Common Array Manager y es explotable a través de la red sin necesidad de credenciales, pudiendo ser utilizada para revelar información sensible.
1	**Oracle Virtualization**	De puntuación baja y que afecta a la aplicación de virtualización Virtual Box. Solo explotables localmente.
18	**Oracle MySQL Product Suite**	En su mayoría denegaciones de servicio que podrían afectar solo a la aplicación o al sistema al completo. Destacan las vulnerabilidades CVE-2012-5611 y CVE-2012-5612, que podrían provocar un compromiso total del sistema en Windows (parcial en *nix, con una puntuación CVSS de 6,5).
86	**TOTAL**	

Tabla N° 38. Vulnerabilidades corregidas con la actualización de Base de Datos Oracle

Elaborado por: Investigadora

Los productos que reciben estas actualizaciones se encuentran en el siguiente listado:

Base de datos Oracle

Oracle Database 11g Release 2, versiones 11.2.0.2, 11.2.0.3

Oracle Database 11g Release 1, versión 11.1.0.7

Oracle Database 10g Release 2, versiones 10.2.0.3, **10.2.0.4**, 10.2.0.5

Oracle Database Mobile Server, versión 11.1.0.0

Oracle Database Lite Server, versión 10.3.0.3

7) Testeo de sistemas confiados

a. Sistemas dependientes de otros sistemas

Se trabajó con las herramientas de testeo y análisis de vulnerabilidades Kali Linux y NeXpose que son de tipo Open Source (de uso libre) que no necesitan inversión económica en adquisiciones de licencias de propiedad y uso, facilitando así la realización de la presente propuesta, dichas herramientas se utilizan para análisis de tipo auditoría de seguridad.

Se realizó los análisis de detección de vulnerabilidades al servidor Oracle Linux (Dirección IP: 192.168.1.4), el mismo que aloja la Base de Datos - Oracle Database versión 10.2.0.4, adicionalmente se tiene alojado un servidor de aplicaciones Apache HTTPD versión 2.2.3 y un servicio de correo Sendmail versión 8.13.8.

El servicio de Apache y Sendmail, fueron implementados en el servidor que contiene la base de datos pero nunca fueron utilizados, sin embargo al encontrarse implementados no dejan de ser un posible problema de seguridad para la Base de Datos.

El sistema ZEUS - ERP, es un software que tiene su propia gestión Web con que la empresa puede gestionar todos los procesos administrativos, por lo que no fue necesario el uso de un servicio web como Apache.

Para la emisión de comprobantes electrónicos se utiliza un módulo que presenta en formato XML los comprobantes, a través del paquete UTL_SMTP de Oracle que está diseñado para el envío de correos electrónicos (emails) sobre Simple Mail Transfer Protocol (SMTP),este paquete UTL_SMTP proporciona interfaces para los comandos SMTP además que para muchos de los comandos proporciona tanto una interfaz de procedimiento como una interfaz funcional; es por esto que el servicio de Sendmail que se detectó implementado en el servidor que contiene la base de datos no tiene funcionalidad alguna, pero si puede ser origen de posibles amenazas y riesgos de seguridad para la base de datos. En la *Figura N° 38. Emisión de Comprobantes Electrónico,* se explica el proceso del sistema ZEUS - ERP y la base de datos.

DIAGRAMA FUNCIONAL DE LA EMISIÓN DE COMPROBANTES ELECTRÓNICOS

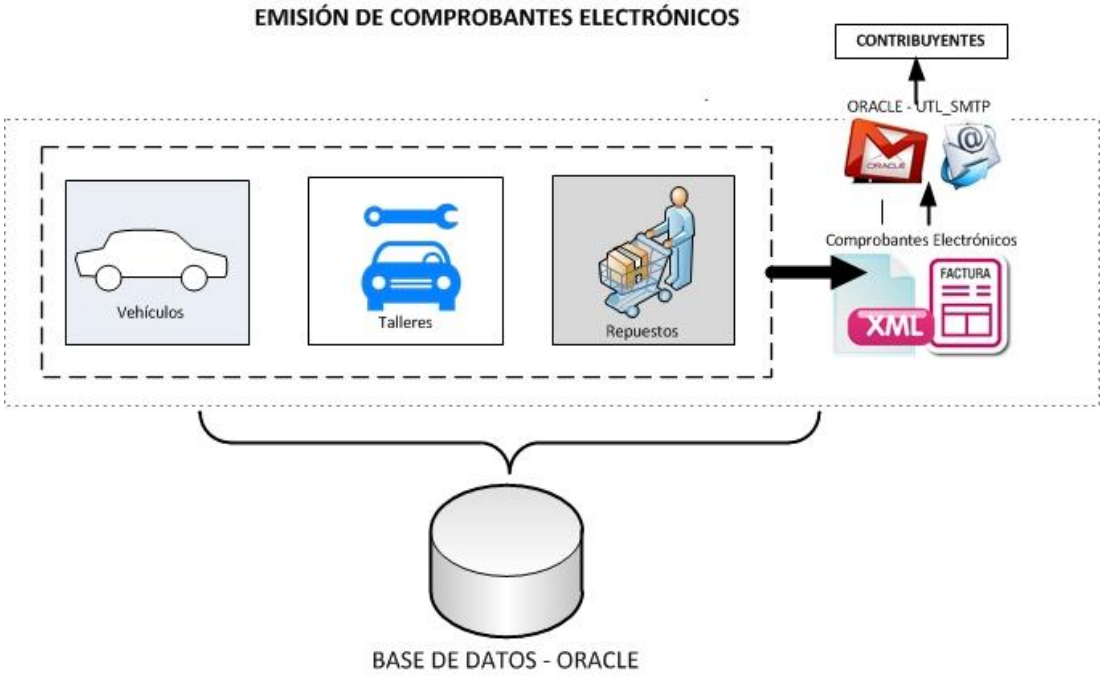


Figura N° 38. Diagrama Funcional de la Emisión de Comprobantes Electrónicos

Elaborado por: Investigadora

De no eliminarse los servicios de Apache y Sendmail del servidor que contiene la base de datos, y más aún de ser necesario mantener la implementación de varios servicios en el mismo servidor debe contemplarse una implementación de virtualización que puede aplicarse para lograr la independencia lo los servidores de base de datos Oracle Database, servidor de aplicaciones Web Apache HTTPD y el servidor de correo Sendmail; que ahora se encuentran alojados en un solo servidor físico. Con la virtualización se puede lograr trabajar de forma independiente los temas de análisis de detección de vulnerabilidades, así como trabajar en la mitigación, aseguramiento y fortalecimiento de cada uno de los servidores de forma independiente como se muestra en la *Figura N° 38. Implementación actual* -

Implementación recomendad, de esta forma además las vulnerabilidades de otros servidores no atentarían a la base de datos.

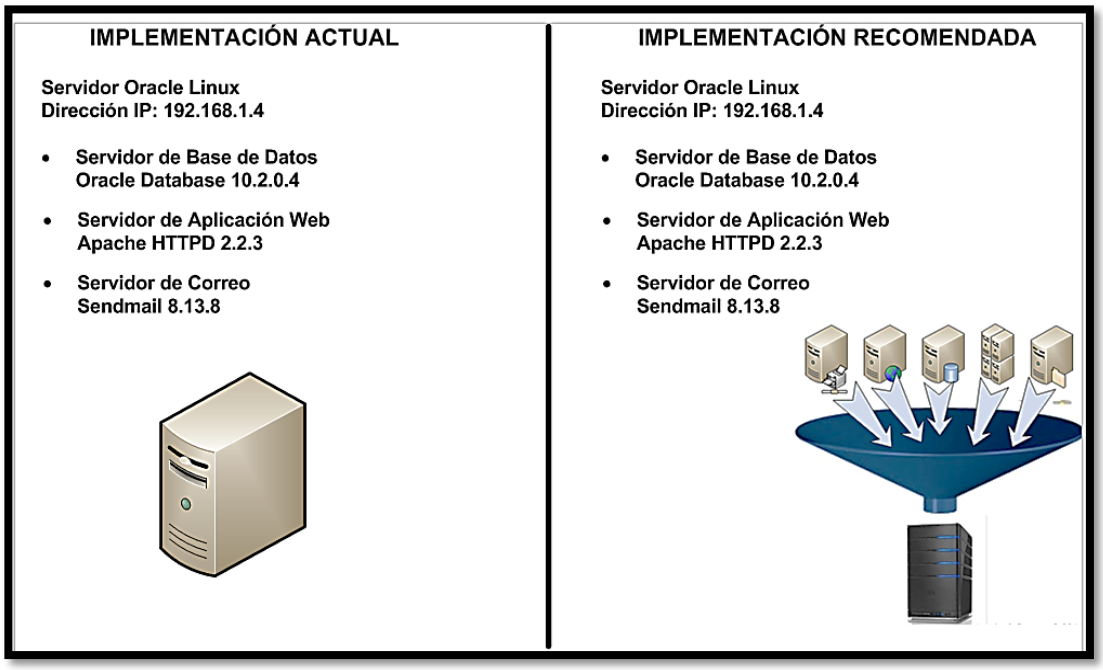


Figura N° 39. Implementación actual – Implementación recomendada

Elaborado por: Investigadora

b. Tipo de vulnerabilidades que afectan a los sistemas de confianza y aplicaciones

La mayoría de vulnerabilidades halladas pertenecen al servidor de aplicaciones Apache HTTPD que no dejan de atentar a la seguridad de la base de datos puesto que están alojados en el mismo servidor, por lo que se podría presentarse amenazas críticas y graves que van desde la posible divulgación o modificación de información, proporcionar accesos no autorizados y llegar hasta la interrupción del servicio, lo que podría también perjudicar el desempeño del equipo, además podría verse afectada la confidencialidad, integridad y disponibilidad de la información de la base de datos.

Un alto porcentaje de las vulnerabilidades detectadas se deben al uso de versiones obsoletas en los sistemas de los servidores Apache Web y servidor de base de datos Oracle.

Existe un porcentaje mínimo de vulnerabilidades, pero no menos importantes que se detectaron debido a conservar configuraciones por defecto que habilitan métodos innecesarios, permitiendo así la presencia de amenazas de seguridad.

Se detectó el uso de protocolos que hacen uso de certificados digitales para establecer conexiones seguras a internet que trabajan y aceptan algoritmos de cifrado obsoletos y vulnerados; además que, dichos certificados digitales no cuentan con la firma de autenticación de una CA (Autoridad Certificadora).

8) Análisis de resultados

- ✓ Los resultados de los análisis que se realizaron al servidor que contiene la base de datos, el sistema operativo y los servidores de aplicación y correo, pueden revisarse en el *Informe de Mitigación de Vulnerabilidades Críticas* y *el Informe de Mitigación de Vulnerabilidades Graves* del **Anexo 5** y **Anexo 6** respectivamente, cada vulnerabilidad presentada en dichos informes presentan las recomendaciones de mitigación.

- ✓ La base de datos presenta problemas de vulnerabilidad por mantener una versión obsoleta del servidor de base de datos Oracle; por lo que la medida inmediata mientras se espera que la empresa adquiera una versión más reciente para el Sistema Gestor de Base de Datos Oracle es considerar de manera urgente la creación de una regla en las políticas de seguridad de la herramienta se seguridad perimetral de red (cortafuego), que permita bloquear el puerto 1521 desde Internet;

- ✓ En la mayoría de vulnerabilidades halladas es indispensable implementar la actualización a la última versión estable tanto para el servidor de base de datos Oracle como para el servidor Apache HTTPD.

- ✓ Para corregir el uso de Certificados digitales que no cuentan con la firma de autenticación de una CA (Autoridad Certificadora). La empresa podría tener su propia autoridad interna de certificados, caso contrario podría pagarse por un certificado de una autoridad de certificación externo de confianza, tales como Thawte o Verisign.

a. Recomendaciones de mitigación

El informe técnico de las vulnerabilidades encontradas en la base de datos de la empresa, así como en los sistemas y aplicaciones que se alojan en el mismo servidor, que a pesar de considerarse sistemas de confianza presentaron un número significativo de vulnerabilidades, las mismas que fueron analizadas para establecer su respectiva mitigación. El detalle del *Informe de Mitigación de Vulnerabilidades Críticas* y el *Informe de Mitigación de Vulnerabilidades Graves* pueden revisarse a detalle en el **Anexo 5** y **Anexo 6**, respectivamente.

- **CONCLUSIONES**

- ✓ La Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos (DMV-BDD), tiene una estructura muy competa y totalmente aplicable para el análisis de seguridad de la base de datos y los sistemas de confianza que conviven en el servidor de la misma, si fuere el caso.

- ✓ Existen muchas razones para aplicar la metodología propuesta, ya que se describe el proceso secuencial que permite realizar etapa por etapa las tareas necesarias para el análisis, búsqueda y detección de vulnerabilidades de bases de datos0; presenta ejemplos que guiarán al investigador en la presentación de los análisis de vulnerabilidades, así como en la presentación de los informes de mitigación.

- ✓ Se puede decir que la metodología propuesta puede convertirse en una herramienta indispensable para que las empresas puedan medir cómo evoluciona

la seguridad a lo largo del tiempo, independientemente de los sistemas de base de datos que se utilice y las herramientas de análisis y testeos que se apliquen.

- **RECOMENDACIONES**

✓ Se recomienda la aplicación de la metodología propuesta que se elabora en el presente proyecto de investigación; la misma que facilitará al investigador que, con tan solo tener conocimientos básicos de seguridad de información y algo de experiencia como analista y testeador de seguridad, puede empezar a realizar sus primeros trabajos de detección y mitigación de vulnerabilidades de base de datos en pymes.

✓ Aplicar la metodología propuesta, ya que no solamente es posible demostrar las vulnerabilidades de la base de datos, sino que también permite al investigador analizar la información encontrada para emitir las recomendaciones de prevención y mitigación a la empresa, con lo que se podrá brindar un trabajo de investigación que será un aporte valioso para la misma; esto permitirá al personal del Departamento de Sistemas realizar las correcciones necesarias y tomar las medidas pertinentes que ayuden a fortalecer la seguridad de la base de datos, de manera que la empresa pueda mejorar muchos de los aspectos de seguridad de la información.

✓ Se puede recomendar al investigador el uso de Metodología de Detección y Mitigación de Vulnerabilidades de Base de Datos (DMV-BDD), ya que contempla características que le permitirán realizar un proyecto de investigación consistente y que puede repetirse, debido a que tiene una validez más allá del periodo de tiempo “actual” y además es posible aplicarla en empresas similares.

✓ Finalmente se puede determinar que es importante que se continúen realizando investigaciones de nuevos métodos de análisis y detección de vulnerabilidades para base de datos que permita prevenir y mitigar todo tipo de problemas de

seguridad de las bases de datos y permita fortalecer la seguridad de información empresarial.

6.8. Administración

La presente Metodología de Detección y Mitigaciones Vulnerabilidades de Base de Datos, es necesaria sea aplicada por las siguientes personas:

- Gerente: Es quien autoriza y aprueba la política de seguridad de información donde se determine cada qué tiempo o bajo qué circunstancias se deberán llevar a cabo los análisis de detección de vulnerabilidades en la base de datos de la empresa.

- Jefe de Sistemas: Es el encargado de analizar la metodología de detección para futuras evaluaciones; además es el responsable por la aplicación e implementación de cada una de las mitigaciones y recomendaciones establecidas para el aseguramiento de la información contenida en la base de datos empresarial.

6.9. Previsión de la evaluación

La previsión de la evaluación deberá realizarse siempre que se cuente con el personal idóneo para este tipo de accionar, ya que muchos de los procesos que se realizan para el desarrollo de la metodología de detección y mitigaciones vulnerabilidades de base de datos, implica una serie de trabajos que se necesita realizarlo con la ética y prudencia que implica el ejecutar y trabajar sobre herramientas de análisis bastante completas y avanzadas, motivo por el que se contempla varios criterios a tomar en cuenta para la evaluación de los que se detallan en la siguiente matriz:

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Qué evaluar?	La metodología de detección y mitigación de vulnerabilidades en base de datos.

¿Por qué evaluar?	Para verificar que la metodología de detección y mitigación de vulnerabilidades de base de datos, cumple con los objetivos establecidos y logra que incrementar la seguridad de la información.
¿Para qué evaluar?	Para mitigar las vulnerabilidades halladas en la presente investigación, además de poder aplicar y probar la metodología de detección de vulnerabilidades establecida para nuevos procesos de detección de vulnerabilidades de la base de datos.
¿Con que criterios?	Basados en la efectividad, eficiencia y eficacia de la metodología de detección y mitigación de vulnerabilidades de base de datos.
¿Quién evalúa?	El Jefe de Sistemas
¿Cuándo evaluar?	Debido a la evolución continua y rápida de las amenazas y riesgos que tiene la información empresarial, se recomienda se realice este tipo de procesos de detección y mitigación de vulnerabilidades de base de datos al menos 3 (tres) veces al año. También se puede realizar una evaluación emergente de presentarse cierto indicio o sospecha de algún tipo de amenaza o ataque a la seguridad de la información de la base de datos.
¿Cómo evaluar?	Siguiendo la logística, procesos que presenta la metodología para la detección de nuevas vulnerabilidades de base de datos.
¿Con qué evaluar?	Siguiendo cuidadosamente la metodología y con la ayuda de las aplicaciones y herramientas de software para el análisis que se establece para la detección de vulnerabilidades de base de datos.

Tabla N° 39. Matriz del plan de evaluación

Elaborado por: Investigadora

Bibliografía

Libros, disertaciones y tesis

- Villalobos, Johonny (2008). Vulnerabilidad de Sistemas Gestores de Bases de Datos. Trabajo de Investigación, Universidad Nacional de Costa Rica, Heredia, Costa Rica.

- García, J. y Formoso, R. (2013). Protección a la Base de Datos de una PYME. Trabajo de Investigación, Universidad Autónoma del Carmen, México.

- Malik M. y Patel T. (s.f.). Database Security – Attacks and Control Methods (Seguridad de Base de Datos Ataques y Métodos de Control). Trabajo de Investigación, Charotar University of Science & Technology (CHARUSAT), Changa.

- Rohilla S. y Kumar P. (2013). Database Security: Threats and Challenges. Trabajo de Investigación, International Journal of Advanced Research in Computer Science and Software Engineering (Revista Internacional de Investigación Avanzada en Ciencias de la. Computación e Ingeniería de Software).

- De Freitas V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Trabajo de investigación. Revista Venezolana de Información, Tecnología y Conocimiento.

- Martínez V. (2010). Concienciación en Seguridad de la Información, la estrategia para fortalecer el eslabón más débil de la cadena. Trabajo de investigación. Fundación Universitaria Iberoamericana, Cartagena de Indias, Colombia.

- Flores A. (2009). Propuesta de políticas de seguridad de la información para el sistema SIABUC. Tesis de Maestría en tecnologías de la Información, Universidad de Colima. Colima, México.

- Juntamay A. y Macas N. (2011). Estudio y aplicación de procedimientos de análisis forense en servidores de base de daros SQL Server y MySQL, caso práctico: DESITEL – ESPOCH. Tesis de grado. Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador.

- Acurio S. (2009). Introducción a la informática forense. Trabajo de Investigación. Fiscalía General del Ecuador, Ecuador.

Referencias de revistas

- La Asamblea Nacional (2014:). Constitución de la República del Ecuador y la Ley Orgánica de la Función Legislativa, Código Orgánico Integral Penal. 37-37.

- Herzog P.V., (2003). OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad, 11.

- Gutiérrez C., (2012) Noticias, opiniones y análisis de la comunidad de seguridad de ESET, ¿Qué es y por qué hacer un Análisis de Riesgos?, 1.

- Mieres J. (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas. Informe blanco. Evil Fingers, 4.

- Herzog P.V., (2003). OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad, 47.

Artículos disponibles en archivos pre-prints

- El Telégrafo, Septiembre (en prensa). Fraude informático se multiplica en tres años. 2012 (Ecuador). Judicial. Recuperado de: http://contenidos.secom.gob.ec/medios/sites/default/files/boletines/5058ec2f8f58b.pdf

- Computer hoy, diciembre (portal web). Los ataques cibernéticos más peligrosos del 2015. 2015. Recuperado de: http://computerhoy.com/noticias/software/ataques-ciberneticos-mas-peligrosos-del-2015-38595

- Acens, (s. f.) (whitepaper). Bases de datos y sus vulnerabilidades más comunes. Recuperado de: https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

- Gómez, (s.f.) (paper). Tipos de Ataques e Intrusos en las Redes Informáticas. Recuperado de: http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

- Benchimol, (2011) (e-book). Hacking. Metodologías de Análisis (pp. 154). Recuperado de: s://upload.wikimedia.org/wikipedia/commons/b/b9/HakingCero.pdf

Referencias de páginas web

- Gobierno de España, Ministerio de educación, cultura y deporte. (s.f.). Seguridad informática. Recuperado de http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

- Microsoft, Developer Network. The STRIDE Threat Model. Commerce Server (2002). Recuperado de https://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx

- ISO27001.ES, El portal de ISO 27001 en español. Glosario (2005). Recuperado de http://www.iso27000.es/glosario.html#section10r

- Desarrollo web, Manual de iniciación a la programación. Sistemas gestores de bases de datos. Álvarez (2007). Recuperado de http://www.desarrolloweb.com/articulos/sistemas-gestores-bases-datos.html

- EcuRed, Sistema Gestor de Base de Datos. (2016). Recuperado de http://www.ecured.cu/Sistema_Gestor_de_Base_de_Datos.

- Documentación oficial Kali Linux. (2013). Recuperado de http://docs.kali.org/pdf/kali-book-es.pdf

- NeXpose Rapid 7. (2015). Recuperado de: https://www.rapid7.com/es/products/nexpose/nexpose-community.jsp

- Nexpose Rapid 7. Vulnerabilidades Cross site scripting**.** (s.f.) Recuperado de: https://www.rapid7.com/db/vulnerabilities/HTTP-CGI-0010

- CMM. Enciclopedia – Seguridad – Ataques- Estafas. Ataques por desbordamiento de búfer. (2016). Recuperado de: http://es.ccm.net/contents/19-ataques-por-desbordamiento-de-bufer#q=ataques+de+desbordamiento+de+bufer&cur=1&url=%2F

- US-CERT. Departamento de Seguridad Nacional de Estados Unidos el Equipo de Emergencias Informáticas. Ataque POODLE (2014). Recuperado de: https://www.us-cert.gov/ncas/alerts/TA14-290A

- US-CERT. Departamento de Seguridad Nacional de Estados Unidos el Equipo de Emergencias Informáticas. Ataque Man-In-The-Middle MITM (Hombre en el medio) (2015). Recuperado de https://www.us-cert.gov/ncas/alerts/TA15-120A

- CSO ESPAÑA. Beast, nuevo exploit para romper la encriptación. Cabanillas, (2011). Recuperado de: http://cso.computerworld.es/alertas/beast-nuevo-exploit-para-romper-la-encriptacion-ssltls

- OISSG. Open Information System Security Group. Information Systems Security Assessment Framework. ISSAF versión 0.2.1. (2006). Recuperado de: https://www.oissg.org

Anexos

ANEXO 1

ENTREVISTA DIRIGIDA AL JEFE DE SISTEMAS DE LA EMPRESA AUTOMEKANO CÍA. LTDA.

Instrucciones: Describa las respuestas con el mayor detalle y veracidad posible

PREGUNTAS:

1. ¿Qué activos de la información podría ser testeados?

_____

_____

2. ¿Por qué realizaría un testeo de seguridad a los activos antes descritos?

_____

_____

3. ¿Conoce usted si existen o no vulnerabilidades en la base de datos de la empresa?

_____

_____

4. ¿Cuál sería el posible origen de las amenazas que podría presentarse?

_____

_____

5. ¿Qué funciones principales realiza el sistema de información?

_____

_____

6. ¿Qué funciones se deberían asegurar en el sistema de información?

_____

_____

7. ¿Qué tipo de ataque informático ha sufrido la base de datos?

_____

_____

8. ¿Qué tipo de ataques relacionados con base de datos se podría presentar?

_____

_____

9. ¿Se cuenta con una metodología para la detección de vulnerabilidades en base de datos?

_____

_____

10. ¿Se cuenta con una metodología para la mitigación de vulnerabilidades en base de datos?

_____

_____

ANEXO 2

CUESTIONARIO SOBRE LA SEGURIDAD BASE DE DATOS EMPRESA AUTOMEKANO CÍA. LTDA.

INSTRUCCIONES: Seleccione la respuesta correcta de las opciones que presenta cada pregunta.

1.- ¿Cuál es el nivel de importancia de la información de la base de datos que maneja la empresa?

a) Normal

b) Alta

2.- ¿Con qué tiempo se realiza un análisis de seguridad de base de datos en busca de vulnerabilidades?

a) Semanal

b) Mensual

c) Semestral

d) Anual

e) Nunca

3.- ¿Qué nivel de seguridad tiene el servidor de la base de datos de la empresa?

Niveles	Parámetros
Bajo	Cualquier usuario tiene acceso a la base de datos de la empresa.
Medio	Solamente personal autorizado accede a la base de datos
Alto	Solo personal autorizado accede a la base de datos, se mantiene historiales de acceso. Además se cuenta con herramientas de seguridad para control y administración de la base de datos.

a) Bajo

b) Medio

c) Alto

4.- ¿Qué software de seguridad se encuentra instalados en la empresa?

a) Antivirus

b) Firewall

c) Detección de Malware

d) IDPS

e) IDS

5.- ¿Qué usuarios pueden acceder a la información confidencial de la base de datos de la empresa?

a) Administradores

b) Analistas de sistemas

c) Otros

6.- ¿Han existido ataques hacia el servidor de la base de datos de la empresa?

a) Si

b) No

c) No lo sabe

7.- ¿Se realizan acciones para la detección y mitigación de vulnerabilidades en base de datos?

a) Si

b) No

ANEXO 3

Ambato, lunes 4 de enero del 2016

ACEPTACIÓN DE PROYECTO DE INVESTIGACIÓN

Señores

POSGRADO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

Presente.-

De mis consideraciones;

Posterior al oficio entregado por la **Ingeniera Carolina Anabel Bonilla Vaca**, en el cual nos solicitó realizar un trabajo de investigación en nuestra empresa AUTOMEKANO CÍA. LTDA., se resuelve:

Autorizar y aprobar el trabajo de investigación bajo el tema: "**ELABORACIÓN DE UNA METODOLOGÍA DE DETECCIÓN Y MITIGACIÓN DE VULNERABILIDADES DE BASE DE DATOS Y SU INCIDENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA AUTOMEKANO CÍA. LTDA., DE LA CIUDAD DE AMBATO**", a desarrollarse por la **Ingeniera Carolina Anabel Bonilla Vaca** en nuestra empresa.

Por la atención se brinde a la presente agradezco y me suscribo

Ing. Francisco Sánchez
GERENTE REGIONAL
AUTOMEKANO CÍA. LTDA.

Ambato: Av. Indoamérica Km. 1 • Telfs.: (03) 2520000 - 2521559 - 2520182 • Cel.: 0993932396
Quito: Av. 10 de Agosto 4976 y Sabanilla esquina • Telfs.: (02) 2480999 – 2475453
Guayaquil: Av. Perimetral Km. 13 ½ delante del Mercado de Transferencia de Víveres • Telfs.: (04) 3901033 – 3901034
www.automekano.com

ANEXO 4

Audit Report

Asset report for 192.168.1.4

Audited on April 2, 2016

Reported on April 2, 2016

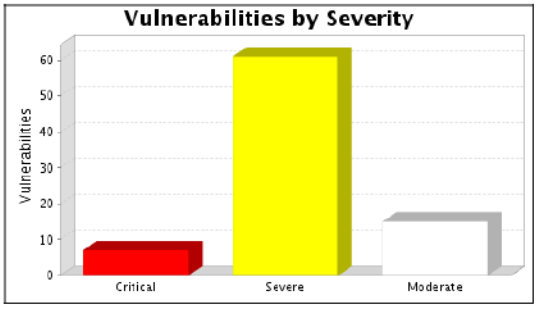
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

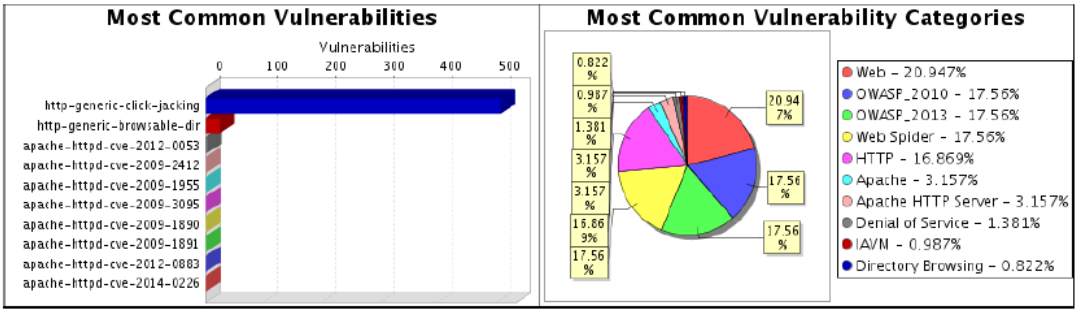
Site Name	Start Time	End Time	Total Time	Status
AUTOMEKANO_SIN_CRED	April 02, 2016 17:03, GMT	April 02, 2016 17:16, GMT	13 minutes	Success

There is not enough historical data to display risk trend.

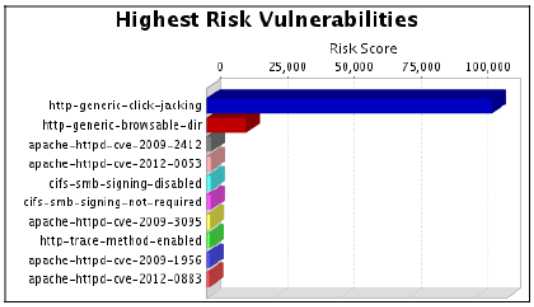
The audit was performed on one system which was found to be active and was scanned.



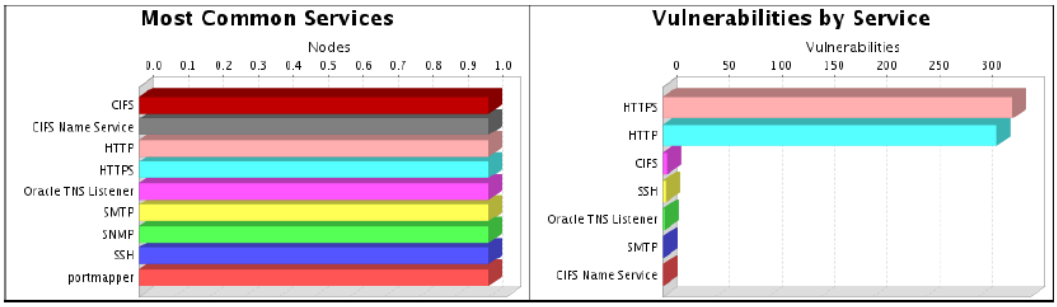
There were 83 vulnerabilities found during this scan. Of these, 7 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 61 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 15 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.



There were 509 occurrences of the http-generic-click-jacking vulnerability, making it the most common vulnerability. There were 637 vulnerability instances in the Web category, making it the most common vulnerability category.



The http-generic-click-jacking vulnerability poses the highest risk to the organization with a risk score of 106,686. Risk scores are based on the types and numbers of vulnerabilities on affected assets.
One operating system was identified during this scan.
There were 10 services found to be running during this scan.



The CIFS, CIFS Name Service, HTTP, HTTPS, Oracle TNS Listener, SMTP, SNMP, SSH and portmapper services were found on 1 systems, making them the most common services. The HTTPS service was found to have the most vulnerabilities during this scan with 333 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
192.168.1.4	Linux 2.6.9	28,244	•amb.automekano.com •AKSERVER

ANEXO 5

INFORME DE MITIGACIÓN DE VULNERABILIDADES CRÍTICAS				
DESCRIPCIÓN	**DATOS TÉCNICOS**	**TIPO DE IMPACTO**	**MITIGACIÓN**	**REFERENCIA**
1. Apache HTTPD: APR apr_palloc () de desbordamiento de pila. El activo afectado es vulnerable a esta vulnerabilidad SÓLO si una aplicación que no pertenezca a Apache pueda pasar sin desinfectar los tamaños proporcionados por el usuario a la función apr_palloc (). Una falla en apr_palloc () en la copia incluida de ARP podría ocasionar desbordamientos de pila en programas que tratan apr_palloc () con un tamaño controlado por el usuario.	**Host y puerto afectado:** 192.168.1.4:80 192.168.1.4:443 Ejecutando HTTP Apache HTTPD 2.2.3 versión vulnerable.	**CRÍTICO:** Permite la interrupción del servicio. Proporciona acceso de administrador, permite una violación total de la confidencialidad, integridad y disponibilidad. Permite la revelación no autorizada de información.	• Actualizar a la última versión estable de Apache HTTPD, que puede ser consultado en su página web oficial: http://httpd.apache.org/ • Descargar la actualización de: https://httpd.apache.org/download.cgi	CVE-2009-2412 https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2412
2. SMTP no autenticado 3ª parte puede hacer retransmisión de correo (SMTP-general-retransmisión abierta). Una "retransmisión abierta" - "open	**Host y puerto afectado:** 192.168.1.4:25 Mensaje	**CRÍTICO:** Permite que la divulgación no autorizada de información. Permite la modificación no autorizada. Permite la interrupción del servicio. El servidor de correo está configurado	Los pasos para la desactivación de un open relay SMTP varía de un producto a otro, una versión a otra. Se deberá consular la documentación del servidor SMTP. No se puntualiza la mitigación puesto que no es una vulnerabilidad del	CVE-1999-0512 https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0512

relay" SMTP es un servidor SMTP que permite que el correo sea enviado por un usuario fuera del sitio a un usuario fuera del sitio. Esta vulnerabilidad es explotada por los spammers (remitentes de envíos masivos) o cualquier persona que quiera enviar un mensaje de correo electrónico imposible de encontrar.	retransmitido con <usuario@ejemplo.com>	explícitamente para permitir la retransmisión de correo SMTP, lo que permite el abuso por los spammers.	servidor de la base de datos como tal.	
3. Base de Datos Oracle Versión obsoleta Una versión obsoleta del servidor de base de datos Oracle se está ejecutando. Oracle sólo produce correcciones correspondientes a los últimos niveles de parches dentro de cada versión del producto. Por lo tanto, si el servidor se ejecuta en un conjunto de modificaciones mayores, parches de seguridad críticos no pueden aplicarse sin primero actualizar a un conjunto de parches más reciente.	**Host y puerto afectado:** 192.168.1.4:1521 Ejecutando Oracle TNS Listener producto de Base de datos Oracle 10.2.0.4 versión vulnerable.	**CRÍTICO:** Las versiones obsoletas de Oracle pueden ser vulnerables. La Base de Datos de Oracle podría ser vulnerables a los ataques de desbordamiento de búfer, inyección SQL, ataques TNS Listener, ataques de cross-site scripting, y los ataques de recorrido de directorio (directory traversal).	Es muy recomendable que actualice un parche o una instalación de Base de Datos Oracle con las últimas actualizaciones disponibles.	URL: http://www.oracle.com/support/library/brochure/lifetime-support-technology.pdf#page=6 URL: http://www.oracle.com/us/support/lifetime-support/index.html
4. Apache HTTPD: APR-util XML DoS El activo afectado es vulnerable a esta vulnerabilidad sólo si un atacante podría convencer a Apache	**Host y puerto afectado:** 192.168.1.4:80 192.168.1.4:443	**CRÍTICO:** Este tipo de ataque permite la interrupción del servicio. Una falla de denegación de servicio se encuentra en la copia incluida de la librería	• Actualizar a la última versión estable de Apache HTTPD, que puede ser consultado en su página web oficial: http://httpd.apache.org/	CVE-2009-1955 https://web.nvd.nist.gov/view/vuln/detail?vulnId=C

para consumir un documento XML especialmente diseñado.	Ejecutando HTTP Apache HTTPD 2.2.3 versión vulnerable.	APR-util Lenguaje de Etiquetado Extensible (XML). Un atacante remoto podría crear un documento XML especialmente diseñado que haría que el consumo excesivo de memoria cuando son procesadas por el motor de decodificación XML.	• Descargar la actualización de: https://httpd.apache.org/download.cgi • Revise la configuración de su servidor web para su validación.	VE-2009-1955
5. Apache HTTPD: mod_proxy_ftp inyección de comandos FTP El activo afectado es vulnerable a esta vulnerabilidad sólo si se está ejecutando uno de los siguientes módulos: mod_proxy_ftp en el Apache HTTP Server.	**Host y puerto afectado:** 192.168.1.4:80 192.168.1.4:443 Ejecutando HTTP Apache HTTPD 2.2.3 versión vulnerable.	**CRÍTICO**: Permite que la divulgación no autorizada de información. Permite la modificación no autorizada. Permite la interrupción del servicio. El módulo mod_proxy_ftp en el Apache HTTP Server permite a atacantes remotos evitar las restricciones de acceso destinados y enviar comandos arbitrarios en un servidor FTP a través de vectores relacionados con la incorporación de estos comandos en el encabezado de autorización HTTP.	• Actualizar a la última versión estable de Apache HTTPD, que puede ser consultado en su página web oficial: http://httpd.apache.org/ • Descargar e instalar la actualización de: https://httpd.apache.org/download.cgi • Revise la configuración de su servidor web para su validación.	CVE-2009-3095 https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095
6. CIFS NULL Sesión Permitida (CIFS-nt-0001) Las sesiones nulas permiten a los usuarios anónimos establecer sesiones de CIFS no autenticado con Windows o implementaciones CIFS de otros fabricantes tales como la Samba o el servidor CIFS de Solaris.	**Host afectado:** 192.168.1.4 Nombre del servidor encontrado: AKSERVER la política encontrado para el	**CRÍTICO**: Proporciona acceso no autorizado, permite violación parcial de confidencialidad, integridad y disponibilidad; la revelación no autorizada de información; y la interrupción del servicio. NetBIOS/SMB proporciona contraseña predeterminada, nula o fallo. Usuarios anónimos pueden ser capaces de enumerar usuarios locales, grupos,	Debido a que se cuenta con un Sistema Operativo Oracle Linux, de determina la siguiente solución: Samba en Linux Restringir el acceso anónimo a Samba, para lo que se debe modificar la configuración del archivo “smb.conf” de la siguiente manera:	CVE-1999-0519 https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519

	dominio(s): Construida AKSERVER	servidores, recursos compartidos, dominios, políticas de dominio local y pueden ser capaces de acceder a varios servicios MSRPC través de llamadas a funciones RPC. Estos servicios han sido históricamente afectados por numerosas vulnerabilidades. La cantidad de información disponible para los atacantes a través de sesiones NULL también puede permitir que se lleven a cabo los ataques más sofisticados.	guest account = nobody restrict anonymous = 1 Nota: Asegúrese de que usted NO incluye un usuario "nobody" en su archivo de contraseñas.	
7. OpenSSH X11 Cookies local de autenticación vulnerabilidad de omisión (openssh-x11-galleta-auth-by-pass) Ssh en OpenSSH antes 4.7 no controla correctamente cuando una cookie no confiable no puede ser creada y utiliza una cookie confiable X11 en su lugar, lo que permite a los atacantes violar de política destinadas y aumento de privilegios haciendo que un cliente X ser tratado como de confianza.	**Host y puerto afectado:** 192.168.1.4:22 OpenBSD OpenSSH 4.3 en Linux 2.6.9 - 2.6.30	**CRÍTICO**: Proporciona acceso a la cuenta del usuario. Permite la confidencialidad parcia, violación de integridad y disponibilidad; la revelación no autorizada de información y la interrupción del servicio.	• Descargar la actualización de: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH. Aunque siempre se puede construir desde la fuente de OpenSSH, muchas plataformas y distribuciones proporcionan paquetes binarios pre-construidos para OpenSSH. Estos paquetes pre-construidos son generalmente personalizados y optimizados para una distribución particular, por lo que recomendamos que utilice ciertos programas que están disponibles para su sistema operativo.	CVE-2007-4752 https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4752

ANEXO 6

INFORME DE MITIGACIÓN DE VULNERABILIDADES GRAVES				
ACTIVO / IMPACTO	**VULNERABILIDAD**	**REFERENCIA**	**DESCRIPCIÓN / IMPACTO**	**MITIGACIÓN**
Apache HTTPD **Permite la interrupción del servicio.**	**mod_proxy** proxy inverso DoS	CVE-2009-1890	Una denegación de servicio falla se encuentra en el módulo mod_proxy cuando fue utilizado como un proxy inverso. Un atacante remoto podría usar este error para forzar un proceso de proxy para consumir grandes cantidades de tiempo de CPU.	• Actualizar a la última versión estable de Apache HTTPD, que puede ser consultado en su página web oficial: http://httpd.apache.org/ • Descargar la actualización de: https://httpd.apache.org/download.cgi • Revise la configuración de su servidor web para su validación.
	mod_deflate DoS	CVE-2009-1891	Este módulo continúo para comprimir archivos de gran tamaño hasta que la compresión sea completa, incluso si la conexión de red que solicitó el contenido fue cerrada antes de completarse la compresión. Esto causaría mod_deflate a consumir grandes cantidades de CPU si mod_deflate se ha habilitado para un archivo grande.	
	mod_cache proxy DoS	CVE-2007-1863	En los sitios donde está activado el almacenamiento en caché, un atacante remoto podría enviar una solicitud cuidadosamente diseñada que haría que el manejo de dicha	

			solicitud a chocar proceso hijo de Apache. Esto podría conducir a una denegación de servicio si se utiliza un módulo de procesamiento multiproceso.	
	Bloqueo **mod_proxy**	CVE-2007-3847	Un error se encontró en el módulo mod_proxy Apache HTTP Server. En los sitios donde se ha configurado un proxy inverso, un atacante remoto podría enviar una solicitud cuidadosamente diseñada que haría que el manejo de dicha solicitud a chocar proceso hijo de Apache. En los sitios donde se ha configurado un proxy de avance, un atacante podría causar un accidente similar, si un usuario podría ser persuadido para visitar un sitio malicioso usando el proxy. Esto podría conducir a una denegación de servicio si se utiliza un módulo de multiproceso anidado.	
	mod_proxy_http DoS	CVE-2008-2364	Un defecto se encontró en el manejo de las respuestas provisionales excesivas de un servidor de origen cuando se utiliza mod_proxy_http. Un atacante remoto podría causar una denegación de servicio o uso de memoria alta.	
	AllowOverride manipulación de opciones bypass	CVE-2009-1195	Un error se encontró en el manejo de las "Opciones" y directivas “AllowOverride". En las configuraciones que utilizan la directiva "AllowOverride" con ciertos argumentos “Options=", los usuarios locales no estaban restringidos de ejecución de comandos a partir de un desde la parte incluida del servidor un script de la forma prevista.	
	expat DoS	CVE-2009-3560 CVE-2009-3720	Una falla de búfer over-read fue encontrado en el Lenguaje de Etiquetado Extensible (XML). Un atacante que es capaz de conseguir Apache para analizar un documento XML no	

			confiable, puede ser capaz de causar un bloqueo. Este accidente sólo sería una denegación de servicio si se utiliza el trabajador MPM.	
	mod_proxy_ajp DoS	CVE-2010-0408	mod_proxy_ajp sería devolver el código de estado incorrecto si se encuentra un error, causando un backend al servidor para ponerse en un estado de error hasta que el tiempo de espera de reintento expiró. Un atacante remoto podría enviar solicitudes maliciosas para desencadenar este problema.	
	mod_dav DoS	CVE-2010-1452	Un atacante remoto malicioso podría enviar una solicitud cuidadosamente diseñada y causar un proceso hijo httpd se bloquee. Este accidente sólo sería una denegación de servicio si se utiliza el trabajador MPM. Este problema es aún más mitigado como mod_dav sólo se ve afectado por las solicitudes que son más propensos a ser autenticado.	
	apr_bridage_split_line DoS	CVE-2010-1623	Un error se encontró en la función apr_brigade_split_line () incluido en la librería APR-util que se utiliza para procesar las solicitudes que no son SSL. Un atacante remoto podría enviar solicitudes, creando cuidadosamente el tiempo de bytes individuales, que consumirían lentamente la memoria.	
	Bloqueo **mod_dav**	CVE-2013-6438	El código de análisis XML en mod_dav calcula incorrectamente el extremo de la cuerda al quitar los espacios iniciales y coloca un carácter NUL fuera del buffer, causando bloqueos aleatorios. Este código de análisis XML sólo se utiliza con los módulos de proveedor DAV que apoyan DeltaV, de los cuales se mod_dav_svn el único	

			proveedor a conocer públicamente.	
	Bloqueo **mod_log_config**	CVE-2014-0098	Un error se encontró en mod_log_config. Un atacante remoto podría enviar una cookie truncado específico que causa un bloqueo. Este accidente sólo sería una denegación de servicio si se utiliza una conexión anidada MPM.	
	mod_cgid negación de servicio	CVE-2014-0231	Un error se encontró en mod_cgid. Si un servidor utilizando mod_cgid alojado scripts CGI que no consumen la entrada estándar, un atacante remoto podría causar procesos secundarios para colgar de forma indefinida.	
	mod_proxy_balancer DoS	CVE-2007-6422	Un error se encuentra en el módulo de mod_proxy_balance. En los sitios donde está activado mod_proxy_balance, un usuario autorizado puede enviar una solicitud cuidadosamente diseñada que haría que el manejo de dicha solicitud a chocar proceso hijo de Apache. Esto podría conducir a una denegación de servicio si se utiliza un módulo de multiprocesamiento anidado.	
	APR-util subscribir almacenamiento dinámico	CVE-2009-0023	Se encontró una suscribir error basados en pila en la forma en que la copia incluida de la librería APR-util creó formas de determinados patrones de búsqueda compilada. Un atacante podría formular una palabra clave de búsqueda especialmente diseñada, que sobrescribirá posiciones de memoria almacenamiento dinámico arbitrariamente al ser procesada por el motor de preparación patrón.	
	Bloqueo **mod_dav**	CVE-2013-1896		

			Enviar una solicitud de MERGE contra un URL manejado por mod_dav_svn con el href código (enviado como parte del cuerpo de la petición como XML) que apunta a un URL que no está configurado para DAV activará un error de segmentación.	
	mod_deflate negación de servicio	CVE-2014-0118	Un error consumo de recursos se encuentra en mod_deflate. Si la descompresión cuerpo de la solicitud fue configurado (usando el filtro de entrada "DESINFLE"), un atacante remoto podría provocar que el servidor consume memoria significativa y / o recursos de la CPU. El uso de la descompresión solicitud cuerpo no es una configuración común.	
	apr_fnmatch error conduce a **mod_autoindex** remota DoS	CVE-2011-0419	Un error se encuentra en la función de apr_fnmatch () de la biblioteca de ARP incluido. Donde mod_autoindex está activado, y un directorio indexado por mod_autoindex contenía archivos con nombres suficientemente largos, un atacante remoto podría enviar una solicitud cuidadosamente lo que causaría uso excesivo de CPU. Esto podría ser utilizado en un ataque de denegación de servicio.	
	Señales a los procesos arbitrarios	CVE-2007-3304	El servidor Apache HTTP no verificó que el proceso fue un proceso hijo de Apache antes de enviarlo señales. Un atacante local con la capacidad de ejecutar secuencias de comandos en el servidor HTTP podría manipular el marcador y provocar procesos arbitrarios para ser terminado, que podría conducir a una denegación de servicio.	
Apache HTTPD	HTTP petición de ataque contrabando	CVE-2015-3183	Una petición HTTP de ataque de contrabando es posible	• Actualizar a la última versión

Permite la modificación no autorizada.	contra la petición del analizador fragmentada		debido a un error en el análisis de solicitudes fragmentadas. Un cliente malicioso podría forzar al servidor a malinterpretar la longitud de petición, lo que permite envenenamiento de caché o el secuestro de credenciales si un proxy intermediario está en uso.	estable de Apache HTTPD, que puede ser consultado en su página web oficial: http://httpd.apache.org/ • Descargar la actualización de: https://httpd.apache.org/download.cgi • Revise la configuración de su servidor web para su validación.
	mod_status cross-site scripting	CVE-2006-5752	Un error se encuentra en el módulo de mod_status. En los sitios donde la página servidor-estado es accesible al público y se habilita ExtendedStatus esto podría conducir a un ataque de cross-site scripting.	
	mod_imap XSS	CVE-2007-5000	Un error se encuentra en el módulo de mod_imap. En los sitios donde está activado mod_imap y un archivo de mapa de imágenes está disponible al público, un ataque de cross-site scripting es posible.	
	mod_status XSS	CVE-2007-6388	Un error se encuentra en el módulo de mod_status. En los sitios donde mod_status está habilitado y las páginas de estado eran accesibles al público, un ataque de cross-site scripting es posible.	
	mod_proxy_balancer CSRF	CVE-2007-6420	El mod_proxy_balance proporciona una interfaz de administración que podría ser vulnerables a la petición en sitios cruzados (CSRF ataques de falsificación).	
	mod_proxy_balancer XSS	CVE-2007-6421	Un error se encuentra en el módulo de mod_proxy_balance. En los sitios donde está activado mod_proxy_balance, un ataque de cross-site scripting en contra de un usuario autorizado es posible.	

	mod_proxy_ftp UTF-7 XSS	CVE-2008-0005	Una solución temporal se añadió en el módulo mod_proxy_ftp. En los sitios donde mod_proxy_ftp está activado y un proxy de reenvío está configurado, un ataque de cross-site scripting es posible frente a los navegadores Web que no se derivan correctamente el conjunto de caracteres de respuesta siguiendo las reglas en RFC 2616.	
	mod_proxy_ftp englobamiento XSS	CVE-2008-2939	Un error se encontró en el manejo de comodines en la ruta de un URL FTP con mod_proxy_ftp. Si mod_proxy_ftp está activado el soporte de FTP sobre HTTP, las peticiones que contienen caracteres con englobamiento podría conducir a ataques cross-site scripting (XSS).	
	mod_proxy exposición de proxy inverso	CVE-2011-4317	Una exposición adicional fue encontrada al usar mod_proxy en el modo de proxy inverso. En ciertas configuraciones que utilizan RewriteRule con el indicador proxy o ProxyPassMatch, un atacante remoto podría provocar que el proxy inverso para conectarse a un servidor arbitrario, posiblemente revelar información confidencial de los servidores web internos no directamente accesibles al atacante.	
	XSS debido a nombres de host sin escape	CVE-2012-3499	El activo afectado es vulnerable a esta vulnerabilidad sólo si se está ejecutando uno de los siguientes módulos: mod_imagemap, mod_info mod_ldap, mod_proxy_ftp, mod_status. Varios defectos XSS debido a los nombres de host sin escape y salida de los URI HTML en mod_info, mod_status, mod_imagemap, mod_ldap y mod_proxy_ftp.	

	XSS en mod_proxy_balancer	CVE-2012-4558	Un fallo de XSS afectó a la interfaz del gestor de mod_proxy_balance.	
Apache HTTPD **Permite la divulgación no autorizada de información.**	Subpetición de manejo de las cabeceras de solicitud (**mod_headers**)	CVE-2010-0434	Cuando se utiliza un MPM multihilo, no maneja adecuadamente las cabeceras de subpeticiones en ciertas circunstancias que implican una petición de los padres que tiene un cuerpo, lo que podría permite a atacantes remotos obtener información sensible a través de una solicitud hecha a mano que dispara el acceso a posiciones de memoria asociados a una petición anterior.	• Actualizar a la última versión estable de Apache HTTPD, que puede ser consultado en su página web oficial: http://httpd.apache.org/ • Descargar la actualización de: https://httpd.apache.org/download.cgi • Revise la configuración de su servidor web para su validación.
	Las respuestas de error pueden exponer las cookies	CVE-2012-0053	Un error se encontró en la respuesta de error predeterminado para el código de estado 400. Este fallo podría ser utilizado por un atacante para exponer cookies "httpOnly" cuando no se especifica ErrorDocument personalizado.	
	mod_proxy la exposición de proxy inverso	CVE-2011-3368	Una exposición fue encontrada al usar mod_proxy en el modo de proxy inverso. En ciertas configuraciones que utilizan RewriteRule con el indicador proxy, un atacante remoto podría causar el proxy inverso para conectarse a un servidor arbitrariamente, posiblemente revelar información confidencial de los servidores web internos no directamente accesibles al atacante.	
Apache HTTPD **Permite la revelación no autorizada de información.**	manejo inseguro **LD_LIBRARY_PATH**	CVE-2012-0883	El manejo inseguro de LD_LIBRARY_PATH se encontró que podría conducir al directorio de trabajo actual que se debe buscar DSOs. Esto podría permitir a un usuario local ejecutar código como root si un administrador ejecuta apachectl desde un directorio que no es de confianza.	• Actualizar a la última versión estable de Apache HTTPD, que puede ser consultado en su página web oficial: http://httpd.apache.org/

Permite la modificación no autorizada. **Permite la interrupción del servicio.**				• Descargar la actualización de: https://httpd.apache.org/download.cgi • Revise la configuración de su servidor web para su validación.
	mod_status desbordamiento de búfer	CVE-2014-0226	Una condición de ejecución se encontró en mod_status. Un atacante acceder a una página de estado del servidor público en el servidor usando un MPM anidado podría enviar una solicitud cuidadosamente diseñada que podría dar lugar a un desbordamiento de búfer de pila.	
	APR-util off-by-one desbordamiento	CVE-2009-1956	Un error de desbordamiento off-by-one se encuentra en la forma en que la copia incluida de la librería APR-util procesa una lista variable de argumentos. Un atacante podría proporcionar una cadena especialmente diseñado como entrada para la rutina de conversión de formato de salida, lo que podría, en plataformas big-endian, lo que podría conducir a la divulgación de información sensible o una denegación de servicio.	
	Padre marcador DoS	CVE-2012-0031	Un error se encontró en el manejo del marcador. Un proceso hijo sin privilegios podría hacer que el proceso padre se bloquee al apagar el equipo en lugar de terminar limpiamente.	
	mod_rewrite log filtrado de escape	CVE-2013-1862	mod_rewrite no filtra secuencias de escape de terminal de registros, lo que podría hacer que sea más fácil para los atacantes para insertar esas secuencias en emuladores de terminal que contienen vulnerabilidades relacionadas con las secuencias de escape.	
	HTTP Bypass de procesamiento de	CVE-2013-5704	Trailers HTTP podría utilizarse para reemplazar las	

	trailers		cabeceras HTTP tarde durante el proceso de peticiones, potencialmente deshacer o de otra manera confusos módulos que examinaron o encabezados de solicitud modificados anteriormente. Esta corrección agrega la directiva "MergeTrailers" para restaurar el comportamiento heredado.	
Servidor TLS/SSL **Permite la divulgación no autorizada de información.**	Está permitiendo el ataque POODLE	CVE-2014-3566	Todos los sistemas y aplicaciones que utilizan el protocolo Secure Socket Layer (SSL) 3.0 con sistemas de cifrado modo de cifrado encadenamiento de bloques (CBC) pueden ser vulnerables a ataques POODLE (Padding Oracle On Downgraded Legacy Encryption). La vulnerabilidad SSL 3.0 se deriva de la forma en que los bloques de datos son encriptados bajo un determinado tipo de algoritmo de cifrado en el protocolo SSL. El ataque POODLE se aprovecha de la función de la negociación versión del protocolo integrado en SSL para forzar el uso de SSL 3.0 y luego aprovecha esta nueva vulnerabilidad para descifrar seleccionando contenidos dentro de la sesión SSL.	Configurar el servidor para requerirá que sus clientes usen TLS versión 1.2 utilizando cifrado autenticado los datos asociados (AEAD) cifrados idóneos.
	Soporta SSLv3 (sslv3-soportado)	CVE-2014-3566	El protocolo SSLv3 y cifrados soportados todos sufren de graves vulnerabilidades que hacen de este protocolo no sea seguro usar.	
	Soporta TLS version 1.0 (tlsv1_0-enabled)	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf	El PCI (Industria de Tarjetas de Pago) Estándar de Seguridad Informática requiere un mínimo de TLS v1.1 y v1.2 recomienda TLS. Además, la norma FIPS 140-2 estándar requiere un mínimo de TLS v1.1 y v1.2 recomienda TLS.	

Apache HTTPD **Proporciona acceso a la cuenta del usuario. Permite la parcial violación de confidencialidad, integridad y disponibilidad. Permite la interrupción del servicio y revelación no autorizada de información.**	**mod_setenvif .htaccess** escalamiento de privilegios	CVE-2011-3607	El activo afectado es vulnerable a esta vulnerabilidad sólo si se está ejecutando uno de los siguientes módulos: mod_setenvif. Revise la configuración de su servidor web para su validación. Un error de desbordamiento de entero se ha encontrado que, cuando se habilita el módulo mod_setenvif, podría permitir a usuarios locales conseguir privilegios a través de un archivo .htaccess.	• Actualizar a la última versión estable de Apache HTTPD, que puede ser consultado en su página web oficial: http://httpd.apache.org/ • Descargar la actualización de: https://httpd.apache.org/download.cgi • Revise la configuración de su servidor web para su validación.
Servidor TLS/SSL **Permite la divulgación no autorizada de información**	Soporta RC4 Algoritmos de Cifrado	CVE-2013-2566	Los resultados recientes de criptoanálisis explotan sesgos en la cadena de claves RC4 para recuperar los textos planos cifrados en varias ocasiones. RC4 ya no puede ser visto como que proporciona un nivel de seguridad suficiente para sesiones SSL / TLS. Tiene muchos prejuicios de un solo byte, lo que hace que sea más fácil para los atacantes remotos llevar a cabo ataques de recuperación de texto claro de a través de un análisis estadístico de texto cifrado en un gran número de sesiones que utilizan el mismo texto plano.	Configurar el servidor para desactivar el soporte y compatibilidad con algoritmos de cifrado RC4, DES e IDE y cifrados débiles.
	Soporta DES and IDEA Paquetes de Cifrado (ssl-des-ciphers)	http://www.nist.gov/manuscript-publication-	Transport Layer Security (TLS) versiones 1.0 (RFC 2246) y 1.1 (RFC 4346) incluyen conjuntos de cifrado basado en el DES (Data Encryption Standard) e IDEA (International Data	

		search.cfm?pub_id=915295	Encryption Algorithm) algoritmos. DES y algoritmos de IDEA ya no se recomiendan para uso general en TLS, y se han eliminado de la versión 1.2 de TLS.	
	Soporta algoritmos de cifrados débiles (ssl-weak-ciphers)	http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295	El servidor TLS/SSL es compatible con paquetes de cifrado basado en algoritmos débiles. Esto puede permitir a un atacante para lanzar ataques man-in-the-middle y controlar o manipular los datos sensibles. En general, los siguientes cifrados se consideran débiles: • Los llamados sistemas de cifrado "nulo", porque no se cifran los datos. • Cifras de exportación utilizando longitudes de clave secreta limitada a 40 bits. Esto generalmente se indica mediante la palabra EXP/exportación en el nombre del conjunto de cifrado. • Algoritmos de cifrado obsoletos con longitudes de claves secretas consideradas cortas para los estándares de hoy en día, por ejemplo. DES o RC4 con claves de 56 bits.	
Servidor TLS/SSL **Permite la divulgación no autorizada de información**	Está permitiendo el ataque BEAST (ssl-cve-2011-3389-beast)	CVE-2011-3389	El protocolo SSL, tal como se utiliza en ciertas configuraciones de Microsoft Windows y navegadores como Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera (y otros productos de negociación conexiones SSL) cifra los datos utilizando el modo CBC con vectores de inicialización encadenados. Esto permite potencialmente man-in-the-middle atacantes para obtener las cabeceras HTTP de texto a través de un ataque al límite por bloques elegido (BCBA) en una sesión HTTPS, en conjunción con el código JavaScript que utiliza (1) de la API	No hay ninguna mitigación del lado del servidor disponible contra el ataque BEAST. La única opción es desactivar los protocolos afectados (SSLv3 y TLS 1.0). La configuración sólo totalmente segura es utilizar cifrado autenticado con datos asociados (AEAD), por ejemplo, AES-GCM, AES-CCM en TLS 1.2.

			de HTML5 WebSocket, (2) el Java API URLConnection, o (3) la API de cliente Web Silverlight, también conocido como un ataque "BEAST". Mediante el apoyo a los protocolos y sistemas de cifrado afectados, el servidor está permitiendo a los clientes para ser explotados.	
Servidor no confiable TLS/SSL **Permite la divulgación no autorizada de información**	X.509 certificado (tls-untrusted-ca)	http://httpd.apache.org/docs/2.2/mod/mod_ssl.html http://nginx.org/en/docs/http/configuring_https_servers.html	El certificado TLS/SSL del servidor está firmado por una autoridad de certificación (CA) que no es conocido o de confianza. Esto podría ocurrir si: la cadena / certificado intermedio no está presente, ha caducado o ha sido revocado; el nombre de host del servidor no coincide con el configurado en el certificado; la hora / fecha es incorrecta; o se está utilizando un certificado autofirmado. El uso de un certificado autofirmado no se recomienda ya que podría indicar que un lugar TLS/SSL un ataque man-in-the-middle se lleva a cabo.	Asegúrese de que el nombre común (CN) refleja el nombre de la entidad que presenta el certificado. Si el(los) certificado(s) de la cadena han vencido o se han revocado, debe obtener un nuevo certificado de la autoridad de certificación (CA) siguiendo su documentación. Si se está utilizando un certificado autofirmado, considerar la obtención de un certificado firmado por una CA.
Certificado TLS/SSL autofirmado	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	Ninguna	Certificado TLS/SSL del servidor es autofirmado. Los certificados auto-firmados no se puede confiar por defecto, sobre todo porque TLS/SSL ataques man-in-the-middle suelen utilizar certificados con firma para escuchar a escondidas en las conexiones TLS/SSL.	Obtener un nuevo certificado de servidor TLS / SSL que no es autofirmado e instalarlo en el servidor.
X.509 Certificado del servidor es invalido/ expirado	X.509 Certificado del servidor es invalido/ expirado (tls-server-cert-expired)	Ninguna	El certificado X.509 del servidor de TLS/SSL o bien contiene una fecha de inicio en el futuro o ha caducado. Favor consulte las pruebas para obtener más detalles.	Obtener un nuevo certificado e instalarlo en el servidor. Las instrucciones exactas para obtener un nuevo certificado dependen de los requisitos de su empresa. Asegúrese de que la fecha de inicio y la fecha final

				en el nuevo certificado son válidas. .
X.509 Certificado campo CN (nombre común) **Permite leer, insertar y modifica información.**	X.509 Certificado campo CN no coincide con el nombre de la entidad (certificate-common-name-mismatch)	Ninguna	El campo Asunto nombre común (CN) en el certificado X.509 no coincide con el nombre de la entidad que presenta el certificado. Antes de emitir un certificado, una autoridad de certificación (CA) debe verificar la identidad de la entidad que solicita el certificado, tal como se especifica en la Declaración de Prácticas de Certificación de la entidad emisora (CPS). Por lo tanto, los procedimientos de validación de certificados estándar requieren el campo CN objeto de un certificado para que coincida con el nombre real de la entidad que presenta el certificado. Por ejemplo, en un certificado presentado por "https://www.example.com/", el CN debe ser "www.example.com". Con el fin de detectar y prevenir los ataques de escucha activa, la validez de un certificado debe ser verificada, o de lo contrario un atacante podría lanzar un ataque man-in-the-middle y obtener el control total del flujo de datos. De particular importancia es la validez del CN del sujeto, que debe coincidir con el nombre de la entidad (nombre de host). Un desajuste CN se produce más a menudo debido a un error de configuración, aunque también puede indicar que un ataque man-in-the-middle está llevando a cabo.	El campo del sujeto nombre común (CN) en el certificado X.509 debe fijarse para reflejar el nombre de la entidad que presenta el certificado (por ejemplo, el nombre de host). Esto se hace mediante la generación de un nuevo certificado firmado por lo general por una autoridad de certificación (CA) de confianza para el cliente y el servidor.
OpenSSL **Permite la divulgación no autorizada de información**	OpenSSL SSL/TLS vulnerabilidad MITM	CVE-2014-0224	OpenSSL antes 0.9.8za, 1.0.0 antes 1.0.0m y 1.0.1 antes 1.0.1h no restringe adecuadamente el procesamiento de los mensajes ChangeCipherSpec, lo que permite que ataques de man-in-the-middle se desencadenen con el uso de una llave maestra de longitud en ciertas comunicaciones de OpenSSL-to-OpenSSL, y por lo tanto robar las sesiones u obtener información sensible, a través de un apretón de manos TLS	• Actualizar a la última versión estable de Open SSL, que puede ser consultado en su página web oficial: https://www.openssl.org/ • Descargar la actualización de: https://www.openssl.org/source/

			manipulada, también conocido como la vulnerabilidad "CCS inyección".	
La firma SMB desactivada / no se requiere **Permite leer, insertar y modifica información.**	La firma SMB desactivada (cifs-smb-signing-disabled) / no se requiere (cifs-smb-signing-not-required)	http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-andsmb2.Aspx	Este sistema no permite la firma SMB / Este sistema permite, pero no requiere la firma SMB. La firma de SMB permite que el destinatario de los paquetes SMB para confirmar su autenticidad y ayuda a evitar ataques man-in-the-middle de SMB. La firma de SMB se puede configurar en una de tres maneras: desactivado por completo (menos seguro), habilitado, y requirió (el más seguro).	Configurar la firma SMB para Samba para permitir o requerir la firma SMB en su caso. Para habilitar la firma SMB, poner el siguiente en el archivo de configuración de Samba, smb.conf, en la sección global: **server signing = auto** Para requerir la firma SMB, poner el siguiente en el archivo de configuración de Samba, típicamente smb.conf, en la sección global: **server signing = mandatory**
Click Jacking **Permite la revelación no autorizada de información.**	Click Jacking (http-generic-click-jacking)	https://www.owasp.org/index.php/Clickjacking	Clickjacking, también conocido como un ataque reparación de interfaz de usuario, es un método en el que un atacante utiliza múltiples capas transparentes u opacos para engañar a un usuario para que haga clic en un botón o enlace en una página distinta de la que ellos creen que están haciendo clic. Por lo tanto, el atacante hace clics "hijacking" significa para una página y enruta al usuario a una página ilegítima.	Enviar las cabeceras de respuesta HTTP con X-Frame-Options que instruyen el navegador para restringir el enmarcado donde no está permitido.
Los usuarios anónimos pueden obtener la directiva de contraseñas de Windows	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	CVE-2000-1200	Los usuarios anónimos pueden obtener la directiva de contraseñas de Windows en el sistema mediante el uso de sesiones CIFS NULL. La política de contraseñas contiene información sensible sobre la longitud mínima o umbral de bloqueo de contraseña, Duración del bloqueo de contraseña, etcétera.	Para restringir el acceso anónimo a Samba en Linux, modificar la configuración de “smb.conf" de la siguiente manera: **guest account = nobody** **restrict anonymous = 1** **Nota:** Asegúrese de que usted no

Permite la divulgación no autorizada de información				incluye un usuario " **nobody**" en su archivo de contraseñas.
HTTP TRACE Método Habilitado **Permite la revelación y la modificación no autorizada de información.**	HTTP TRACE Método Habilitado (http-trace-method-enabled)	CVE-2004-2320	El método HTTP TRACE se utiliza normalmente para devolver la petición HTTP completa de reembolso al cliente solicitante a efectos de proxy-depuración. Un atacante puede crear una página web utilizando XMLHTTP, ActiveX, o XMLDOM para hacer que un cliente para emitir una solicitud de rastreo y capturar las cookies del cliente. Esto se traduce efectivamente en un ataque de Cross Site Scripting.	Desactivar el método HTTP TRACE para Apache HTTPD Las nuevas versiones de Apache 2.0.55 (y posteriores) facilita una directiva de configuración llamado TraceEnable. Para denegar solicitudes TRACE, añada la siguiente línea a la configuración del servidor: **TraceEnable off**
Base de datos acceso abierto	Base de datos acceso abierto (database-open-access)	tps://www.pcisecurity standards.org/documents/PCI_DSS_v3-1.pdf	La base de datos permite a cualquier sistema remoto la posibilidad de conectarse a ella. Se recomienda limitar el acceso directo a los sistemas de confianza, porque las bases de datos pueden contener datos sensibles, y las nuevas vulnerabilidades y exploits que se descubren de forma rutinaria para ellos. Por esta razón, es una violación de la sección 1.3.7 de las PCI DSS para tener bases de datos que escuchan en los puertos accesibles desde Internet, incluso cuando está protegido con seguro mecanismos de autenticación.	Configurar el servidor de base de datos para permitir sólo el acceso a los sistemas de confianza. Por ejemplo, el estándar PCI DSS requiere que se coloque la base de datos en una zona de red interna, segregada del DMZ
Directorio web navegable	Directorio web navegable (http-generic-browsable-dir)	https://www.owasp.org/index.php/Top_10_2010-A6	Se encontró que un directorio web para ser navegable, lo que significa que cualquier persona puede ver el contenido del directorio. Estos directorios se pueden encontrar: • a través de la página rastreo (siguiendo hipervínculos), o	Apache HTTPD Desactivar la exploración de directorios web para todos los directorios y subdirectorios En su archivo httpd.conf, desactivar la

		https://www.owasp.org/index.php/Top_10_2013-A5 https://www.owasp.org/index.php/Top_10_2013-A9	• como parte de una ruta padre (la comprobación de cada directorio de la ruta y la búsqueda de "Lista de directorios" o cadenas similares), o • por fuerza bruta sobre una lista de directorios comunes. Directorios navegables podría permitir a un atacante realizar un ataque de salto de directorio mediante la visualización de archivos "ocultos" en la raíz de la web, incluyendo scripts CGI, archivos de datos o páginas de copia de seguridad.	opción **"Indexes"** para la etiqueta apropiada **<Directory>** quitándolo de la línea de opciones. Además, siempre debe asegurarse de que los permisos adecuados se fijan en todos los archivos y directorios dentro de la raíz web (incluyendo scripts CGI y los archivos de copia de seguridad). No copie los archivos en el directorio raíz web si desea que estos archivos estén disponibles a través de Internet. Periódicamente ir a través de sus directorios web y limpiar todos los archivos y directorios no utilizados, obsoletos o desconocidos.
La vulnerabilidad número de secuencia de aproximación. **Permite la interrupción del servicio.**	La vulnerabilidad número de secuencia de aproximación (tcp-seq-num-approximation)	CVE-2004-0230	TCP, cuando se utiliza un gran tamaño de la ventana, hace que sea más fácil para los atacantes remotos adivinar los números de secuencia y causar una denegación de servicio (pérdida de conexión) a las conexiones TCP persistentes mediante inyecciones repetidas de un paquete TCP RST, sobre todo en los protocolos que utilizan conexiones de larga vida, tal como BGP.	Habilitar TCP Las firmas MD5 Habilitar la opción de firma TCP MD5 como se documenta en RFC 2385. Fue diseñado para reducir el riesgo de ciertos ataques de seguridad de BGP, tales como reinicios de TCP.