ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA

INFORME DE TRABAJO DE TITULACIÓN

PREVIA LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS

MODALIDAD: PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

PLAN DE MEJORA ANTE VULNERABILIDADES ENCONTRADAS EN IMPLEMENTACIONES DE SISTEMAS GESTORES DE BASES DE DATOS

AUTORAS:

DÁVILA MUÑOZ MAYRA ALEXANDRA

MUÑOZ CRUZATI MIRLA LUCÍA

TUTORA:

ING. JÉSSICA JOHANNA MORALES CARRILLO, Mg. Sc.

CALCETA, MAYO 2019

DERECHOS DE AUTORÍA

MAYRA ALEXANDRA DÁVILA MUÑOZ y MIRLA LUCIA MUÑOZ CRUZATI declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su Reglamento.

_____ _____

MAYRA ALEXANDRA DÁVILA MUÑOZ **MIRLA LUCIA MUÑOZ CRUZATI**

CERTIFICACIÓN DE LA TUTORA

ING. JÉSSICA JOHANNA MORALES CARRILLO, Mg. Sc, certifica haber tutelado el trabajo de titulación **PLAN DE MEJORA ANTE VULNERABILIDADES ENCONTRADAS EN IMPLEMENTACIONES DE SISTEMAS GESTORES DE BASES DE DATOS**, que ha sido desarrollada por **MAYRA ALEXANDRA DÁVILA MUÑOZ** y **MIRLA LUCIA MUÑOZ CRUZATI**, previa la obtención del título de Magister en tecnologías de la información mención redes y sistemas distribuidos, de acuerdo al **REGLAMENTO DE UNIDAD DE TITULACIÓN DE LA UNIDAD DE TITULACIÓN ESPECIAL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López**.**

_____

ING. JÉSSICA JOHANNA MORALES CARRILLO, Mg. Sc,

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **PLAN DE MEJORA ANTE VULNERABILIDADES ENCONTRADAS EN IMPLEMENTACIONES DE SISTEMAS GESTORES DE BASES DE DATOS**, que ha sido propuesto, desarrollado por **MIRLA LUCIA MUÑOZ CRUZATI y MAYRA ALEXANDRA DÁVILA MUÑOZ**, previa la obtención del título de Magister en tecnologías de la información mención redes y sistemas distribuidos, de acuerdo al **REGLAMENTO DE UNIDAD DE TITULACIÓN DE LA UNIDAD DE TITULACIÓN ESPECIAL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

_____ _____

ING. Gustavo Molina Garzón., M.Sc
MIEMBRO

ING. Sergio Intriago Briones M.Sc
MIEMBRO

_____

ING. Marlon Navia Mendoza., M.Sc
PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que nos dio la oportunidad de crecer como ser humano a través de una educación superior de calidad y en la cual hemos forjado nuestros conocimientos profesionales día a día.

LAS AUTORAS

DEDICATORIA

A mi amado esposo Leonardo por la confianza y apoyo incondicional y diario para continuar con mi formación profesional, a mis queridas hijas Luisana y Lizbeth por su paciencia y comprensión durante todo el proceso de clases y titulación.

MAYRA ALEXANDRA DÁVILA MUÑOZ

DEDICATORIA

A mi esposo José Luis Almeida por brindarme su apoyo incondicional en el diario vivir.

A mis hijas Nallerly Margarita y Ashley Valentina por su comprensión.

Y a todas las personas que de una manera u otra manera me apoyó durante esta etapa de estudio.

MIRLA LUCIA MUÑOZ CRUZATI

CONTENIDO GENERAL

CONTENIDO DE TABLA

CONTENIDO DE GRÁFICO

RESUMEN

Este trabajo tuvo como objetivo elaborar un plan de mejoras ante las falencias encontradas en dos sistemas gestores de bases de datos empleando dos herramientas de detección de vulnerabilidades, para contribuir a la seguridad de la información que se maneja dentro de las organizaciones. El desarrollo de éste se hizo siguiendo el proceso metodológico planteado por Magerit V3, la cual permitió de forma teórica identificar las amenazas, el nivel de exposición al riesgo y el impacto que causaría su materialización; determinando a los sistemas gestores de bases de datos como objeto de estudio. Se realizó la valoración tanto cualitativa como cuantitativa de las amenazas y su respectivo análisis mediante tablas, además del uso de *Nessus* y *Nexpose* como herramientas de detección de vulnerabilidades con el fin de conocer errores que se pueden dar en la práctica y tomando en consideración las soluciones sugeridas por las herramientas mencionadas, de la realización de este proceso teórico y práctico, se obtuvo un plan de mejoras, el cual se desarrolló con el fin de tener una perspectiva del proceso a seguir para corregir a tiempo los riesgos identificados, contribuyendo a la toma de las mejores decisiones en cuanto a la seguridad de los sistemas gestores de bases de datos que contienen la información.

PALABRAS CLAVE

Gestores de bases de datos, riesgo de gestores de bases de datos, Magerit, scanners de vulnerabilidades, plan de mejoras.

ABSTRACT

The objective of this work was to elaborate an improvement plan in the face of the shortcomings found in two database management systems using two vulnerability detection tools, to contribute to the security of the information handled within the organizations. The development of this was done following the methodological process proposed by Magerit V3, which theoretically allowed to identify the threats, the level of risk exposure and the impact that would cause its materialization; determining the database management systems as the object of study. The qualitative and quantitative assessment of the threats and their respective analysis by means of tables was carried out, as well as the use of Nessus and Nexpose as vulnerability detection tools in order to know errors that may occur in practice and taking into account the solutions Suggested by these tools, of the realization of this theoretical and practical process, an improvement plan was obtained, which was developed in order to have a perspective of the process to be followed in order to correct the identified risks in time, contributing to the taking of the best decisions regarding the security of the database management systems that contain the information.

KEY WORDS

Database managers, risk of database managers, Magerit, vulnerability scanners, improvement plan.

CAPÍTULO I. ANTECEDENTES

1.1 PLANTEAMIENTO DEL PROBLEMA

Hoy en día, con el avance de las tecnologías de la información, las instituciones deben estar alerta ante posibles amenazas que puedan presentarse y que comprometan el buen funcionamiento de los equipos o del sistema de información, cabe mencionar que cualquier sistema de información está expuesto a diversos factores de riesgo que pueden ser humanos, físicos o naturales; ante la ocurrencia de un escenario de riesgo, lo primero que se tiene en cuenta es saber cuánto tiempo llevara recuperar la normalidad de las labores, cabe mencionar que la protección de la información es vital ante la posible pérdida, destrucción, robo y otras amenazas que se presentan (Ladines, 2017)

Uno de los sistemas que con mucha frecuencia es objeto de atacantes son los gestores de bases de datos. El 17 de agosto de 2009, el Departamento de Justicia de los Estados Unidos acusó a un ciudadano por el robo de 130 millones en tarjetas de crédito usando ataques de inyección de SQL. Aproximadamente 500.000 páginas web que usaban como servidor el Microsoft IIS y el servidor de SQL, fueron atacadas entre abril y agosto del 2008 usando la inyección de SQL. La cantidad de vulnerabilidades reportadas a través de este ataque han ido aumentando en los últimos años según el Instituto Nacional de Vulnerabilidades de Estados Unidos de América (Azán, et al., 2014).

Los Sistemas Gestores de Bases de datos (SGBD), al igual que todos los sistemas informáticos, tienen vulnerabilidades que pueden ser aprovechadas por terceras personas no autorizadas para acceder a la información, haciendo que los atacantes centren su esfuerzo en acceder a ella por medio de las diferentes vulnerabilidades contienen los SGBD, las cuales pueden ser causadas por problemas de seguridad en el software o a una mala configuración por parte del administrador de sistemas. (Pérez, 2016).

La información de las empresas se almacena en sistemas gestores de bases de datos. Estos gestores pueden ser vulnerables a ataques externos, internos o a

errores humanos y la información puede verse comprometida y accedida por personas no autorizadas, siendo la información de una institución un activo crítico debe estar protegida, tomando en cuenta todos los mecanismos necesarios para esta sea segura, confidencial, y confiable.

Por los motivos antes mencionados las autoras del presente trabajo plantean la siguiente interrogante:

¿De qué manera se podría proveer estrategias de acción ante vulnerabilidades encontradas en implementaciones de Sistemas Gestores de Bases de Datos?

1.2 JUSTIFICACIÓN

Los trascendentales cambios operados en el mundo moderno, caracterizado por su incesante desarrollo; la acelerada globalización de la economía, la acentuada dependencia que incorpora un alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, imponen nuevos retos a la práctica de la profesión de auditoría, en particular a la auditoría de seguridad Informática (Díaz et al., 2014).

Con la realización de este trabajo se podrán exponer las vulnerabilidades a las que están sujetos los sistemas gestores de gases de datos considerando todos los aspectos necesarios propuestos por la metodología de análisis y gestión de riesgos de los Sistemas de Información Magerit, que permitirá tener una mejor perspectiva al momento de elegir un mejor SGBD.

Partiendo del hecho de que no se evidencia la existencia de que este tipo de investigaciones se han realizado antes, surge la necesidad de llevarlo a cabo, con el fin de contribuir con pautas importantes a tomar en cuenta antes de elegir un SGBD para así lograr que éste cumpla con las necesidades básicas de seguridad y que las organizaciones cuenten con información segura y confiable en el tiempo requerido.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

- Elaborar un plan de mejoras ante las falencias que puedan encontrarse en dos sistemas gestores de bases de datos empleando una herramienta de detección de vulnerabilidades, para contribuir a la seguridad de los sistemas de las organizaciones.

1.3.2. OBJETIVOS ESPECÍFICOS

- Definir los lineamientos para el estudio de los gestores de bases de datos.
- Identificar las vulnerabilidades que pueden afectar el buen desempeño de un gestor de base de datos
- Evaluar los riesgos a los que están expuestos los gestores de bases de datos.
- Establecer un plan de mejoras para el tratamiento de los riesgos a los que están expuestos los gestores de bases de datos.

1.4. HIPÓTESIS/ IDEA A DEFENDER

La elaboración de un plan de mejoras permitirá proveer estrategias de acción ante vulnerabilidades encontradas en los Sistemas Gestores de Bases de Datos

CAPÍTULO II. REVISIÓN BIBLIOGRÁFICA

2.1. SISTEMAS DE BASES DE DATOS

Un sistema de base de datos tiene elementos como una base de datos, un sistema gestor de base de datos consta de hardware, software y personal apropiado para la administración, es decir que un sistema de base de datos es básicamente un sistema computarizado para guardar registros; es decir es un sistema computarizado cuya finalidad general es almacenar información y permitir a los usuarios recuperar y actualizar esa información con base a peticiones (Alaro, 2017)

2.2. SISTEMA GESTOR DE BASES DE DATOS

En la actualidad los Sistemas Gestores de Bases de Datos (SGBD), permiten resolver problemas, brindando a los administradores de la información comodidad y eficiencia en el tratamiento de los datos (Navas et *al.,* 2018), las tareas fundamentales que desempeñan estos sistemas hacen referencia a la seguridad de acceso a los datos, al mantenimiento de la integridad de los datos, a mecanismos de recuperación debidos a fallos físicos y lógicos, al control de concurrencia en el momento de acceder a los datos y a la eficiencia del sistema evaluada, generalmente, en términos del tiempo de respuesta a las consultas de los usuarios (Millán, 2017).

Los Sistemas Gestores de Base de Datos, independientemente del desarrollador de los mismos, deben prestar servicios como:

- **Creación y definición de una Base de Datos:** se refiere al hecho de especificar el tipo de estructura y de datos, las relaciones y restricciones existentes entre los datos almacenados.

- **Manipulación de datos:** permitiendo al usuario realizar consultas, insertar, actualizar o eliminar datos.

- **Control de acceso a los datos almacenados:** mediante mecanismos o políticas de seguridad para permitir o restringir el acceso a los datos por parte de los usuarios.

- **Concurrencia:** mediante esta característica es posible que varios usuarios accedan a los datos a la vez y puedan manipular los mismos.

- **Mantener la integridad y consistencia de los datos**, además de contar con mecanismos que permitan respaldar, exportar y recuperar información. (Arias, 2015)

2.3. COMPONENTES DE LOS GESTORES DE BASES DE DATOS

Según Arias (2015), los Sistemas Gestores de Base de Datos, son programas muy complejos debido a que deben permitir manejar de forma eficiente grandes cantidades de datos, sus componentes principales son los siguientes:

2.3.1. LENGUAJE

Existen varios lenguajes utilizados en diferentes SGBD, los cuales permiten al administrador especificar los datos que componen la Base de datos, la estructura y relaciones que existen en la misma, las reglas y controles de acceso.

2.3.2. DICCIONARIO DE DATOS

Es el lugar en donde se deposita la información acerca de los datos que forman la Base de Datos. “El diccionario contiene las características lógicas de los sitios donde se almacenan los datos del sistema, incluyendo nombre, descripción, alias, contenido y organización”.

- Mecanismos de seguridad e integridad de datos

- Administrador de la Base de Datos

2.4. ARQUITECTURA DE LOS SISTEMAS DE BASES DE DATOS

En 1975, el comité ANSI-SPARC (American National Standard Institute - Standards Planning and Requirements Committee) propuso una arquitectura de tres niveles para los SGBD cuyo objetivo principal era el de separar los programas de aplicación de la BD físico. En esta arquitectura el esquema de una BD se define en tres niveles de abstracción distintos:

*** Nivel interno o físico**: el más cercano al almacenamiento físico, es decir, tal y como están almacenados en el ordenador. Describe la estructura física de la BD mediante un esquema interno. Este esquema se especifica con un modelo físico y describe los detalles de cómo se almacenan físicamente los datos: los archivos que contienen la información, su organización, los métodos de acceso a los registros, los tipos de registros, la longitud, los campos que los componen, etcétera.

• Nivel externo o de visión: es el más cercano a los usuarios, es decir, es donde se describen varios esquemas externos o vistas de usuarios. Cada esquema describe la parte de la BD que interesa a un grupo de usuarios en este nivel se representa la visión individual de un usuario o de un grupo de usuarios.

• Nivel conceptual: describe la estructura de toda la BD para un grupo de usuarios mediante un esquema conceptual. Este esquema describe las entidades, atributos, relaciones, operaciones de los usuarios y restricciones, ocultando los detalles de las estructuras físicas de almacenamiento. Representa la información contenida en la BD. (Grajales, 2015)

2.5. SEGURIDAD DE LA INFORMACIÓN

Montesino *et al., (*2013) determinan que la seguridad informática, o seguridad de la información, es la preservación de la confidencialidad, integridad y disponibilidad de la información. Esto se logra mediante la implantación de un grupo de controles que incluyen políticas, procedimientos, estructuras organizativas y sistemas de hardware y software; La seguridad de la información

en una organización, es un proceso de mejora continua que demanda la participación activa de toda la organización y busca preservar, entre otros, las siguientes características de la información:

- **La confidencialidad:** asegurando que solo las personas debidamente autorizadas tengan acceso a la información.
- **Disponibilidad:** asegurando que la información esté totalmente disponible para las personas debidamente autorizadas cuando ellos la requieran.
- **La integridad:** asegurando que la información no sea modificada sin la debida autorización.
- **La autenticidad:** con el propósito de garantizar la identidad de la persona que genera la información. La autenticidad de la información, es la capacidad de asegurar que el emisor de la información es quien dice ser y no un tercero que esté intentando suplantarlo. (Urrutia *et al.,* 2010)

2.6. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI

Un sistema de gestión de la seguridad informática, se basa en un contexto básico y es que la información es un conjunto de datos establecidos por la entidad de gran valor para esta. La seguridad de la información –según ISO 27001, se basa en protección de sus datos mediante la confidencialidad, integridad y disponibilidad una regla simple dentro de una organización (Briñez, 2018)

2.6.1. VULNERABILIDAD INFORMÁTICA

Según Solarte *et al. (*2015), la seguridad informática está relacionada con las metodologías, procesos y procedimientos para mantener salvaguardada la información y los datos confidenciales de una organización, al interior de los sistemas informáticos. Los procesos se estructuran con el uso de estándares,

normas, protocolos y metodologías para mitigar y minimizar los riesgos asociados a la infraestructura tecnológica.

Por otra parte, Paucar (2017), dice que una vulnerabilidad informática es un error que puede ser aprovechada por un atacante malintencionado con el fin de violar la seguridad del sistema causando daños ya sea robando información, estas son internas las cuales deben ser detectadas por los administradores, dándoles valor para llevar a cabo la reducción de las mismas:

- **Físicas:** Son los puntos débiles que están presentes en el ambiente y los equipos en los que esta almacenada la información.
- **Naturales:** Son los que se relacionan con la naturaleza y ponen en riesgo la información.
- **Hardware:** Defectos que vienen en los equipos cuando fueron fabricados o configurados y estos permiten un ataque o alteración de los mismos.
- **Software:** Debilidad en la aplicación o sistema operativo, accesos no autorizados a los sistemas
- **Medios de almacenamiento:** Son los dispositivos externos en los que se almacena la información.
- **Comunicación:** Abarca la comunicación mediante el tránsito de la información mediante la red.
- **Humanas:** Esta es la vulnerabilidad en la que menos control se tiene ya que el personal humano interno o externo, puede causar daños tanto a la información como a los equipos tecnológicos que la contienen

2.6.2. AMENAZA INFORMÁTICA

Es principalmente la posibilidad de que ocurra algún evento que pueda causar un daño, en la seguridad informática, estas amenazas serian directamente a algún elemento de la red de información, o específicamente donde se encuentre

la información, estas amenazas pueden ser de origen interno u origen externo, un ejemplo de las amenazas de origen externo puede ser un evento natural o un ataque de alguna persona externa, un ejemplo de una amenaza de origen interno puede ser causado por el mismo personal de la organización que comete una negligencia. Hay amenazas como los virus que son muy difíciles de controlar y por esto es tan necesario prevenirlas para lograr contrarrestarlas o minimizar los daños ya que una amenaza surge debido a una vulnerabilidad.

2.6.3. RIESGO INFORMÁTICO

La Organización Internacional de Normalización ISO define riesgo tecnológico como: “La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños” (Peñuela, 2018)

2.7. MAGERIT

La metodología de análisis y gestión de riesgos en su versión 3 contiene tres libros definidos como: Libro I el método, aquí describe la metodología a seguir, buscando una integración de las tareas de análisis de riesgos dentro de un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno,

Libro II, catálogo de elementos, éste permite, por una parte, facilitar la labor de las personas que acometen el proyecto, centrándose en lo específico del sistema objeto del análisis, por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Capitulo tres. Se presume el conocimiento y comprensión de los conceptos de análisis y gestión de riesgos, según se exponen en la guía metodológica. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

Utilizando esta metodología se seguirán los pasos que propone como identificar los activos más importantes de las instituciones, determinar a qué amenazas

están expuestos para establecer medidas que aporte al buen uso y desempeño de las herramientas disponibles.

CAPÍTULO III. DESARROLLO METODOLÓGICO

El presente trabajó consistió en la detección, análisis y gestión de las vulnerabilidades a las que se ven expuestos los sistemas gestores de bases de datos, con el fin de presentar un plan de mejoras que permita dar una visión de las vulnerabilidades a las que se encuentran expuestos. Para el desarrollo de la investigación se la realizó mediante la consecución de objetivos, así como el uso de la metodología para gestión de riesgos Magerit V3.

Cabe mencionar que luego de realizar una evaluación profunda de las herramientas disponibles y al no haber tenido la posibilidad acceder a la normativa ISO 31000 propuesta en el proyecto de titulación para el desarrollo del presente trabajo se consideró oportuno hacer uso de la metodología Magerit, considerándola como la adecuada, ya que el proceso metodológico requiere seguir los mismos pasos, lo cual permite la realización del mismo sin cambiar los objetivos.

Para la realización del presente trabajo se realizaron las siguientes actividades:

3.1. DEFINICIÓN DE LINEAMIENTOS PARA EL ESTUDIO DE LOS GESTORES DE BASE DE DATOS

En esta etapa se realizó la definición de los sistemas gestores de bases de datos objeto de estudio y herramientas de detección de vulnerabilidades, se lo realizó a través de la técnica de revisión bibliográfica, la cual consistió en la búsqueda de información relacionada al tema de estudio, logrando determinar los sistemas gestores de bases de datos de uso frecuente y el escáner de vulnerabilidades de mayor uso, fácil acceso, seguro y de resultados confiables como se detalla en la tabla 1.

Tabla 1: Definición de herramientas de estudio.

Nº	TITULO DEL PROYECTO	APLICACIÓN UTILIZADA PARA LA EVALUCIÓN DE LOS DATOS	SISTEMA GESTOR DE BASE DE DATOS	AUTORES	PAIS
1	Seguridad En Aplicaciones Web	Nessus	MySQL,	(Rodríguez 2014)	España
2	Análisis De Vulnerabilidades En La Red Lan Jerárquica De La Universidad Nacional De Loja, En El Área De La energía, Industrias Y Los Recursos Naturales No Renovables	Nessus OpenVas OWASP Retina	Mysql	(Malla, Et Al., 2016)	Ecuador
3	Desarrollo E Implementación Práctica De Un Pentest	OpenVAS, Nessus y Nexpose	MySQL	(Martí,2016)	España
4	Desarrollo De Practica De Laboratorio Utilizando La Filosofia Hacking Ético Profesional, Para El Apoyo De La Docencia De Las Asignaturas Relacionadas Con La Seguridad Informática Del Departamento De Computación De La Unan-León.	OpenVAS, Nessus, etc	MySQL	(Centeno, 2015)	Nicaragua
5	Desarrollo De Metodología Para Hallazgos De Vulnerabilidades En Redes Corporativas E Intrusiones Controladas.	Tenable Nessus ProfessionalFeed, Nmap ("Network Mapper"), “KALI”, “BackTrack” y “BugTraq”	Postgresq, MYSQL.	(Ortiz, 2015)	Colombia
6	Evaluación De Seguridad A Sistemas De Información En Cuanto A Ataques Maliciosos Con Base En Normatividad, Tendencias, Impacto Y Técnicas Vigentes Para Ambientes Empresariales A Nivel Nacional	Kali Linux (Distribución Linux), Metasploit, OpenVAS, Nessus y Burp Suite	Windows, Linux MacOS	(Alonso,2015)	COLOMBIA
7	Chequeo De Vulnerabilidades De Seguridad En Entidades De Una Red	Nmap, Nessus, GFI LANguard y MBSA	MySQL	(Vera,2012)	Cuba
8	Altair-T: Sistema De Detección Y Gestión De Amenazas Sobre Activos	Nessus, OpenVAS, Retina, Shadow Security Scanner, GFI LANguard N.S.S., SAINT y X-Sca	MySQL, PostgreSQL, Oracle, SQLite o IBM DB2.	(Berlanga, 2012)	
9	Monitoreo De vulnerabilidades En Servicios De Red Para Empresas Con Nagios Implementado	NESSUs, SAINT y OpenVAS	Microsof server sql	(Méndez,2015)	Colombia
10	Análisis De Vunerabilidades Del Sistema Web Siser De Grupo Iusacell, Basado En La Metodología De Ec-Council.	Nessus, Nikto y acunetix	Microsoft server sql, unix	(Blancas, Et Al.,2012)	México

11	Security Testing of Web BasedApplications.	Nessus, Checkmarks, Micro focus Fortify Web Inspect y OWASP ZAP	MySql	(Erdogan, 2009)	USA
12	"Estudio De La Seguridad Informática Y Sus Aplicaciones Para Prevenir La Infiltración De Los Hackers En Las Empresas"	Nessus	Oracle, SQL Server, MySQL, DB2, Informix/DRDA y PostgreSQL.	(Albarracín,2011)	Ecuador
13	Estudio Comparativo De Las Distribuciones Linux Orientado A La Seguridad De Redes De Comunicación	Nessus, OpenVAS, Nexpose entre otros.	MySQL	(Badillo, 2015)	
14	Test De Penetración "Pentesting" Aplicado En Entornos Gnu/Linux En Una Empresa Guatemalteca	Nessu	Mysql	(De León, 2017)	Guatemala
15	Diseño De Procedimientos De Seguridad Basados En Pruebas De Pentesting Aplicadas A La Empresa Cjt&T Ingeniería De Software	Nessus, Nexpose y otros	MySQL, Microsoft SQL Server	(López, 2017)	COLOMBIA
16	Escaneo De Vulnerabilidades Al Servidor Principal De La Empresa Caso De Estudio	OPENVAS, NESSUS, NMAP y Microsoft Baseline Security	Microsoft SQL Server	(Ramirez & Avila, 2018)	Colombia
17	Hacking Ético Para Analizar Y Evaluar La Seguridad Informática En La Infraestructura De La Empresa Plasticaucho Industrial S.A.	Nessus, OpenVAS	Windows Server	(Rojas, 2018).	Ecuador
18	Cloud Vulnerability Assessment	Nessus, OpenVAS, Nexpose	MySQL	(Ayenson,2012)	
19	Diseño De Un Protocolo Para La Detección De Vulnerabilidades En Los Principales Servidores De La Superintendencia De Puertos Y Transportes.	Nessus OpenVAS Metasploit, Wireshark, John the Ripper, TCH-Hydra, Nmap ("Network Mapper"), TheHarvester.	Mysql, Oracle	(Meneses & Llanos, 2016).	Colombia
20	Laboratorio Virtual Para El Estudio De Vulnerabilidades En La Nube	Nessus, OpenVAS	Mysql	(Llorente,2016)	España
21	A Contactless 'Active' Reconnaissance Known Vulnerability Assessment Tool	Nessus, OpenVAS	PostgreSQL, MYSQL, MS-SQL	(Hare, 2018)	Reino Unido
22	Estudio de seguridad informática para las bases de datos del Campus virtual de la unad.	Nessus, Nmap, SQL Map, entre otras	Oracle, MySQL, SQL Server, PostGreSQL	(Uribe, 2016)	COLOMBIA
23	Web Platform for Auditing as a Service	OpenVAS Nessus Acunetix	MySQL.	(Llobet, 2017)	ESPAÑA
24	Vulnerabilidades de los relojes biométricos en los	foram o Nessus, o OWASP ZAP e o w3af	MYSQL	(Teran y Fonseca,2013)	ECUADOR

	Registros del personal para la protección de la Información en determinadas empresas de ambato				
25	A Web Interface for Nessus Network Security Scanner	NESSUS	MySQL.	(Chen & Matthews,2004)	USA
26	Diseño de un plan estrategico para la seguridad de la Información tributaria en una entidad publica	Nessus	SQLMAP, MYSQL	(Rodriguez & Rozo, 2015)	COLOMBIA
27	Diagnóstico de la seguridad informática de la red de datos de la Empresa sunshine bouquet zona norte bogotá, colombia	NESSUS, NMAP	Ubuntu, y Windows server	(López, 2017)	COLOMBIA
28	Sistema de deteccão de vulnerabilidade em aplicacões instaladas em sistemas Windows	Nessus, OpenVAS	MySQL	(Monteiro, 2016)	BRAZIL

Fuente: Las autoras.

3.2. IDENTIFICACIÓN DE LAS AMENAZAS QUE AFECTAN EL DESEMPEÑO DE LOS GESTORES DE BASE DE DATOS

Luego de establecer los gestores a evaluar y la herramienta a utilizar se procedió a hacer la identificación de las amenazas a las que están expuestos los sistemas gestores de bases de datos, utilizando estructura de la metodología Magerit V.3 para el establecimiento de las mismas, siguiendo el proceso metodológico indicado se realizaron los siguientes pasos:

- ✓ Identificación de los activos
- ✓ Dependencia de activos
- ✓ Identificación de las amenazas
- ✓ Valoración cualitativa de las amenazas
- ✓ Valoración cuantitativa de las amenazas
- ✓ Análisis mediante tablas

3.2.1. IDENTIFICACIÓN DE LOS ACTIVOS

Se determino que como activo a evaluar se emplearán únicamente los sistemas Gestores de Base de Datos, debido a que el trabajo está dirigido a identificar las

amenazas y el riesgo a las que se encuentran expuestos y que afectan a su buen funcionamiento.

3.2.2. DEPENDENCIA DE ACTIVOS

En este gráfico de evidencia la forma en que las que las amenazas penetran en el sistema gestor de base de datos, en este caso para llegar a él o a las aplicaciones, estas deben ingresan en primer plano a atacar al servidor de seguridad, si éste no la detecta avanza con el fin de vulnerar el gestor y acceder a la base de datos o a las aplicaciones de la empresa.

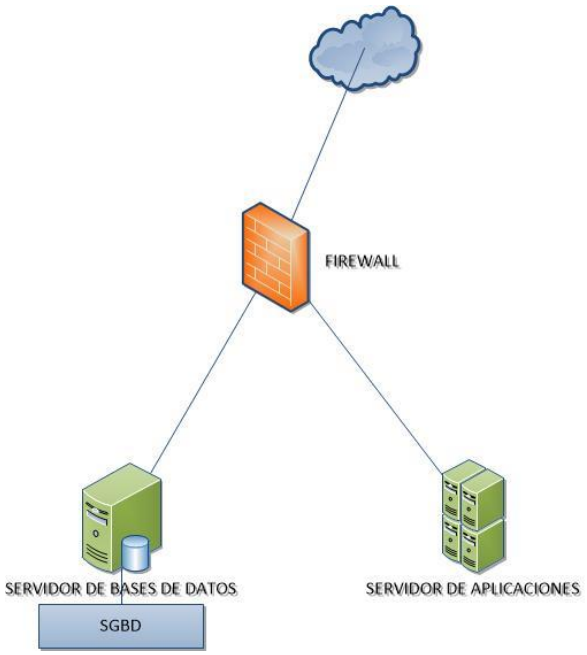


Gráfico 1: Dependencia de Activos

Fuente: Las autoras.

3.2.3 IDENTIFICACIÓN DE LAS AMENAZAS

Una vez establecidos los activos se procede a la identificación de las amenazas a las que están expuestos, considerado los aspectos descritos por la metodología, considerando únicamente los que afecten a los sistemas gestores de bases de datos, estos son:

[A.] Ataques Intencionados

- Manipulación de registro de actividades (log)
- Manipulación de los ficheros de configuración
- Suplantación de identidad del usuario
- Abuso de privilegios de acceso
- Uso no previsto
- Difusión de Software dañino
- (re) encaminamiento de mensajes
- Alteración de secuencia
- Acceso no autorizado
- Interceptación de información (escucha)
- Manipulación de programas
- Denegación de Servicio

[I.] De Origen Industrial

- Avería de origen físico o lógico
- Fallo de servicio de comunicaciones
- Degradación de los soportes de almacenamiento de la información

[E.] Errores y Fallos no intencionados

- Errores de los usuarios
- Errores del Administrador
- Errores de monitorización (Log)

- Errores de configuración
- Difusión de Software dañino
- Errores de (re)encaminamiento
- Errores de secuencia
- Alteración accidental de la información
- Vulnerabilidades de los programas (software)
- Errores de Mantenimiento / Actualización de Equipos
- Caída del sistema por agotamiento de recursos

Una vez establecidas las amenazas, se procedió a la estimación del riesgo al que se encuentran expuestos los gestores y el impacto que causaría su materialización, esto se lo hizo de forma cualitativa y cuantitativa, con el fin de estimar el nivel de exposición al riesgo al que están sujetos los gestores de bases de datos objeto de estudio.

3.2.3.1. VALORACIÓN CUALITATIVA DE LAS AMENAZAS

Se determinó de la probabilidad de ocurrencia considerando las secuencias descritas en la metodología Magerit:

Tabla 2: Probabilidad de ocurrencia

DEFINICIÓN	SIGLAS
Poco Frecuente (cada varios años)	PF
Frecuencia Normal (una vez al año)	FN
Frecuente (una vez al mes)	F

Fuente: Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

Así mismo se determinó el impacto que tendría si se materializa la amenaza:

Tabla 3: Impacto

DEFINICIÓN	SIGLAS
Bajo (sin consecuencias relevantes)	B
Medio (consecuencias reseñables para la organización)	M
Alto (consecuencias graves)	A

Fuente: Ministerio de Hacienda y Administraciones Públicas de España, 2012

Tomando en consideración las definiciones que propone Magerit, se estimó por cada amenaza tanto la probabilidad de ocurrencia como el impacto que causaría su materialización, considerando cada uno de los aspectos señalados en las tablas con el fin de obtener como resultado el factor de riesgo al que se está expuesto.

3.2.3.2. VALORACION CUANTITATIVA DE LAS AMENAZAS

Se determinó la valoración cuantitativa, la cual consiste en darle un valor numérico a cada amenaza tanto para la probabilidad de ocurrencia, como para el impacto con los siguientes valores, sugeridos por la metodología:

Tabla 4: Probabilidad de ocurrencia.

DEFINICIÓN	VALOR
Poco Frecuente (cada varios años)	1
Frecuencia Normal (una vez al año)	2
Frecuente (una vez al mes)	3

Fuente: Ministerio de Hacienda y Administraciones Públicas de España, 2012

Tabla 5: Impacto.

DEFINICIÓN	VALOR
Bajo (sin consecuencias relevantes)	1
Medio (consecuencias reseñables para la organización)	2
Alto (consecuencias graves)	3

Fuente Ministerio de Hacienda y Administraciones Públicas de España, 2012

Con estos valores numéricos asignados se procedió al cálculo de la exposición al riesgo y para a partir de este resultado a determinar las mejoras, el proceso fue el siguiente:

- Se calculó el valor del impacto, considerando los valores asignados de acuerdo a cada amenaza.

Impacto = Valor Activo * Degradación

- Con el resultado obtenido del cálculo anterior se calculó el riesgo.

Riesgo= Impacto * Probabilidad de Ocurrencia

De acuerdo a los criterios de valoración sugeridos por la metodología se asignaron los niveles de criticidad como se detalla en la tabla 6.

Tabla 6: Criterios de valoración

VALOR	NIVEL	CRITERIO
6-8	Alto	Daños graves
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos.

Fuente: Ministerio de Hacienda y Administraciones Públicas de España, 2012

Cabe mencionar que los valores de 0 que resultan irrelevantes para efectos prácticos, suelen darse por errores cometidos por personal de la institución, sea por falta de experiencia o por causas ajenas a su voluntad, por lo tanto, la

metodología propone que las amenazas que sean de tipo error, tomen el valor de 0 siendo estas despreciables.

3.2.4. ANÁLISIS MEDIANTE TABLAS

Luego de haber realizado la identificación de las amenazas se realizaron las matrices para determinar los riesgos a los que se exponen los sistemas gestores de bases de datos, tomando en consideración las estimaciones anteriores en el análisis cualitativo, es decir, es la representación gráfica del análisis realizado, tomando en consideración el modelo propuesto por la metodología.

Tabla 7: Matriz para estimar la valoración del impacto

ESTIMACIÓN DEL IMPACTO				
IMPACTO		DEGRADACIÓN		
		1%	10%	100%
VALOR	A	B	M	A
	M	MB	B	M
	B	MB	MB	B

Fuente: Ministerio de Hacienda y Administraciones Públicas de España, 2012

Tabla 8: Matriz para estimar la valoración del riesgo.

ESTIMACIÓN DEL RIESGO				
RIESGO		FRECUENCIA		
		PF	FN	F
IMPACTO	A	B	M	A
	M	MB	B	M
	B	MB	MB	B

Fuente: Ministerio de Hacienda y Administraciones Públicas de España, 2012

3.3. EVALUAR LOS RIESGOS A LOS QUE ESTÁN EXPUESTOS LOS GESTORES DE BASES DE DATOS

Se procedió a realizar el análisis de vulnerabilidades de los sistemas gestores de bases de datos utilizando la herramienta Nessus previamente establecida.

Una vez realizado el escaneo a los dos gestores de bases de datos objeto de estudio y obtenidas las vulnerabilidades a las que se encuentran expuestos, se

consideró necesario realizar el mismo procedimiento de escaneo con la herramienta Nexpose, con el fin de comparar los resultados obtenidos en cada herramienta.

Este procedimiento se llevó a cabo utilizando una computadora de marca HP con un procesador AMD A12-9720 RADEON, 12 COMPUTE 4C+8G 2,70 GHz, con una memoria RAM 12.0GB, un sistema de 64 bits, procesador x64; sobre la cual se instalaron 2 maquinas virtuales con las siguientes características: disco duro de 100GB y memoria de 1024 tanto para CentOS Linux release 7 como para operativo Linux Kernel 3.10 on CentOS Linux release 7.

3.4. ESTABLECER UN PLAN DE MEJORAS PARA EL TRATAMIENTO DE LOS RIESGOS A LOS QUE ESTÁN EXPUESTOS LOS GESTORES DE BASES DE DATOS

En esta etapa se llevó a cabo la elaboración de un plan de mejoras a partir de las amenazas detectadas y el riesgo que representa su materialización, en el caso de las vulnerabilidades detectadas con la metodología Magerit las mejoras han sido seleccionadas por las autoras, en el caso de las vulnerabilidades halladas por las herramientas Nessus y Nexpose incluyen entre sus resultados la solución a las amenazas encontradas.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

En el proceso realizado para definir los lineamientos para el estudio de los gestores de bases de datos se obtuvo como primer resultado que los dos sistemas gestores de bases de datos más utilizados son MySQL y Microsoft SQL Server de acuerdo a la tabulación de los datos realizada como se expresa en la tabla 9:

Tabla 9: Sistema Gestores de bases de datos más utilizados en los trabajos consultados.

SGBD	% DE USO
MySQL	44,47
Microsoft SQL Server	14,29
PostgreSQL	10,2
Oracle	8,6
Windows Server	4,08
Windows	2,04
Linux	2,04
Mac OS	2,04
SQ Lite	2,04
Unix	2,04
DB2	2,04
Informix	2,04
SQLmap	2,04
Ubuntu	2,04

Fuente: Revisión bibliográfica.

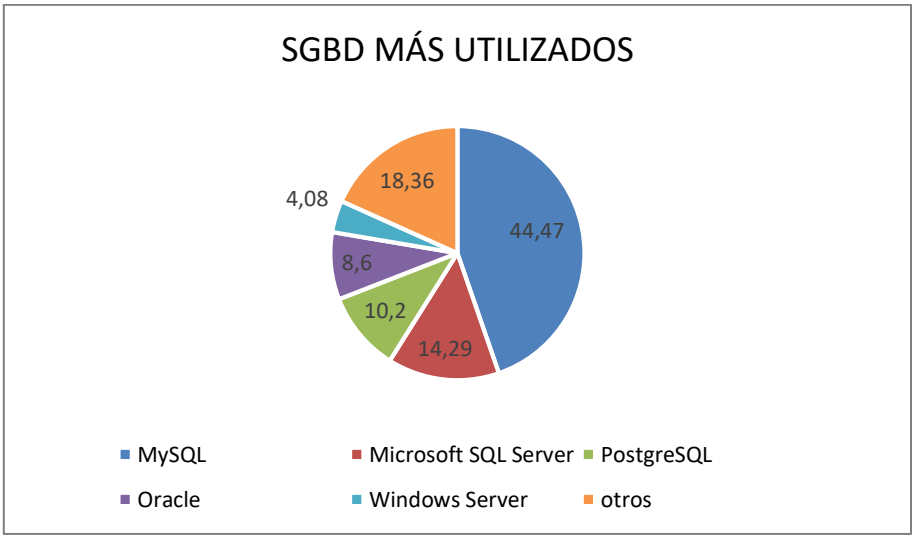


Gráfico 2: SGBD más utilizados.

Fuente: Las Autoras.

Los dos Sistemas Gestores de Bases de Datos escogidos para el análisis de vulnerabilidades son: MySQL Server, Microsoft SQL Server, ya que son gestores robustos y que brindan las características que las instituciones necesitan para alojar su información, son robustos, de fácil acceso, seguros y confiables, también aparecen otros como PostgreSQL con el 10,2% de uso, Oracle con un 8.6% Windows Server con un 4,08% y Windows con el 2,04%, Linux 2,04%, Mac OS 2,04%, SQ Lite 2,04%, Unix 2,04%, DB2 2,04%, Informix 2,04%, SQLmap 2,04%, Ubuntu 2,04% que entre todos conforman el campo de otros y hacen un total del 18.36%.

Como resultado de la misma revisión bibliográfica, en la tabla 10 se detallan los escáners de vulnerabilidades más utilizados:

Tabla 10: Escáners de vulnerabilidad más utilizados.

SCANNER	PORCENTAJE
Nessus	36,97
Open Vas	19,82
Nexpose	4,5
Nmap	8,11

Metasploit	2,7
GFI LanGuard	2,7
Kali	2,7
OWASP	2,7
Burp Suite	1,8
Wireshark	1,8
Retina	1,8
Acunetix	1,8
Linux	0,9
Shadow Security Scanner	0,9
NSS	0,9
Microsoft Baseline Security Analyzer	0,9
Tcpdump	0,9
Checkmarx	0,9
Micro focus	0,9
Fortify webinspect	0,9
U de Scanner	0,9
SAINT	0,9
John the Ripper	0,9
TCH Dydra	0,9
NMap	0,9
Mapper	0,9

Fuente: Las Autoras

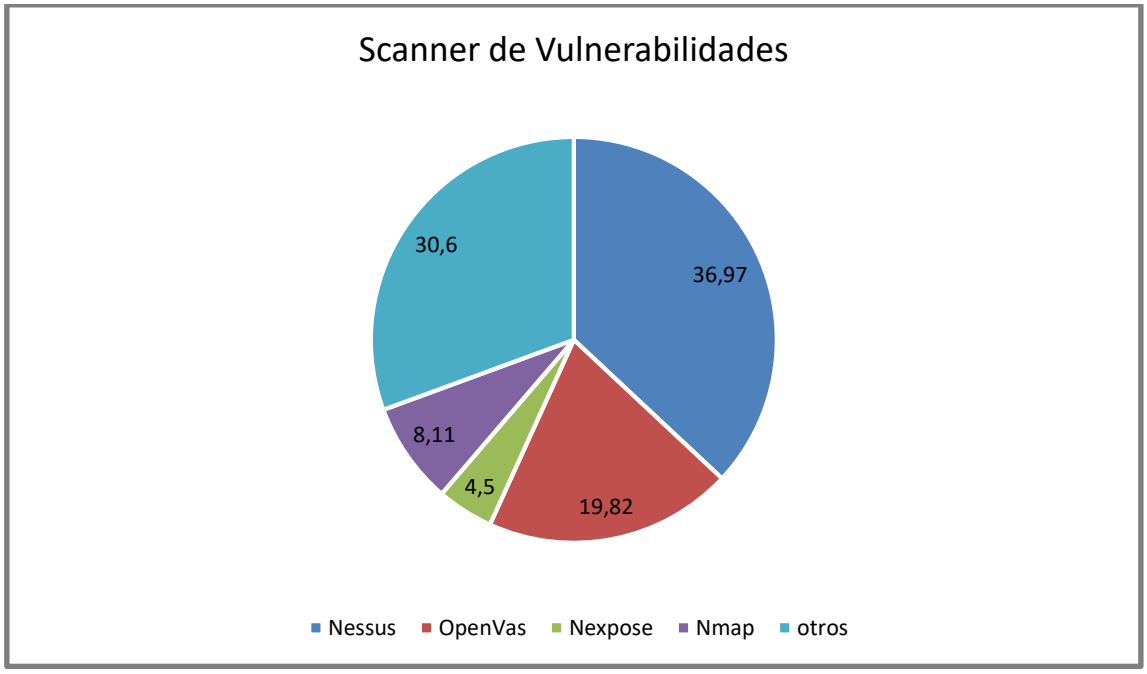


Gráfico 3: Escáners de vulnerabilidad más utilizados

Fuente: Las Autoras

Una vez analizados los datos obtenidos, se determinó que Nessus es el scanner de vulnerabilidades más utilizado, ya que es una herramienta completa de uso frecuente para determinar falencias en gestores de bases de datos, sistemas operativos, sistemas de información, entre otros, a diferencia de otras que se utilizan como Open Vas (19,82%), Nexpose (4,5%), Nmap (8,11%), que se utilizan en menor escala y están también otras herramientas como: Metasploit 2,7%, GFI LanGuard 2,7%, Kali 2,7%, OWASP 2,7%, Burp Suite 1,8%, Wireshark 1,8%, Retina 1,8%, Acunetix 1,8%, Li nux 1,8%, Shadow 1,8%, Security Scanner 1,8%, NSS 1,8%, Microsoft Baseline Security Analyzer 1,8%, Tcpdump 1,8%, Checkmarx 1,8%, Micro focus 1,8%, Fortify webinspect 1,8%, U de Scanner 1,8%, SAINT, John the Rippe 1,8%, TCH Dydra 1,8%, NMap 1,8%, Mapper 1,8%, que se utilizan en menor frecuencia que los otros scanners de vulnerabilidades y entre ellos suman un total de 30.6%

Luego de realizada la revisión bibliográfica se estableció que los SGBD a evaluar son: MySQL Server, Microsoft SQL Server, y el scanner de vulnerabilidades a utilizar es Nessus debido al gran uso de esta herramienta y sus incidencias en el desarrollo de las actividades realizadas.

Una vez establecidos los gestores y la herramienta a utilizar, se procedió a la identificación de las potenciales amenazas, sugeridas por la metodología utilizada Magerit, que afectan su buen funcionamiento, además de la estimación del impacto (Anexo 1) y del riesgo (Anexo 2) las cuales se realizaron a través de matrices de riesgo impacto.

En la tabla 11 se puede apreciar el listado de las amenazas potenciales que afectan en el buen funcionamiento de los sistemas gestores de bases de datos con su estimación tanto cualitativa como cuantitativa de cada amenaza.

Tabla 11: Potenciales Amenazas, estimación del impacto.

			IMPACTO						
NOMBRE	**CÓDIGO**	**AMENAZA**	**P.O NUM**	**P.O**	**SIGLAS**	**I. NUM**	**DEGRADACIÓN**	**SIGLAS**	**IMPACTO**
SISTEMA DE GESTIÓN DE BASE DE DATOS	I. 5	Avería de origen físico o lógico	2	Medio	**M**	2	Alto	**A**	4
	I.8	Fallo de servicio de comunicaciones	2	Alto	**A**	1	Bajo	**B**	3
	I.10	Degradación de los soportes de almacenamiento de la información	3	Alto	**A**	2	Medio	**M**	6
	E. 1	Errores de los usuarios	1	Bajo	**A**	0	Bajo	**B**	0
	E.2	Errores del Administrador	1	Bajo	**A**	0	Bajo	**B**	0
	E.3	Errores de monitorización (Log)	1	Bajo	**A**	0	Bajo	**B**	0
	E. 4	Errores de configuración	1	Bajo	**A**	0	Bajo	**B**	0
	E.8	Difusión de Software dañino	2	Medio	**M**	2	Alto	**A**	4
	E.9	Errores de (re)encaminamiento	2	Medio	**M**	0	Bajo	**B**	0
	E. 10	Errores de secuencia	2	Medio	**M**	0	Bajo	**B**	0
	E.15	Alteración accidental de la información	3	Alto	**A**	3	Alto	**A**	9
	E. 20	Vulnerabilidades de los programas (software)	3	Alto	**A**	3	Alto	**A**	9
	E.21	Errores de Mantenimiento / Actualización de Equipos	1	Bajo	**A**	3	Alto	**A**	3
	E.24	Caída del sistema por agotamiento de recursos	2	Medio	**M**	2	Alto	**M**	4
	A. 3	Manipulación de registro de actividades (log)	3	Alto	**A**	3	Alto	**A**	9
	A. 4	Manipulación de los ficheros de configuración	3	Alto	**A**	3	Alto	**A**	9
	A.5	Suplantación de identidad del usuario	3	Alto	**A**	2	Medio	**M**	6
	A.6	Abuso de privilegios de acceso	3	Alto	**A**	2	Medio	**M**	6
	A.7	Uso no previsto	2	Medio	**M**	2	Medio	**M**	4
	A. 8	Difusión de Software dañino	3	Alto	**A**	3	Alto	**A**	9
	A. 9	(re) encaminamiento de mensajes	3	Alto	**A**	2	Medio	**M**	6
	A 10	Alteración de secuencia	2	Medio	**M**	2	Medio	**M**	4
	A.11	Acceso no autorizado	3	Alto	**A**	2	Medio	**M**	6
	A.14	interceptación de información (escucha)	3	Alto	**A**	2	Medio	**M**	6
	A.22	Manipulación de programas	3	Alto	**A**	2	Medio	**M**	6
	A.24	Denegación de Servicio	3	Alto	**A**	3	Alto	**A**	9

Fuente: Las Autoras.

Tabla 12: Potenciales Amenazas, estimación del riesgo.

						RIESGO				
NOMBRE	CÓDIGO	AMENAZA	P.O NUM	P. OCURRENCIA	SIGLAS	I. RESULTANTE	IMPACTO	SIGLAS	RIESGO	RIESGO
SISTEMA DE GESTIÓN DE BASE DE DATOS	I. 5	Avería de origen físico o lógico	2	Frecuencia normal	FN	4	Alto	A	Alto	8
	I.8	Fallo de servicio de comunicaciones	2	Frecuencia normal	FN	2	Medio	M	Medio	4
	I.10	Degradación de los soportes de almacenamiento de la información	1	Poco frecuente	PF	6	Alto	A	Medio	6
	E. 1	Errores de los usuarios	2	Frecuencia normal	FN	0	Despreciable	D	Medio	0
	E.2	Errores del Administrador	2	Frecuencia normal	FN	0	Despreciable	D	Medio	0
	E.3	Errores de monitorización (Log)	2	Frecuencia normal	FN	0	Despreciable	D	Medio	0
	E. 4	Errores de configuración	2	Frecuencia normal	FN	0	Despreciable	D	Medio	0
	E.8	Difusión de Software dañino	2	Frecuencia normal	FN	4	Alto	A	Alto	8
	E.9	Errores de (re)encaminamiento	1	Poco frecuente	PF	0	Despreciable	D	Bajo	0
	E. 10	Errores de secuencia	1	Poco frecuente	PF	0	Despreciable	D	Bajo	0
	E.15	Alteración accidental de la información	1	Poco frecuente	PF	9	Muy Alto	MA	Muy Alto	9
	E. 20	Vulnerabilidades de los programas (software)	2	Frecuencia normal	FN	9	Muy Alto	MA	Muy Alto	18
	E.21	Errores de Mantenimiento / Actualización de Equipos	2	Frecuencia normal	FN	3	Medio	M	Muy Alto	6
	E.24	Caída del sistema por agotamiento de recursos	1	Poco frecuente	PF	4	Medio	M	Medio	4
	A. 3	Manipulación de registro de actividades (log)	2	Frecuencia normal	FN	9	Muy Alto	MA	Alto	18
	A. 4	Manipulación de los ficheros de configuración	1	Poco frecuente	PF	9	Muy Alto	MA	Muy Alto	9
	A.5	Suplantación de identidad del usuario	2	Frecuencia normal	FN	6	Alto	A	Alto	12
	A.6	Abuso de privilegios de acceso	2	Frecuencia normal	FN	6	Alto	A	Alto	12
	A.7	Uso no previsto	2	Frecuencia normal	FN	4	Medio	M	Medio	8
	A. 8	Difusión de Software dañino	2	Frecuencia normal	FN	9	Muy Alto	MA	Muy Alto	18
	A. 9	(re) encaminamiento de mensajes	2	Frecuencia normal	FN	6	Alto	A	Alto	12
	A 10	Alteración de secuencia	2	Frecuencia normal	FN	4	Medio	M	Medio	8
	A.11	Acceso no autorizado	2	Frecuencia normal	FN	6	Alto	A	Alto	12
	A.14	interceptación de información (escucha)	2	Frecuencia normal	FN	6	Alto	A	Alto	12
	A.22	Manipulación de programas	2	Frecuencia normal	FN	6	Alto	A	Alto	12
	A.24	Denegación de Servicio	2	Frecuencia normal	FN	9	Muy Alto	MA	Muy Alto	18
									MEDIA	8,23
									MEDIANA	8

Fuente: Las Autoras.

En la tabla 12 se procedió a la estimación del riesgo cuantitativo y cualitativo de cada amenaza, con el fin de obtener la mediana de los valores de riesgo obtenidos, esta toma el nombre de exposición al riesgo cuyo valor es de **8** evidenciando un nivel de riesgo **ALTO,** de acuerdo a los criterios de valoración establecidos por la metodología Tabla 6.

Una vez calculada la exposición al riesgo, se procedió de acuerdo a lo descrito por Magerit a la toma de decisión de tratamiento del riesgo, siendo estas las detalladas a continuación en la tabla 13.

Tabla 13: Decisión de tratamiento de riesgo.

COD.	AMENAZA	IMPACTO	RIESGO	P. DE OCURRENCIA	TRATAMIENTO DEL RIESGO
I. 5	Avería de origen físico o lógico	Alto	Alto	Frecuencia normal	Evita
I.8	Fallo de servicio de comunicaciones	Medio	Medio	Frecuencia normal	Evita
I.10	Degradación de los soportes de almacenamiento de la información	Alto	Medio	Poco frecuente	Evita
E. 1	Errores de los usuarios	Despreciable	Medio	Frecuencia normal	Reduce
E.2	Errores del Administrador	Despreciable	Medio	Frecuencia normal	Reduce
E.3	Errores de monitorización (Log)	Despreciable	Medio	Frecuencia normal	Evita
E. 4	Errores de configuración	Despreciable	Medio	Frecuencia normal	Evita
E.8	Difusión de Software dañino	Alto	Alto	Frecuencia normal	Elimina
E.9	Errores de (re)encaminamiento	Despreciable	Bajo	Poco frecuente	Reduce
E. 10	Errores de secuencia	Despreciable	Bajo	Poco frecuente	Acepta
E.15	Alteración accidental de la información	Muy Alto	Muy Alto	Poco frecuente	Reduce
E. 20	Vulnerabilidades de los programas (software)	Muy Alto	Muy Alto	Frecuencia normal	Elimina
E.21	Errores de Mantenimiento / Actualización de Equipos	Medio	Muy Alto	Frecuencia normal	Reduce
E.24	Caída del sistema por agotamiento de recursos	Medio	Medio	Poco frecuente	Evita
A. 3	Manipulación de registro de actividades (log)	Muy Alto	Alto	Frecuencia normal	Elimina
A. 4	Manipulación de los ficheros de configuración	Muy Alto	Muy Alto	Poco frecuente	Reduce
A.5	Suplantación de identidad del usuario	Alto	Alto	Frecuencia normal	Elimina
A.6	Abuso de privilegios de acceso	Alto	Alto	Frecuencia normal	Reduce
A.7	Uso no previsto	Medio	Medio	Frecuencia normal	Acepta
A. 8	Difusión de Software dañino	Muy Alto	Muy Alto	Frecuencia normal	Elimina
A. 9	(re) encaminamiento de mensajes	Alto	Alto	Frecuencia normal	Elimina
A 10	Alteración de secuencia	Medio	Medio	Frecuencia normal	Evita
A.11	Acceso no autorizado	Alto	Alto	Frecuencia normal	Reduce
A.14	Interceptación de información (escucha)	Alto	Alto	Frecuencia normal	Evita
A.22	Manipulación de programas	Alto	Alto	Frecuencia normal	Reduce
A.24	Denegación de Servicio	Muy Alto	Muy Alto	Frecuencia normal	Elimina

Fuente: Las Autoras.

Una vez realizado el escaneo con la herramienta propuesta NESSUS, se obtuvo como resultado 2 vulnerabilidades una de nivel medio y una de nivel bajo correspondiente a MySQL, que se evidencian en la tabla 14.

Tabla 14: Vulnerabilidades obtenidas con Nessus (MySQL)

VULNERABILIDAD	NIVEL
11213 - Métodos HTTP TRACE / TRACK permitidos	Medio
70658 - Cifras en modo CBC del servidor SSH habilitadas	Bajo

Fuente: Nessus.

Utilizando la misma herramienta Nessus, se realizó el escaneo en el gestor Microsoft SQLServer obteniendo los siguientes datos: 2 vulnerabilidades de nivel medio como se evidencia en la tabla 15.

Tabla 15: Vulnerabilidades obtenidas con Nessus (MySQL)

VULNERABILIDAD	NIVEL
90510 - MS16-047: Actualización de seguridad para los protocolos remotos SAM y LSAD (3148527) (bloqueo) (verificación sin credenciales)	Medio
57608 - No se requiere firma SMB	Medio

Fuente: Nessus.

Una vez realizado el escaneo con Nessus, se realizó el mismo procedimiento utilizando la herramienta Nexpose que es otra herramienta de escaneo de vulnerabilidades, con la finalidad de comparar los resultados obtenidos con Nessus, obteniendo como resultado en MySQL un total de 73 vulnerabilidades, 3 altas, 68 de nivel medio y 2 de nivel bajo, como se evidencia en la tabla 16.

Tabla 16: Vulnerabilidades obtenidas con Nexpose (MySQL).

VULNERABILIDAD	NIVEL
Apache HTTPD: Ap_get_basic_auth_pw () Omisión de autenticación (CVE-2017-3167) (apache-httpd-cve-2017-3167)	Alto
Apache HTTPD: mod_ssl Dereferencia de puntero nulo (CVE-2017-3169) (apache-httpd-cve-2017-3169)	Alto
Apache HTTPD: Mod_mime Buffer Overread (CVE-2017-7679) (apache-httpd-cve-2017-7679)	Alto
Apache HTTPD: mod_status desbordamiento de búfer (CVE-2014-0226) (apache-httpd-cve-2014-0226)	Media
Apache HTTPD: omitir <FilesMatch> con una nueva línea final en el nombre del archivo (CVE-2017-15715) (apache-httpd-cve-2017-15715)	Media
Apache HTTPD: generación de autenticación de débiles compilaciones en mod_auth_digest (CVE-2018-1312) (apache-httpd-cve-2018-1312)	Media
Vulnerabilidad de PHP: CVE-2015-9253 (php-cve-2015-9253)	Media
Apache HTTPD: Reflexión de la memoria sin inicializar en mod_auth_digest (CVE-2017-9788) (apache-httpd-cve-2017-9788)	Media
Método HTTP TRACE habilitado (http-trace-method-enabled)	Media
Vulnerabilidad de Oracle MySQL: CVE-2018-3185 (oracle-mysql-cve-2018-3185)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3187 (oracle-mysql-cve-2018-3187)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3247 (oracle-mysql-cve-2018-3247)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2019-2534 (oracle-mysql-cve-2019-2534)	Media
Apache HTTPD: Derivación de procesamiento de HTTP Trailers (CVE-2013-5704) (apache-httpd-cve-2013-5704)	Media
Apache HTTPD: mod_dav crash (CVE-2013-6438) (apache-httpd-cve-2013-6438)	Media
Apache HTTPD: mod_log_config crash (CVE-2014-0098) (apache-httpd-cve-2014-0098)	Media
Apache HTTPD: mod_cgid denegación de servicio (CVE-2014-0231) (apache-httpd-cve-2014-0231)	Media
Apache HTTPD: bloqueo de mod_cache con el encabezado Content-Type vacío (CVE-2014-3581) (apache-httpd-cve-2014-3581)	Media
Apache HTTPD: ataque de contrabando de solicitudes HTTP contra analizador de solicitudes fragmentadas (CVE-2015-3183) (apache-httpd-cve-2015-3183)	Media
Apache HTTPD: Relleno de Oracle en Apache mod_session_crypto (CVE-2016-0736) (apache-httpd-cve-2016-0736)	Media
Apache HTTPD: Vulnerabilidad de DoS en mod_auth_digest (CVE-2016-2161) (apache-httpd-cve-2016-2161)	Media
Apache HTTPD: Mitigación de entorno HTTP_PROXY "httpoxy" (CVE-2016-5387) (apache-httpd-cve-2016-5387)	Media

Apache HTTPD: Solicitud HTTP de Apache que analiza los defectos de los espacios en blanco (CVE-2016-8743) (apache-httpd-cve-2016-8743)	Media
Apache HTTPD: Escritura fuera de límite en mod_authnz_ldap cuando se usan valores de Accept-Language demasiado pequeños (CVE-2017-15710) (apache-httpd-cve-2017-15710)	Media
Apache HTTPD: uso después de usar cuando se usa <Limit> con un método no reconocido en .htaccess ("OptionsBleed") (CVE-2017-9798) (apache-httpd-cve-2017-9798)	Media
Apache HTTPD: posible lectura fuera de límite en mod_cache_socache (CVE-2018-1303) (apache-httpd-cve-2018-1303)	Media
Base de datos de acceso abierto (base de datos de acceso abierto)	Media
Instalación predeterminada de Apache / página de bienvenida instalada (http-apache-default-install-page)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3171 (oracle-mysql-cve-2018-3171)	Media
Vulnerabilidad de PHP: CVE-2018-19396 (php-cve-2018-19396)	Media
Vulnerabilidad de PHP: CVE-2018-19935 (php-cve-2018-19935)	Media
Apache HTTPD: bloqueo de mod_cache (CVE-2013-4352) (apache-httpd-cve-2013-4352)	Media
Apache HTTPD: mod_proxy denegación de servicio (CVE-2014-0117) (apache-httpd-cve-2014-0117)	Media
Apache HTTPD: mod_deflate denegación de servicio (CVE-2014-0118) (apache-httpd-cve-2014-0118)	Media
Apache HTTPD: mod_lua múltiple "Require" el manejo de directivas no funciona (CVE-2014-8109) (apache-httpd-cve-2014-8109)	Media
Apache HTTPD: ap_some_auth_required API inutilizable (CVE-2015-3185) (apache-httpd-cve-2015-3185)	Media
Apache HTTPD: inyección mod_userdir CRLF (CVE-2016-4975) (apache-httpd-cve-2016-4975)	Media
Apache HTTPD: manipulación de datos mod_session para aplicaciones CGI (CVE-2018-1283) (apache-httpd-cve-2018-1283)	Media
Apache HTTPD: posible acceso fuera de enlace después de un error en la lectura de la solicitud HTTP (CVE-2018-1301) (apache-httpd-cve-2018-1301)	Media
Apache HTTPD: mod_session_cookie no respeta el tiempo de caducidad (CVE-2018-17199) (apache-httpd-cve-2018-17199)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3133 (oracle-mysql-cve-2018-3133)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3143 (oracle-mysql-cve-2018-3143)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3144 (oracle-mysql-cve-2018-3144)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3155 (oracle-mysql-cve-2018-3155)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3156 (oracle-mysql-cve-2018-3156)	Media
Vulnerabilidad de Oracle MySQL: CVE-2018-3161 (oracle-mysql-cve-2018-3161)	Media

Vulnerabilidad de Oracle MySQL: CVE-2018-3162 (oracle-mysql-cve-2018-3162)	Media
Vulnerabilidad de Oracle MySQL: CVE-2018-3173 (oracle-mysql-cve-2018-3173)	Media
Vulnerabilidad en MySQL de Oracle: CVE-2018-3200 (oracle-mysql-cve-2018-3200)	Media
Vulnerabilidad de Oracle MySQL: CVE-2018-3251 (oracle-mysql-cve-2018-3251)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3276 (oracle-mysql-cve-2018-3276)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3277 (oracle-mysql-cve-2018-3277)	Media
Vulnerabilidad en MySQL de Oracle: CVE-2018-3278 (oracle-mysql-cve-2018-3278)	Media
Vulnerabilidad en MySQL de Oracle: CVE-2018-3282 (oracle-mysql-cve-2018-3282)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3283 (oracle-mysql-cve-2018-3283)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2018-3284 (oracle-mysql-cve-2018-3284)	Media
Vulnerabilidad en MySQL de Oracle: CVE-2019-2420 (oracle-mysql-cve-2019-2420)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2019-2434 (oracle-mysql-cve-2019-2434)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2019-2455 (oracle-mysql-cve-2019-2455)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2019-2481 (oracle-mysql-cve-2019-2481)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2019-2482 (oracle-mysql-cve-2019-2482)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2019-2486 (oracle-mysql-cve-2019-2486)	Media
Vulnerabilidad en Oracle MySQL: CVE-2019-2503 (oracle-mysql-cve-2019-2503)	Media
Vulnerabilidad en MySQL de Oracle: CVE-2019-2507 (oracle-mysql-cve-2019-2507)	Media
Vulnerabilidad de MySQL en Oracle: CVE-2019-2510 (oracle-mysql-cve-2019-2510)	Media
Vulnerabilidad en Oracle MySQL: CVE-2019-2528 (oracle-mysql-cve-2019-2528)	Media
Vulnerabilidad en MySQL de Oracle: CVE-2019-2529 (oracle-mysql-cve-2019-2529)	Media
Vulnerabilidad en MySQL de Oracle: CVE-2019-2531 (oracle-mysql-cve-2019-2531)	Media
Vulnerabilidad en MySQL de Oracle: CVE-2019-2532 (oracle-mysql-cve-2019-2532)	Media
Vulnerabilidad en MySQL de Oracle: CVE-2019-2537 (oracle-mysql-cve-2019-2537)	Media
Vulnerabilidad de PHP: CVE-2018-17082 (php-cve-2018-17082)	Media
Método HTTP OPTIONS habilitado (http-options-method-enabled)	Bajo
Vulnerabilidad de Oracle MySQL: CVE-2018-3174 (oracle-mysql-cve-2018-3174)	Bajo

Fuente: Nexpose.

Así mismo se realizó en SQL Server el escaneo de vulnerabilidades con Nexpose, obteniendo 5 vulnerabilidades; 4 de nivel medio y una de nivel bajo, como se evidencia a continuación en la tabla 17

Tabla 17: Vulnerabilidades obtenidas con Nexpose (SQL Server)

VULNERABILIDAD	NIVEL
Firma de SMB deshabilitada (cifs-smb-signature-disabled)	Medio
Windows Autologin habilitado (Windows-Autologin-habilitado)	Medio

Firma de SMB no requerida (cifs-smb-firmando-no-requerida)	Medio
No se requiere la firma SMBv2 (cifs-smb2-signature-no-required)	Medio
Amplificación del tráfico NetBIOS NBSTAT (amplificación netbios-nbstat)	Bajo

Fuente: Nexpose.

Comparado los resultados obtenidos una vez realizado el escaneo tanto con Nessus como con Nexpose, en MySQL tabla 18

Tabla 18: Resultado de escaneo MySQL.

MYSQL		
NIVEL	**NESSUS**	**NEXPOSE**
Critica o Alta.	0	3
Media.	1	68
Baja / Información/moderado	30	2
Total.	31	73

Fuente: Las Autoras.

Expresión gráfica del escaneo realizado con Nessus y Nexpose Gráfico 4.

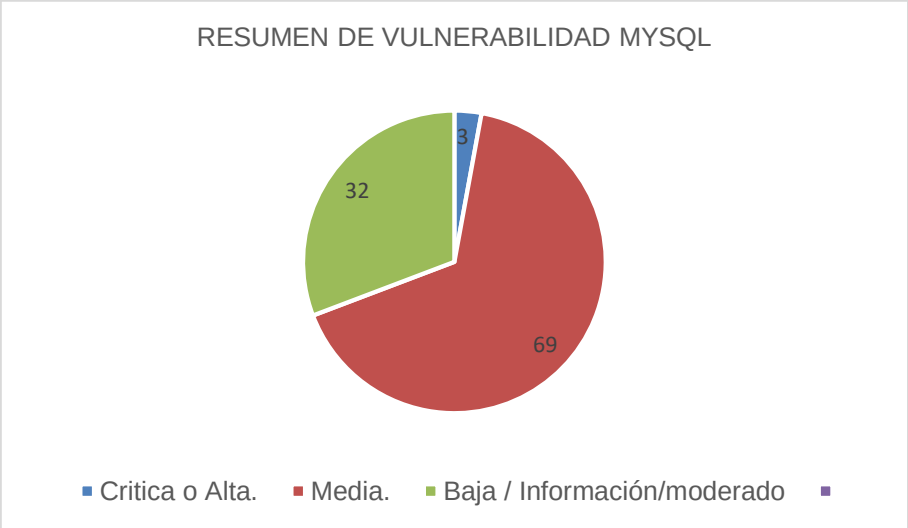


Gráfico 4: Resultado de escaneo MySQL.

Fuente: Las Autoras.

Comparación de los resultados obtenidos una vez realizado el escaneo tanto con Nessus como con Nexpose, en SQL Server tabla 19.

Tabla 19: Resultado de escaneo SQL Server.

SQLSERVER		
NIVEL	**NESSUS**	**NEXPOSE**
Critica o Alta.	0	0
Media.	2	4
Baja / Información/moderado	0	1
Total.	2	5

Fuente: Las Autoras.

Expresando gráficamente el resultado obtenido luego del escaneo realizado con Nessus y Nexpose Gráfico 5.

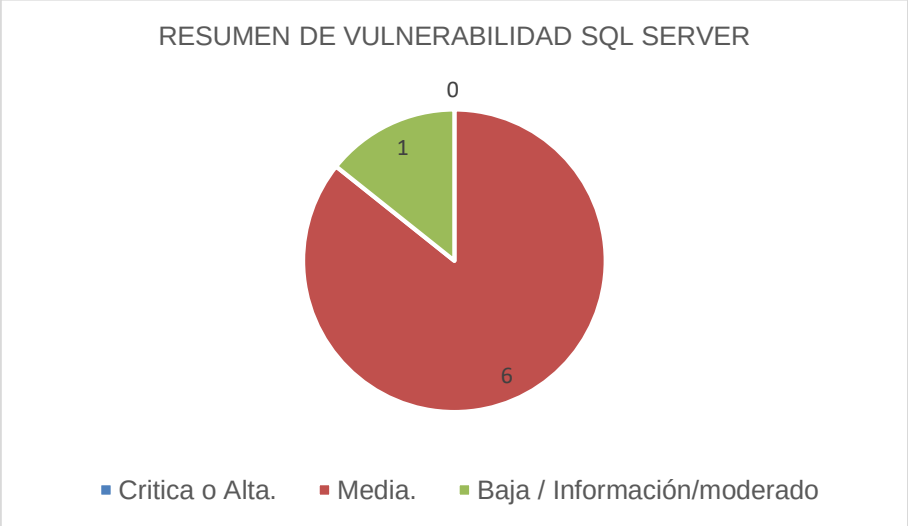


Gráfico 5: Resultado de escaneo SQL Server.

Fuente: Las Autoras.

Como se puede evidenciar en las tablas 18 y 19, los resultados obtenidos entre los escáneres de vulnerabilidades varían dependiendo la herramienta que se utilice, la herramienta Nessus detecta únicamente las vulnerabilidades que afectan directamente al sistema gestor de bases de datos, razón por la cual evidencia menor cantidad de vulnerabilidades, en el caso de Nexpose se registran una cantidad mayor de vulnerabilidades, ya que este no solo detecta las vulnerabilidades que afectan al gestor, sino una serie de amenazas que

influyen a que el gestor sea vulnerable, es decir amenazas están ligadas al gestor y que permiten que las amenazas directas se vuelvan potenciales.

Una vez detectadas las amenazas que comprometen el buen funcionamiento de los sistemas gestores de bases de datos, se procedió a la selección de mejoras que permitan mitigar los fallos que puedan presentarse como se detalla en la tabla 20.

Tabla 20: Determinación de plan de mejora

CÓDIGO	AMENAZA	MEJORAS
I. 5	Avería de origen físico o lógico	Disponer de sensores de monitoreo del estado del hardware, esto permitirá verificar el tiempo de vida útil para así elaborar un plan de renovación para el mismo y para el estado del software con escaneo permitirá verificar su vulnerabilidad
I.8	Fallo de servicio de comunicaciones	Realizar una evaluación de los sistemas, con el fin de elaborar un plan de gestión para mitigar los riesgos
		Disponer de sistemas de comunicación redundantes con el fin de dar continuidad a los procesos en caso de fallos. (RAID, Tarjetas de red, fuentes de alimentación)
		Elaborar documentos de respaldo de la configuración de los dispositivos y del acceso al sistema
I.10	Degradación de los soportes de almacenamiento de la información	Elaborar inventarios actualizados cada 3 meses de los recursos con los que se cuenta
		Llevar un control del tiempo de vida de cada recurso para evitar su desgaste.
		Disponer de elementos redundantes que permitan la continuidad de las operaciones sin pérdidas de tiempo en caso de fallos.
E. 1	Errores de los usuarios	Capacitar al personal sobre la importancia de cuidar sus claves de acceso y demás datos que puedan comprometer el buen desempeño de las actividades de las instituciones.
E.2	Errores del Administrador	Presentar al personal un manual de políticas de responsabilidades y procedimientos de operación en caso de errores
		Asignar a cada usuario un orden especifico de tareas claras y directas para evitar errores de omisión o que las tareas se realicen de forma redundante.
		Documentar los permisos de accesos y privilegios por roles de cada usuario de la información.
E.3	Errores de monitorización (Log)	Capacitar al personal sobre la importancia de cuidar sus claves de acceso y demás datos que puedan comprometer el buen desempeño de las actividades de las instituciones. Concienciación, educación y capacitación en seguimiento de la información

E. 4	Errores de configuración	Realizar pruebas de actualizaciones previo a la instalación.
		Realizar pruebas mensuales del cortafuegos.
		Definir procesos de configuración de los equipos según el rol que desempeñe el usuario dentro de la institución.
		Uso de principios de ingeniería en protección de sistemas: Rigor y formalidad, separación de intereses, modularidad, abstracción, anticipación al cambio, generalidad, incrementalidad)
		Disponer de equipos alternos para realizar pruebas de concepto, con el fin adaptar y mejorar las ideas y lograr una mejor aceptación.
E.8	Difusión de Software dañino	Realizar semanal o mensualmente controles contra códigos maliciosos.
E.9	Errores de (re)encaminamiento	Realizar una adecuada configuración de los switches.
		Disponer de personal capacitado para la administración de los equipos.
E. 10	Errores de secuencia	Disponer de plan de recuperación de la información integra para evitar su alteración.
E.15	Alteración accidental de la información	Crear perfiles de usuario con los permisos correspondientes para cada empleado. Realizar diariamente copias de seguridad de la información, para su verificación en caso de cambios inesperados.
E. 20	Vulnerabilidades de los programas (software)	Evitar el uso de cualquier dispositivo de almacenamiento en los equipos de la institución. Evitar la instalación o uso de aplicaciones no autorizadas en los equipos de la institución. Utilizar protocolos de seguridad para proteger las comunicaciones.
E.21	Errores de Mantenimiento / Actualización de Equipos	Creación de perfiles de seguridad.
		Creación de puntos de recuperación de la información para evitar cambios no deseados en los equipos.
E.24	Caída del sistema por agotamiento de recursos	Disponer de elementos redundantes, para suplir en caso de agotamiento de los recursos disponibles en la institución.
		Realizar periódicamente mantenimiento preventivo de los equipos, para evitar la pérdida del recurso.
		Mantenimiento correctivo de los equipos, en caso de fallos en el mismo.
A. 3	Manipulación de registro de actividades (log)	Contar con políticas de control de acceso. Realizar copias de seguridad de la información para el análisis, gestión de logs y control de acceso lógico.
A. 4	Manipulación de los ficheros de configuración	Asignación de privilegios de acceso de los usuarios.
A.5	Suplantación de identidad del usuario	Cifrado de información sensible.
		Solicitar el uso de información confidencial para la autenticación.
A.6	Abuso de privilegios de acceso	Aplicar perfiles de seguridad de usuarios.
		Revisión de los derechos de acceso de los usuarios.
A.7	Uso no previsto	Formación y concientización del personal en cuanto a seguridad
		Uso aceptable de los activos, según la normativa institucional.
A. 8	Difusión de Software dañino	Implementar procesos de hardering de servidores con el fin de reducir las vulnerabilidades a las que se expone el sistema. Revisar y actualizar periódicamente los incidentes que se presenten y la solución aplicada.
A. 9	(re) encaminamiento de mensajes	Crear políticas y procedimientos de intercambio de información. Capacitar al personal sobre el adecuado uso y envío de la información
A. 10	Alteración de secuencia	Realizar controles de acceso a la información de acuerdo al orden establecido.

A. 11	Acceso no autorizado	Establecer y aplicar políticas de acceso a la información.
		Cambiar siempre las configuraciones por defecto de los equipos.
		Implementación de sistema de detección de intrusos
		Asignar cuentas para la administración de sistemas
A. 14	Interceptación de información (escucha)	Establecer políticas para el control de la seguridad de la información y capacitar al personal para su correcta aplicación.
		Aplicar políticas de seguridad a la red.
		Utilizar cifrado de datos para evitar que sean leídos por todos.
A. 22	Manipulación de programas	Uso de herramientas de administración de sistemas, para hacer un seguimiento de las actividades que realiza cada empleado.
A.24	Denegación de Servicio	Configurar correctamente el firewall para que analice de forma exhaustiva el tráfico tanto de entrada como de salida.

Fuente: Las Autoras.

Luego de establecer la propuesta de mejoras detectadas para cada una de las amenazas detectadas, se procedió a la estimación de los costos que implica la aplicación de las mismas como se evidencia en la tabla 21.

Tabla 21: Valoración económica de las mejoras

CÓDIGO	AMENAZA	COSTO	DETALLE
I. 5	Avería de origen físico o lógico	**$2345,00**	La revisión física de los equipos se aplicará 3 veces al año, con un costo de $750,00 la lógica mediante Nessus con un costo anual es de $2495,00
I.8	Fallo de servicio de comunicaciones	**$3,000**	El plan de gestión se realiza una vez y tiene un costo estimado de $3000,00
		$3,500	Adquirir sistemas de comunicación redundantes significa un costo de $3500,00
		$520,00	La elaboración de respaldos de configuración se realiza diariamente con un costo estimado de $2,00 diarios lo que da un total de
I.10	Degradación de los soportes de almacenamiento de la información	**$100,00**	La elaboración de inventarios y control de vida útil se hará cada 3 meses con un costo estimado de $25,00
		$2000,00	Contar con elementos redundantes de comunicación estima un costo de $2000,00
E. 1	Errores de los usuarios	**$1500,00**	Por capacitación permanente en seguridad y sentido de pertenencia a una institución, se considera un costo de $1500,00
E.2	Errores del Administrador	**$100,00**	En la elaboración de manuales de políticas de responsabilidades se estima un costo de $100,00
		$150,00	Capacitar al personal en su rol a cumplir dentro de la institución $150,00

		$20,00	La documentación de los permisos de usuario se realizará en cada contratación o ascenso del empleado $20,00
E.3	Errores de monitorización (Log)	**$1200,00**	Las capacitaciones se realizarán de forma bimensual con un costo de $200,00 cada una además de campañas digitales.
E. 4	Errores de configuración	**$240,00**	Las pruebas de actualización se realizan mensualmente con un costo de $20,00
		$540,00	Las pruebas a cortafuegos suponen un costo de $45,00 mensuales
		$400,00	La definición de procesos de roles de usuario se lo hará 2 veces al año con un costo de $200,00
		$8000,00	En adquisición de equipos alternos se estima un costo de $8000,00
E.8	Difusión de Software dañino	**$3000,00**	En la adquisición de antivirus se estima un costo de $3000,00
E.9	Errores de (re)encaminamiento	**$1700,00**	Adquirir switches origina un costo de $1700,00 con instalación y mantenimiento por 1 año
E. 10	Errores de secuencia		Disponer de un plan de recuperación de la información tiene un costo de $300,00
E.15	Alteración accidental de la información	**$360,00**	Las copias de seguridad se realizarán diariamente con un costo de $1,00 diario
E. 20	Vulnerabilidades de los programas (software)	**$800,00**	Se capacita al personal en temas de seguridad del uso de programas cada 3 meses con un costo de $200,00 por capacitación
E.21	Errores de Mantenimiento / Actualización de Equipos	**$500,00**	Crear perfiles y puntos de recuperación de información se realizará 2 veces al año con un costo de $250,00
E.24	Caída del sistema por agotamiento de recursos	**$1000,00**	El mantenimiento de los equipos se lo hará 2 veces al año con un costo de $500,00 cada uno
A. 3	Manipulación de registro de actividades (log)	**$500,00**	Las políticas de control de acceso y sus copias de seguridad se harán una vez al año con un costo de $500,00
A. 4	Manipulación de los ficheros de configuración	**$160,00**	La capacitación para el asignar acceso al sistema se revisará 2 veces al año con un costo de $80,00
A.5	Suplantación de identidad del usuario	**$720,00**	Cifrado de información sensible se lo hará diariamente con un costo de $2,0
		$500,00	La capacitación en seguridad se hará dos veces al año con un costo de $500,00
A.6	Abuso de privilegios de acceso	**$500,00**	Contratar a un experto en seguridad que verifique los procesos llevados a cabo supone un costo de $400,00 al año
A.7	Uso no previsto	**$600,00**	Capacitar al personal en una vez cada 3 meses supone un costo de $600,00
A. 8	Difusión de Software dañino	**$850,00**	La actualización de protocolos de seguridad estima un costo de $850,00 al año
A. 9	(re) encaminamiento de mensajes	**$650,00**	Crear políticas de seguridad y capacitar al personal supone un costo anual de $650,00
A. 10	Alteración de secuencia	**$360,00**	Revisión mensual del plan de controles de acción establecido supone un costo de $30,00 mensuales
A. 11	Acceso no autorizado	**$100,00**	Elaborar el plan de políticas de acceso supone un costo anual de $100,00

		$80,00	La configuración de los equipos supone un costo de $80,00 se lo hace al momento de la compra.
		$600,00	La implementación de sistema de detección de intrusos representa un costo de $600,00
			La capacitación en seguridad se hará una vez al año con un costo de $500,00
A. 14	Interceptación de información (escucha)	**$650,00**	Crear políticas de seguridad y capacitar al personal supone un costo anual de $650,00
		$750,00	La instalación de sensores el tráfico de información representa un costo de $750,00
		$1500,00	Capacitación en seguridad de información se hará 3 veces al año con un costo de $500,00 cada una
A. 22	Manipulación de programas	**$600,00**	La aplicación genera un costo de $600,00
A.24	Denegación de Servicio	**$450,00**	La actualización del firewall genera un costo de $450,00 al año

Fuente: Las Autoras.

En el anexo 6, ver las soluciones establecidas tanto por Nessus y en el Anexo 6 las establecidas por Nexpose para las vulnerabilidades encontradas luego del escaneo de los sistemas gestores de bases de datos.

4.1. DISCUSIÓN

En el trabajo titulado “Estudio de seguridad informática para las bases de datos del campus virtual de la UNAD”, se realizó un estudio de seguridad informática para sus bases de datos virtual, para evaluar las vulnerabilidades que existen en el acceso directo a su sistema gestor de bases de datos y a medios usados para acceder a él, buscando formular estrategias y políticas que ayuden a reducir las amenazas, esta se realizó usando la metodología de análisis de vulnerabilidad, y herramientas de ataques programas de software libre.

Referente al trabajo mencionado con anterioridad, la elaboración del trabajo plan de mejoras ante vulnerabilidades encontradas en implementaciones de sistemas gestores de bases de datos, contrasta con ella, ya que se pudo evidenciar las amenazas a las que se encuentran expuestos los sistemas gestores de bases de datos más utilizados en el medio como son MySQL y Microsoft SQL Server, el nivel de exposición al riesgo, el impacto que puede tener en caso de su materialización, facilitando un plan de mejoras a seguir para mitigar los riesgos

con su respectiva valoración económica para prevenir daños y costos económicos altos para su recuperación; al ser un procedimiento que no se realiza con frecuencia en el medio, resulta importante realizarlo no solo para evidenciar las fallas que se pueden presentar, sino también para tener una guía específica a seguir para evitar daños mayores.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Después de culminar el presente trabajo se puede concluir que:

- Es esencial definir de forma clara los elementos que van a ser objeto de estudio considerando factores como usabilidad, acceso y demás factores necesarios para la elección adecuada de los sistemas gestores de bases de datos que se van a evaluar. (Pág. 38 Gráfico 1 y gráfico 2)

- Se debe contar con políticas de control interno probadas y actualizadas, que permitan identificar a tiempo de amenazas que afectan a los sistemas gestores de bases de datos, el nivel de riesgo al que se expone en caso de su materialización. (Pág. 40 Tabla 11)

- Es necesario realizar una constante actualización y búsqueda de las mejores herramientas disponibles para la detección de amenazas a las que se exponen los sistemas gestores de bases de datos. (Pág. 47, Gráfico 4 y 5)

- Contar con un plan de mejoras permite tener una mejor visión de los problemas que pueden presentarse al momento de la materialización de una amenaza, ya que a través de su uso se mitigan los riesgos, además que aportan a la toma decisiones para el pronto restablecimiento de los servicios. (Pág. 49, Tabla 20)

5.2. RECOMENDACIONES

Una vez culminado el trabajo realizado, se pueden describir las siguientes recomendaciones:

- Es primordial establecer los criterios de evaluación identificando los gestores de base de datos tomando en cuenta factores imprescindibles como seguridad, demanda, disponibilidad de información, actualizaciones y facilidad de uso, que contribuyan a su adecuado desempeño.

- En las instituciones se deben realizar y actualizar periódicamente un análisis de los riesgos a los que se exponen y aplicar medidas que le permitan la mitigación de los mismos.

- Hacer monitoreos constantes del nivel de exposición al riesgo, para corregirlos a tiempo y evitar los daños que ocasionaría la materialización de las amenazas.

- Se debe contar con políticas de control interno probadas y actualizadas, que permitan identificar a tiempo de amenazas que afectan a los sistemas gestores de bases de datos, el nivel de riesgo al que se expone y el impacto que causaría de su materialización.

- Una vez identificadas las amenazas a las que se exponen los sistemas gestores de bases de datos, es imprescindible ajustar el plan de mejoras establecidos de acuerdo a sus necesidades, aplicarlo y documentar en caso de aplicar mejoras diferentes, con el fin de mantenerlo actualizado y difundirlo con el fin que sirva de referente para otros.

BIBLIOGRAFÍA

Administración electrónica-PA, P. (2012). MAGERIT v. 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Alaro, V. (2017). Desarrollo e implementación de técnicas de recuperación y respaldos de base de datos. (Tesis Pregrado). Universidad Mayor de San Andrés facultad de Ciencias Puras y Naturales carrera de Informática. Recuperado de https://repositorio.umsa.bo/bitstream/handle/123456789/12547/T.3281.pdf

Albarracín, C. (2011). Estudio de la Seguridad Informática y sus aplicaciones para prevenir la infiltración de los Hackers en las empresas. (Tesis Pregrado). Instituto Tecnológica Israel facultad de Sistemas Informáticos. Recuperado de http://157.100.241.244/bitstream/47000/167/1/UISRAEL-EC-SIS-378.242-403.pdf

Alonso, D. (2015). Evaluación de seguridad a sistemas de información en cuanto a ataques maliciosos con base en normatividad, tendencias, impacto y técnicas vigentes para ambientes empresariales a nivel nacional. (Tesis Pregrado). Universidad de La Sabana. Recuperado de https://intellectum.unisabana.edu.co/bitstream/handle/10818/15761/David%20Hernando%20Alonso%20Torres%20%20%28tesis%29.pdf

Arias, C. (2015). Diseño e implementación de un sistema prototipo de gestión de acceso a las aulas de la facultad de ingeniería mediante llaves electrónicas (Bachelor's thesis). (Tesis Pregrado). Universidad de Cuenca facultad de Ingeniería escuela de Electrónica y Telecomunicaciones. Recuperado de http://dspace.ucuenca.edu.ec/jspui/bitstream/123456789/21663/1/tesis.pdf

Ayenson, M. (2012). Seguridad en aplicaciones Web.Recuperado de https://pdfs.semanticscholar.org/ecab/7008dc58345d0e1f4a14e26bb1218aad776c.pdf

Azán, Y., Bravo, L., Rosales, W., Trujillo, D., García, E., Pimentel, A. (2014). Solución basada en el Razonamiento Basado en Casos para el apoyo a las auditorías informáticas a bases de datos. Revista. Cubana de Ciencias Informáticas, 8(2). Recuperado de: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992014000200004

Badillo, D. (2015). Estudio Comparativo de las Distribuciones Linux Orientado a la Seguridad de Redes de Comunicación. (Tesis Pregrado). Instituto Tecnológica Israel facultad de Sistemas Informáticos. Recuperado de http://157.100.241.244/bitstream/47000/167/1/UISRAEL-EC-SIS-378.242-403.pdf

Badillo, D. (2015). Estudio Comparativo de las Distribuciones Linux Orientado a la Seguridad de Redes de Comunicación. (Tesis Pregrado). Instituto Tecnológica Israel facultad de Sistemas Informáticos. Recuperado de https://www.researchgate.net/publication/268418932_Security_Testing_of_Web_Based_Applications/download

Berlanga, J. (2012). Altair-T: Sistema de detección y gestión de amenazas sobre activos. (Tesis Pregrado). Universidad Politécnica de Catalunya. Recuperado de https://upcommons.upc.edu/bitstream/handle/2099.1/14109/78036.pdf

Blancas, Y., Castillo, A., Eugenio, E., Reyes, A., Ruiz, E. (2012). Análisis de Vulnerabilidades del Sistema Web SISER de Grupo Iusacell, Basado en la Metodología de Ec-Council.. (Tesis Pregrado). Instituto Politécnico Nacional escuela Superior de Ingeniería Mecánica y Eléctrica unidad Culhuacán. Recuperado de: https://tesis.ipn.mx/jspui/bitstream/123456789/14887/1/ic%20105%2012.pdf

Briñez, M. (2018). Diseño de un sistema de gestión de seguridad informática para la alcaldía municipal de la Jagua de Ibirico–Cesar basado en la Norma ISO 27001: 2013. (Tesis Pregrado). Universidad Nacional Abierta y a Distancia UNAD. Recuperado de https://repository.unad.edu.co/handle/10596/14253

Centeno, J. (2015). Desarrollo de prácticas de laboratorio utilizando la filosofía Hacking Ético Profesional, para apoyo de la docencia de las asignaturas relacionadas con la Seguridad informática del Departamento de Computación de la UNAN-León. (Tesis Pregrado). Universidad Nacional Autónoma de NicaraguaUNAN – León. Recuperado de http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/4306/1/228560.pdf

Chen, Ch., Matthews, M. (2004). A Web Interface for Nessus Network Security Scanner. (Tesis Pregrado). University of South Carolina. Recuperado de https://www.eecis.udel.edu/~chenc/pubs/ICC2479.pdf

De León, C. (2017). Test de Penetración “Pentesting” Aplicado en Entornos Gnu/Linux En Una Empresa Guatemalteca. (Tesis Pregrado). Universidad Mariano Gálvez de Guatemala. Recuperado de https://www.academia.edu/34520501/test_de_penetraci%c3%93n_pentesting_aplicado_en_entornos_gnu_linux_en_una_empresa_guatemalteca

Díaz, R., Pérez, Y., Proenza., D. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. Revista. Ciencias Holguín, 20(2). Recuperado de: http://www.redalyc.org/pdf/1815/181531232002.pdf

Erdogan, G. (2009). Security Testing of Web BasedApplications. (Tesis Pregrado). Norwegian university of Science and Technology. Recuperado de https://core.ac.uk/download/pdf/52104649.pdf

Grajales, A. (2015). Estudio sistema de información por georreferencia para la ESE Hospital San Pedro y San Pablo. (Tesis Pregrado). Universidad Católica Popular del Risaralda programa de Ingeniería en Sistemas y

Telecomunicaciones. Recuperado de http://repositorio.ucp.edu.co/bitstream/10785/3034/1/CDPEIST39.pdf

Hare, J. (2018). A Contactless ‘Active’ Reconnaissance Known Vulnerability Assessment Tool. (Tesis Pregrado).Edinburgh Napier University. Recuperado de https://www.researchgate.net/profile/Jamie_Ohare4/publication/325857437_Honours_Project_-_Scout_A_Contactless_'Active'_Reconnaissance_Known_Vulnerability_Assessment_Tool/links/5b2949454585150c63dd1bc3/Honours-Project-Scout-A-Contactless-Active-Reconnaissance-Known-Vulnerability-Assessment-Tool.pdf

Ladines, K. (2017). Plan informático de contingencia para la seguridad de la información del departamento de tic de la PUCESE. (Tesis Pregrado). Pontificia Universidad Católica del Ecuador Sede Esmeraldas. Recuperado de https://repositorio.pucese.edu.ec/bitstream/123456789/1010/1/LADINES%20GARC%C3%89S%20KATHERINE%20STEFANIA.pdf

Llobet, C. (2017). Web Platform for Auditing as a Service. (Tesis Pregrado). Facultat D’inform`Atica de Barcelona (Fib). Recuperado de https://upcommons.upc.edu/bitstream/handle/2117/114117/121082.pdf

Llorente, T. (2016). laboratorio virtual para el estudio de vulnerabilidades en la nube. (Tesis Pregrado). Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación universidad de Cantabria. Recuperado de https://repositorio.unican.es/xmlui/bitstream/handle/10902/9329/387584.pdf

López, M. (2017). Diseño de Procedimientos de Seguridad Basados en Pruebas de Pentesting Aplicadas A La Empresa Cjt&T Ingeniería De Software. (Tesis Pregrado). Universidad Nacional Abierta y a Distancia escuela de Ciencias Básicas, Tecnología e Ingeniería especialización en Seguridad Informática. Recuperado de

https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14929/1/1085285379.pdf

López, S. (2017). Diagnóstico de la seguridad informática de la red de datos de la empresa sunshine bouquet zona norte bogotá, colombia. (Tesis Pregrado). Universidad nacional abierta y a distancia “UNAD” escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática. Recuperado de https://repository.unad.edu.co/handle/10596/21490

Malla, Q., David, H. (2016). Análisis de vulnerabilidades en la red LAN jerárquica de la Universidad Nacional de Loja, en el Área de la Energía, las Industrias y los Recursos Naturales no Renovables (Bachelor's thesis). (Tesis Pregrado). Recuperado de http://dspace.unl.edu.ec/jspui/bitstream/123456789/16039/1/Quishpe%20Malla%2c%20Henry%20David.pdf

Martí, R. (2016). Desarrollo e Implementación Práctica de un Pentest. (Tesis Pregrado). Universidad Politécnica De Valencia Recuperado de https://riunet.upv.es/bitstream/handle/10251/70164/MART%c3%8d%20-%20Desarrollo%20e%20implementaci%c3%b3n%20pr%c3%a1ctica%20de%20un%20PENTEST.pdf

Méndez, C. (2015). Monitoreo de Vulnerabilidades en Servicios de Red para empresas con Nagios Implementado. (Tesis Pregrado). Universidad Piloto de Colombia dirección de Postgrados especialización en Seguridad Informática. Recuperado de http://polux.unipiloto.edu.co:8080/00002826.pdf

Meneses, M., Llanos, A. (2016). Diseño de un protocolo para la detección de vulnerabilidades en los principales servidores de la superintendencia de puertos y transportes. (Tesis Pregrado). Universidad Católica de Colombia. Recuperado de https://repository.ucatolica.edu.co/bitstream/10983/14013/4/Proyecto%20de%20Grado.pdf

Millán, E. (2017). Fundamentos de bases de datos notas de referencia. Recuperado de: http://bibliotecadigital.univalle.edu.co/bitstream/10893/10313/3/Fundamentos%20de%20Bases%20de%20Datos.pdf

Monteiro, P. (2016). Sistema de detecção de vulnerabilidade em aplicacõesinstaladas em sistemas Windows. (Tesis Pregrado). Escola Superior de Tecnologia e GestaoMestrado em Engenhariade Segurança Informática. Recuperado de https://repositorio.ipbeja.pt/bitstream/20.500.12207/4718/1/Pedro%20Godinho.pdf

Montesino, R., Baluja, W., Porvén, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. Revista. Ingeniería Electrónica, Automática y Comunicaciones, 34(1), 40-58. Recuperado de http://scielo.sld.cu/scielo.php?pid=S1815-59282013000100004&script=sci_arttext&tlng=pt

Navas, P., Mendoza, R., Alajo, A. (2018). La administración de los sistemas de gestor de base de datos (SGBD'S) de los sistemas de información y su incidencia en el control de las seguridades de las bases de datos. Revista Electrónica Formación y Calidad Educativa. ISSN 1390-9010, 6(1), 57-70. Recuperado de: http://www.refcale.uleam.edu.ec/index.php/refcale/article/view/2110/1445

Ortiz, D. (2015). Desarrollo de metodología para hallazgos de vulnerabilidades en redes corporativas e intrusiones controladas. (Tesis Pregrado). Fundación Universitaria los Libertadores facultad de Ingenierías Programa de Ingeniería Electrónica. Recuperado de https://repository.libertadores.edu.co/bitstream/handle/11371/342/DiegoFernandoOrtizAristizabal.pdf

Paucar, M. (2017). Diseño de un Sistema de Gestión de Seguridad de la Información Basado en el Estándar ISO/IEC 27005 para la Infraestructura tecnológica de Mediasist SA. (Tesis Pregrado). Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en

Sistemas Computacionales. Recuperado de http://repositorio.ug.edu.ec/bitstream/redug/24104/1/B-CISC-PTG.1363.Paucar%20Castillo%20Mariana%20Alexandra.pdf

Peñuela, Y. (2018). Análisis e identificación del estado actual de la seguridad informática, dirigido a las organizaciones en Colombia, que brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información. (Tesis Pregrado). Universidad Nacional Abierta y a Distancia UNAD. Recuperado de https://repository.unad.edu.co/handle/10596/17260

Pérez, A. (2016). Análisis de los principales sistemas de gestión de bases de datos ante ataques básicos. (Tesis Posgrado). Universidad Internacional de La Rioja Máster universitario en Seguridad Informática. Recuperado de https://reunir.unir.net/bitstream/handle/123456789/3619/ARMENDARIZ%20PEREZ%2C%20I%C3%91IGO.pdf?sequence=1&isAllowed=y .pdf

Ramírez, J., Ávila, W. (2018). Escaneo de Vulnerabilidades al Servidor Principal de la Empresa Caso de Estudio. (Tesis Pregrado). Universidad Nacional Abierta y a Distancia –UNAD escuela de Ciencias Básicas Tecnología e Ingeniería especialización en Seguridad Informática. Recuperado de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18321/1/1121877957.pdf

Rodríguez, A., Rozo, R. (2015). Diseño de un plan estratégico para la seguridad de la información tributaria en una entidad pública. (Tesis Pregrado). Universidad nacional abierta y a distancia “UNAD” escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática. Recuperado de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3613/3/52761210_60334684.pdf

Rodríguez, I. (2014). Seguridad en aplicaciones Web. (Tesis Posgrado). Universidad Autónoma de Barcelona. Recuperado de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/33721/6/isidoro_ciervaTFM0614memoria.pdf

Rojas, A. (2018). Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa plasticaucho industrial S.A. (Tesis Pregrado). Universidad técnica de Ambato. Recuperado de http://repo.uta.edu.ec/bitstream/123456789/28102/1/Tesis_%20t1417si.pdf

Solarte, F., Rosero, E., Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista. Tecnológica-ESPOL, 28(5). Recuperado de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321.

Terán, R., Fonseca, G. (2013). Vulnerabilidades de los relojes biométricos en los registros del personal para proteger la información en determinadas empresas de Ambato. (Tesis Pregrado). Universidad Técnica de Ambato. Recuperado de http://repo.uta.edu.ec/handle/123456789/5851

Uribe, C. (2018). Estudio de seguridad informática para las bases de datos del Campus virtual de la UNAD. (Tesis Pregrado). Universidad Nacional Abierta y a Distancia “UNAD” Escuela De Ciencias Básicas tecnología e Ingeniería especialización en Seguridad Informática. Recuperado de https://repository.unad.edu.co/handle/10596/8893

Urrutia, A., Galindo, J., Sepúlveda, A. (2010). Implementación de una base de datos difusa con First-2 y PostgreSQL. Recuperado de https://www.researchgate.net/profile/Jose_Lugo_Garcia/post/Is_there_any_methodology_for_creating_a_fuzzy_relational_database/attachment/59d61ddc79197b807797b281/AS:273745191604248@1442277347892/download/Implementacion+de+una+base+de+datos+difusa+con+FIRST-2+y+PosgreSQL.pdf

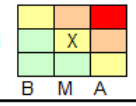
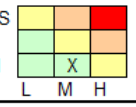
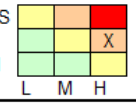
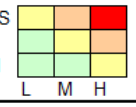
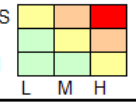
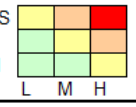
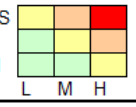
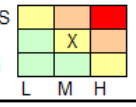
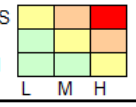
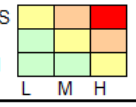
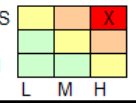
Vera, R. (2012). Chequeo de Vulnerabilidades de Seguridad en Entidades de una Red, (Tesis Pregrado). Universidad Central “Marta Abreu” de Las Villas Facultad de Ingeniería Eléctrica Departamento de Telecomunicaciones y Electrónica. Recuperado de

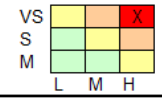
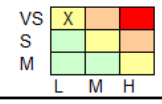
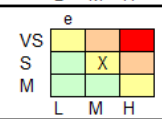
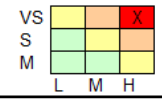
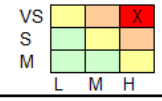
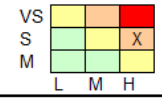
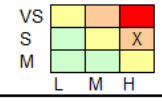
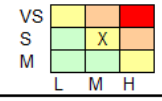
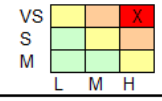
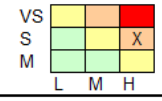
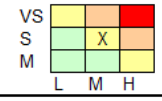
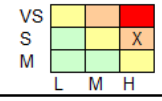
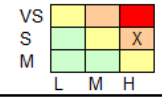
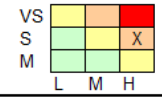
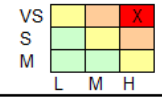
http://dspace.uclv.edu.cu/bitstream/handle/123456789/1571/Redner%20Licea%20Vera.pdf?sequence=1&isAllowed=y

ANEXOS

ANEXO 1

TABLAS DE IMPACTO SEGÚN METODOLOGIA MAGERIT

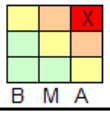
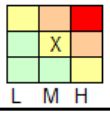
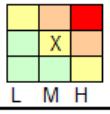
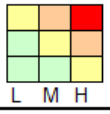
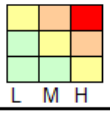
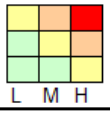
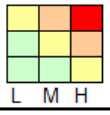
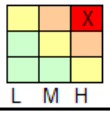
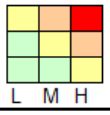
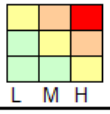
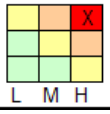
CÓDIGO	Description	PROBABILIDAD	IMPACTO	NIVEL	Matriz de riesgo
I.5	Avería de origen físico o lógico	Medio	Alto	Medio	
		2	2		
I.8	Fallo de servicio de comunicaciones	Alto	Medio	Bajo	
		2	1		
I.10	Degradación de los soportes de almacenamiento de la información	Alto	Medio	Alto	
		3	2		
E.1	Errores de los usuarios	Bajo	Bajo	Bajo	
		1	0		
E.2	Errores del Administrador	Bajo	Bajo	Bajo	
		1	0		
E,3	Errores de monitorización (Log)	Bajo	Bajo	Bajo	
		1	0		
E,4	Errores de configuración	Bajo	Bajo	Bajo	
		1	0		
E,8	Difusión de Software dañino	Medio	Alto	Medio	
		2	2		
E.9	Errores de (re)encaminamiento	Medio	Bajo	Bajo	
		2	0		
E.10	Errores de secuencia	Medio	Bajo	Bajo	
		2	0		
E.15	Alteración accidental de la información	Alto	Alto	Critico	
		3	3		

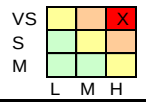
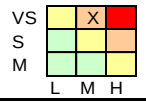
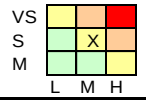
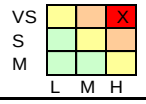
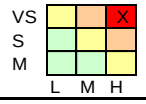
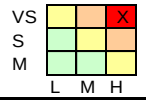
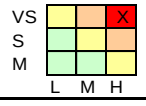
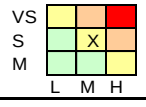
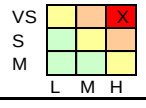
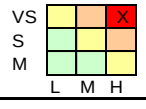
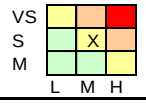
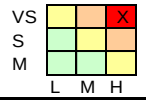
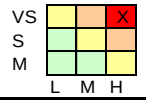
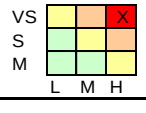
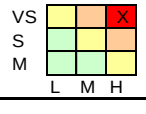
E.20	Vulnerabilidades de los programas (software)	Alto	Alto	Critico	
		3	3		
E.21	Errores de Mantenimiento / Actualización de Equipos	Bajo	Alto	Medio	
		1	3		
E.24	Caída del sistema por agotamiento de recursos	Medio	Minor	Medio	
		2	2		
A,3	Manipulación de registro de actividades (log)	Alto	Alto	Critico	
		3	3		
A,4	Manipulación de los ficheros de configuración	Alto	Alto	Critico	
		3	3		
A.5	Suplantación de identidad del usuario	Alto	Medio	Alto	
		3	2		
A.6	Abuso de privilegios de acceso	Alto	Medio	Alto	
		3	2		
A.7	Uso no previsto	Medio	Medio	Medio	
		2	2		
A.8	Difusión de Software dañino	Alto	Alto	Critico	
		3	3		
A.9	(re) encaminamiento de mensajes	Alto	Medio	Alto	
		3	2		
A.10	Alteración de secuencia	Medio	Medio	Medio	
		2	2		
A.11	Acceso no autorizado	Alto	Medio	Alto	
		3	2		
A.14	interceptación de información (escucha)	Alto	Medio	Alto	
		3	2		
A.22	Manipulación de programas	Alto	Medio	Alto	
		3	2		
A.24	Denegación de Servicio	Alto	Alto	Critico	
		3	3		

Anexo 1: Tablas de impacto según metodología Magerit

ANEXO 2

TABLAS DE RIESGO SEGÚN METODOLOGIA MAGERIT

CÓDIGO	Description	PROBABILIDAD	IMPACTO	NIVEL	Matriz de riesgo
I.5	Avería de origen físico o lógico	Frecuencia Normal	Alto	Alto	
		2	4		
I.8	Fallo de servicio de comunicaciones	Frecuencia Normal	Medio	Medio	
		2	2		
I.10	Degradación de los soportes de almacenamiento de la información	Poco Frecuente	Alto	Medio	
		1	6		
E.1	Errores de los usuarios	Frecuencia Normal	Despreciable	Medio	
		2	0		
E.2	Errores del Administrador	Frecuencia Normal	Despreciable	Medio	
		2	0		
E,3	Errores de monitorización (Log)	Frecuencia Normal	Despreciable	Medio	
		2	0		
E,4	Errores de configuración	Frecuencia Normal	Despreciable	Medio	
		2	0		
E,8	Difusión de Software dañino	Frecuencia Normal	Alto	Alto	
		2	4		
E.9	Errores de (re)encaminamiento	Poco Frecuente	Despreciable	Bajo	
		1	0		
E.10	Errores de secuencia	Poco Frecuente	Despreciable	bajo	
		1	0		
E.15	Alteración accidental de la información	Poco Frecuente	Muy Alto	Muy Alto	
		1	9		

E.20	Vulnerabilidades de los programas (software)	Frecuencia Normal 2	Muy Alto 9	Muy Alto	
E.21	Errores de Mantenimiento / Actualización de Equipos	Frecuencia Normal 2	Medio 3	Muy Alto	
E.24	Caída del sistema por agotamiento de recursos	Poco Frecuente 1	Medio 4	Medio	
A,3	Manipulación de registro de actividades (log)	Frecuencia Normal 2	Muy Alto 9	Alto	
A,4	Manipulación de los ficheros de configuración	Poco Frecuente 1	Muy Alto 9	Muy Alto	
A.5	Suplantación de identidad del usuario	Frecuencia Normal 2	Alto 6	Alto	
A.6	Abuso de privilegios de acceso	Frecuencia Normal 2	Alto 6	Alto	
A.7	Uso no previsto	Frecuencia Normal 2	Medio 4	Medio	
A.8	Difusión de Software dañino	Frecuencia Normal 2	Muy Alto 9	Muy Alto	
A.9	(re) encaminamiento de mensajes	Frecuencia Normal 2	Alto 6	Alto	
A.10	Alteración de secuencia	Frecuencia Normal 2	Medio 4	Medio	
A.11	Acceso no autorizado	Frecuencia Normal 2	Alto 6	Alto	
A.14	interceptación de información (escucha)	Frecuencia Normal 2	Alto 6	Alto	
A.22	Manipulación de programas	Frecuencia Normal 2	Alto 6	Alto	
A.24	Denegación de Servicio	Frecuencia Normal 2	Muy Alto 9	Muy Alto	

Anexo 2: Tablas de riesgo según metodología Magerit

ANEXO 3

VULNERABILIDADES ENCONTRADAS EN EL ESCANEO REALIZADO CON NESSUS

VULNERABILIDAD	DESCRIPCIÓN	RIESGO
Firma de SMB deshabilitada (cifs-smb-signature-disabled)	Este sistema no permite la firma SMB. La firma de SMB permite que el destinatario de paquetes de SMB confirme su autenticidad y ayuda a prevenir ataques de hombres en el medio contra SMB. La firma de SMB se puede configurar de una de las tres formas siguientes: deshabilitado por completo (menos seguro), habilitado y requerido (más seguro).	Medio
Windows Autologin habilitado (Windows-Autologin-habilitado)	Microsoft Windows NT proporciona una función llamada "Inicio de sesión automático", que le permite a un usuario iniciar sesión automáticamente en su estación de trabajo local sin ingresar una contraseña. Esta característica, aunque es conveniente, compromete la seguridad física de la estación de trabajo. Además, almacena el nombre de usuario y la contraseña de inicio de sesión automático en texto sin formato en el registro de Windows: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon NOTA: En las versiones anteriores a SP4 de Windows NT4, las ACL del registro se configuraron incorrectamente en la clave de registro correspondiente, lo que permite a cualquier usuario leer el nombre de usuario y la contraseña.	Medio
Firma de SMB no requerida (cifs-smb-firmando-no-requerida)	Este sistema habilita, pero no requiere firma SMB. La firma de SMB permite que el destinatario de paquetes de SMB confirme su autenticidad y ayuda a prevenir ataques de hombres en el medio contra SMB. La firma de SMB se puede configurar de una de las tres formas siguientes: deshabilitado por completo (menos seguro), habilitado y requerido (más seguro).	Medio
No se requiere la firma SMBv2 (cifs-smb2-signature-no-required)	Este sistema habilita, pero no requiere firma SMB. La firma de SMB permite que el destinatario de paquetes de SMB confirme su autenticidad y ayuda a prevenir ataques de hombres en el medio contra SMB. La firma de SMB 2.x se puede configurar de una de las dos formas siguientes: no se requiere (menos seguro) y se requiere (más seguro).	Medio
Firma de SMB no requerida (cifs-smb-firmando-no-requerida)	Este sistema habilita, pero no requiere firma SMB. La firma de SMB permite que el destinatario de paquetes de SMB confirme su autenticidad y ayuda a prevenir ataques de hombres en el medio contra SMB. La firma de SMB se puede configurar de una de las tres formas siguientes: deshabilitado por completo (menos seguro), habilitado y requerido (más seguro).	Medio
MS16-047: Actualización de seguridad para los protocolos remotos SAM y LSAD (3148527) (bloqueo) (verificación sin credenciales)	El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Gestor de cuentas de seguridad (SAM) y Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación de nivel de autenticación incorrecta en los canales de llamada a procedimiento remoto (RPC). Un atacante de tipo intermediario capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM puede explotar esto para forzar la degradación del nivel de autenticación, lo que permite al atacante hacerse pasar por un usuario autenticado y acceder a la base de datos SAM.	Medio
No se requiere firma SMB	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques de intermediarios contra el servidor SMB.	Medio

Amplificación del tráfico NetBIOS NBSTAT (amplificación netbios-nbstat)	Una consulta NetBIOS NBSTAT obtendrá el estado de un punto final que habla NetBIOS, que incluirá cualquier nombre al que se sepa que el punto extremo responde, así como la dirección MAC del dispositivo para ese punto final. Una respuesta NBSTAT es aproximadamente 3 veces el tamaño de la solicitud, y debido a que NetBIOS utiliza UDP, se puede usar para llevar a cabo ataques de amplificación de tráfico contra otros activos, generalmente en forma de ataques distribuidos de denegación de servicio (DRDoS).	Bajo

Anexo 3: Vulnerabilidades encontradas en el escaneo realizado con Nessus

ANEXO 4

VULNERABILIDADES ENCONTRADAS EN EL ESCANEO REALIZADO CON NEXPOSE (AFECTAN DIRECTAMENTE AL SISTEMA GESTOR DE BASE DE DATOS)

VULNERABILIDAD	DESCRIPCIÓN	RIESGO
Vulnerabilidad de Oracle MySQL: CVE-2018-3185 (oracle-mysql-cve-2018-3185)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: InnoDB). Las versiones admitidas que están afectadas son 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible (DOS completo) de MySQL Server, así como la actualización no autorizada, insertar o eliminar el acceso a algunos de los datos accesibles de MySQL Server. CVSS 3.0 Base Score 5.5 (impactos de integridad y disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: L / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2018-3187 (oracle-mysql-cve-2018-3187)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Optimizer). Las versiones admitidas que están afectadas son 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible (DOS completo) de MySQL Server, así como la actualización no autorizada, insertar o eliminar el acceso a algunos de los datos accesibles de MySQL Server. CVSS 3.0 Base Score 5.5 (impactos de integridad y disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: L / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2018-3247 (oracle-mysql-cve-2018-3247)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Merge). Las versiones compatibles que están afectadas son 5.6.41 y anteriores, 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible (DOS completo) de MySQL Server, así como la actualización no autorizada, insertar o eliminar el acceso a algunos de los datos accesibles de MySQL Server. CVSS 3.0 Base Score 5.5 (impactos de integridad y disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: L / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2019-2534 (oracle-mysql-cve-2019-2534)		
Vulnerabilidad de MySQL en Oracle: CVE-2018-3171 (oracle-mysql-cve-2018-3171)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Partition). Las versiones admitidas que están afectadas son 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad difícil de explotar permite a los atacantes con privilegios altos con acceso a la red a través de múltiples protocolos para comprometer el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible (DOS completo) de MySQL Server, así como la actualización no autorizada, insertar o eliminar el acceso a algunos de los datos accesibles de MySQL Server. CVSS 3.0 Base Score 5.0 (impactos de integridad y disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: H / PR: H / UI: N / S: U / C: N / I: L /	Medio

Vulnerabilidad de MySQL en Oracle: CVE-2018-3133 (oracle-mysql-cve-2018-3133)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Parser). Las versiones admitidas que se ven afectadas son 5.5.61 y anteriores, 5.6.41 y anteriores, 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 6.5 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2018-3143 (oracle-mysql-cve-2018-3143)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: InnoDB). Las versiones compatibles que están afectadas son 5.6.41 y anteriores, 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 6.5 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2018-3144 (oracle-mysql-cve-2018-3144)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Servidor: Seguridad: Auditoría). Las versiones admitidas que están afectadas son 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad difícil de explotar permite que un atacante no autenticado con acceso a la red a través de múltiples protocolos comprometa el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 5.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: H / PR: N / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2018-3155 (oracle-mysql-cve-2018-3155)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Parser). Las versiones admitidas que están afectadas son 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Si bien la vulnerabilidad está en el servidor MySQL, los ataques pueden tener un impacto significativo en productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 7.7 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: C / C: N / I: N / A: H).	Medio

Vulnerabilidad de MySQL en Oracle: CVE-2018-3156 (oracle-mysql-cve-2018-3156)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: InnoDB). Las versiones compatibles que están afectadas son 5.6.41 y anteriores, 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 6.5 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de Oracle MySQL: CVE-2018-3161 (oracle-mysql-cve-2018-3161)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Partition). Las versiones admitidas que están afectadas son 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de Oracle MySQL: CVE-2018-3162 (oracle-mysql-cve-2018-3162) Vulnerabilidad de Oracle MySQL: CVE-2018-3173 (oracle-mysql-cve-2018-3173) Vulnerabilidad en MySQL de Oracle: CVE-2018-3200 (oracle-mysql-cve-2018-3200) Vulnerabilidad de MySQL en Oracle: CVE-2018-3277 (oracle-mysql-cve-2018-3277)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: InnoDB). Las versiones admitidas que están afectadas son 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de Oracle MySQL: CVE-2018-3251 (oracle-mysql-cve-2018-3251)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: InnoDB). Las versiones compatibles que están afectadas son 5.6.41 y anteriores, 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 6.5 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2018-3276 (oracle-mysql-cve-2018-3276)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Memcached). Las versiones compatibles que están afectadas son 5.6.41 y anteriores, 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo	Medio

	repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	
Vulnerabilidad en MySQL de Oracle: CVE-2018-3278 (oracle-mysql-cve-2018-3278)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: RBR). Las versiones compatibles que están afectadas son 5.6.41 y anteriores, 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad en MySQL de Oracle: CVE-2018-3282 (oracle-mysql-cve-2018-3282)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Storage Engines). Las versiones admitidas que se ven afectadas son 5.5.61 y anteriores, 5.6.41 y anteriores, 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2018-3283 (oracle-mysql-cve-2018-3283)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Logging). Las versiones admitidas que están afectadas son 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad difícil de explotar permite a los atacantes con privilegios altos con acceso a la red a través de múltiples protocolos para comprometer el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.4 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: H / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2018-3284 (oracle-mysql-cve-2018-3284)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: InnoDB). Las versiones admitidas que están afectadas son 5.7.23 y anteriores y 8.0.12 y anteriores. Una vulnerabilidad difícil de explotar permite a los atacantes con privilegios altos con acceso a la red a través de múltiples protocolos para comprometer el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.4 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: H / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio

Vulnerabilidad en MySQL de Oracle: CVE-2019-2420 (oracle-mysql-cve-2019-2420)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Optimizer). Las versiones admitidas que están afectadas son 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2019-2434 (oracle-mysql-cve-2019-2434)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Parser). Las versiones admitidas que están afectadas son 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 6.5 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2019-2455 (oracle-mysql-cve-2019-2455)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Parser). Las versiones admitidas que están afectadas son 5.6.42 y anteriores, 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 6.5 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2019-2481 (oracle-mysql-cve-2019-2481)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Optimizer). Las versiones admitidas que están afectadas son 5.6.42 y anteriores, 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2019-2482 (oracle-mysql-cve-2019-2482)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: PS). Las versiones admitidas que están afectadas son 5.6.42 y anteriores, 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con	Medio

	frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 6.5 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: U / C: N / I: N / A: H).	
Vulnerabilidad de MySQL en Oracle: CVE-2019-2486 (oracle-mysql-cve-2019-2486)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Servidor: Seguridad: Privilegios). Las versiones admitidas que están afectadas son 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad en Oracle MySQL: CVE-2019-2503 (oracle-mysql-cve-2019-2503)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Connection Handling). Las versiones admitidas que están afectadas son 5.6.42 y anteriores, 5.7.24 y anteriores y 8.0.13 y anteriores. La vulnerabilidad difícil de explotar permite que un atacante con privilegios bajos tenga acceso al segmento de comunicación física conectado al hardware donde se ejecuta el servidor MySQL para comprometer el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden dar como resultado el acceso no autorizado a datos críticos o el acceso completo a todos los datos accesibles del Servidor MySQL y la capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) del Servidor MySQL. CVSS 3.0 Base Score 6.4 (Impactos de confidencialidad y disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: A / AC: H / PR: L / UI: N / S: U / C: H / I: N / A: H).	Medio
Vulnerabilidad en MySQL de Oracle: CVE-2019-2507 (oracle-mysql-cve-2019-2507)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Optimizer). Las versiones admitidas que están afectadas son 5.6.42 y anteriores, 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de MySQL en Oracle: CVE-2019-2510 (oracle-mysql-cve-2019-2510)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: InnoDB). Las versiones admitidas que están afectadas son 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS	Medio

	completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	
Vulnerabilidad en Oracle MySQL: CVE-2019-2528 (oracle-mysql-cve-2019-2528)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Partition). Las versiones admitidas que están afectadas son 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad en MySQL de Oracle: CVE-2019-2529 (oracle-mysql-cve-2019-2529)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Optimizer). Las versiones admitidas que están afectadas son 5.6.42 y anteriores, 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante con privilegios bajos con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 6.5 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: L / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad en MySQL de Oracle: CVE-2019-2531 (oracle-mysql-cve-2019-2531)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: Replication). Las versiones admitidas que están afectadas son 5.6.42 y anteriores, 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad en MySQL de Oracle: CVE-2019-2532 (oracle-mysql-cve-2019-2532)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Servidor: Seguridad: Privilegios). Las versiones admitidas que están afectadas son 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio

Vulnerabilidad en MySQL de Oracle: CVE-2019-2537 (oracle-mysql-cve-2019-2537)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: Server: DDL). Las versiones admitidas que están afectadas son 5.6.42 y anteriores, 5.7.24 y anteriores y 8.0.13 y anteriores. Una vulnerabilidad fácilmente explotable permite que un atacante de alto privilegio con acceso a la red a través de múltiples protocolos ponga en peligro el servidor MySQL. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 4.9 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: U / C: N / I: N / A: H).	Medio
Vulnerabilidad de Oracle MySQL: CVE-2018-3174 (oracle-mysql-cve-2018-3174)	El componente Apache2 en PHP antes de 5.6.38, 7.0.x antes de 7.0.32, 7.1.x antes de 7.1.22 y 7.2.x antes de 7.2.10 permite a XSS a través del cuerpo de una solicitud de "Codificación de transferencia: fragmentada", porque la brigada del grupo se maneja mal en la función php_handler en sapi / apache2handler / sapi_apache2.c.	Medio
Vulnerabilidad de Oracle MySQL: CVE-2018-3174 (oracle-mysql-cve-2018-3174)	Vulnerabilidad en el componente MySQL Server de Oracle MySQL (subcomponente: programas de cliente). Las versiones admitidas que se ven afectadas son 5.5.61 y anteriores, 5.6.41 y anteriores, 5.7.23 y anteriores y 8.0.12 y anteriores. La vulnerabilidad difícil de explotar permite que un atacante con privilegios altos inicie sesión en la infraestructura donde se ejecuta el servidor MySQL para comprometer el servidor MySQL. Si bien la vulnerabilidad está en el servidor MySQL, los ataques pueden tener un impacto significativo en productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en una capacidad no autorizada para causar un bloqueo o un bloqueo repetible con frecuencia (DOS completo) de MySQL Server. CVSS 3.0 Base Score 5.3 (Impactos en la disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: L / AC: H / PR: H / UI: N / S: C / C: N / I: N / A: H).	Bajo

Anexo 3: Vulnerabilidades encontradas con Nexpose (afectan directamente al sistema gestor de base de datos)

ANEXO 5

VULNERABILIDADES ENCONTRADAS EN EL ESCANEO REALIZADO CON NEXPOSE (ASOCIADAS AL SISTEMA GESTOR DE BASE DE DATOS)

VULNERABILIDAD	DESCRIPCIÓN	RIESGO
Apache HTTPD: Ap_get_basic_auth_pw () Omisión de autenticación (CVE-2017-3167) (apache-httpd-cve-2017-3167)	El uso de ap_get_basic_auth_pw () por parte de módulos de terceros fuera de la fase de autenticación puede hacer que se omitan los requisitos de autenticación. Los escritores de módulos de terceros DEBERÍAN utilizar ap_get_basic_auth_components (), disponibles en 2.2.34 y 2.4.26, en lugar de ap_get_basic_auth_pw (). Los módulos que llaman al legado ap_get_basic_auth_pw () durante la fase de autenticación DEBEN autenticar inmediatamente al usuario después de la llamada, o bien detener la solicitud inmediatamente con una respuesta de error, para evitar la autenticación incorrecta de la solicitud actual.	Media
Apache HTTPD: mod_ssl Dereferencia de puntero nulo (CVE-2017-3169) (apache-httpd-cve-2017-3169)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_ssl. Revise la configuración de su servidor web para su validación. mod_ssl puede anular la referencia a un puntero NULO cuando los módulos de terceros llaman a ap_hook_process_connection () durante una solicitud HTTP a un puerto HTTPS.	Media
Apache HTTPD: Mod_mime Buffer Overread (CVE-2017-7679) (apache-httpd-cve-2017-7679)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_mime. Revise la configuración de su servidor web para su validación. mod_mime puede leer un byte más allá del final de un búfer cuando se envía un encabezado de respuesta de tipo de contenido malicioso.	Media
Apache HTTPD: mod_status desbordamiento de búfer (CVE-2014-0226) (apache-httpd-cve-2014-0226)	El activo afectado es vulnerable a esta vulnerabilidad SOLAMENTE si está ejecutando uno de los siguientes módulos: mod_status. Revise la configuración de su servidor web para su validación. Se encontró una condición de carrera en mod_status. Un atacante capaz de acceder a una página de estado del servidor público en un servidor utilizando un MPM con hilos podría enviar una solicitud cuidadosamente elaborada que podría provocar un desbordamiento del búfer del montón. Tenga en cuenta que no es una configuración predeterminada o recomendada tener una página de estado de servidor accesible al público.	Media
Apache HTTPD: omitir <FilesMatch> con una nueva línea final en el nombre del archivo (CVE-2017-15715) (apache-httpd-cve-2017-15715)	La expresión especificada en <FilesMatch> podría hacer coincidir '$' con un carácter de nueva línea en un nombre de archivo malicioso, en lugar de coincidir solo con el final del nombre de archivo. Esto podría explotarse en entornos donde las cargas de algunos archivos se bloquean externamente, pero solo haciendo coincidir la parte final del nombre de archivo.	Media
Apache HTTPD: generación de autenticación de débiles compilaciones en mod_auth_digest (CVE-2018-1312) (apache-httpd-cve-2018-1312)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_auth_digest. Revise la configuración de su servidor web para su validación. Cuando se genera un desafío de autenticación HTTP Digest, el nonce enviado para evitar los ataques de respuesta no se generó correctamente utilizando una semilla pseudoaleatoria. En un grupo de servidores que utilizan una configuración de autenticación Digest común, un atacante puede reproducir las solicitudes HTTP en un servidor sin ser detectado.	Media
Vulnerabilidad de PHP: CVE-2015-9253 (php-cve-2015-9253)	Se descubrió un problema en PHP 7.3.x antes de 7.3.0alpha3, 7.2.x antes de 7.2.8 y antes de 7.1.20. El proceso maestro de php-fpm reinicia un proceso secundario en un bucle sin fin cuando se usan las funciones de ejecución del programa (por ejemplo, passthru, exec, shell_exec o sistema) con una secuencia STDIN sin bloqueo, lo que hace que este proceso maestro consuma el 100% de la CPU , y consumir espacio en disco con un gran volumen de registros de errores, como lo demuestra un ataque de un cliente a una instalación de alojamiento compartido.	Media

Apache HTTPD: Reflexión de la memoria sin inicializar en mod_auth_digest (CVE-2017-9788) (apache-httpd-cve-2017-9788)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_auth_digest. Revise la configuración de su servidor web para su validación. El marcador de posición de valor en [Proxy-] Encabezados de autorización de tipo 'Digest' no se inicializó ni se restableció antes o entre las asignaciones de valor = clave sucesivas. por mod_auth_digest. Proporcionar una clave inicial sin una asignación '=' podría reflejar el valor obsoleto de la memoria de la agrupación sin inicializar utilizada por la solicitud anterior, lo que provocaría una fuga de información potencialmente confidencial y un fallo de seguridad.	Media
Método HTTP TRACE habilitado (http-trace-method-enabled)	El método HTTP TRACE se usa normalmente para devolver la solicitud HTTP completa al cliente que lo solicita para propósitos de depuración de proxy. Un atacante puede crear una página web utilizando XMLHTTP, ActiveX o XMLDOM para hacer que un cliente emita una solicitud TRACE y capture las cookies del cliente. Esto resulta efectivamente en un ataque de secuencias de comandos entre sitios.	Media
Apache HTTPD: Derivación de procesamiento de HTTP Trailers (CVE-2013-5704) (apache-httpd-cve-2013-5704)	Los remolques HTTP podrían usarse para reemplazar los encabezados HTTP más tarde durante el procesamiento de la solicitud, deshaciendo potencialmente o confundiendo de alguna otra manera los módulos que examinaron o modificaron los encabezados de la solicitud anteriormente. Esta solución agrega la directiva "MergeTrailers" para restaurar el comportamiento heredado.	Media
Apache HTTPD: mod_dav crash (CVE-2013-6438) (apache-httpd-cve-2013-6438)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_dav. Revise la configuración de su servidor web para su validación. El código de análisis XML en mod_dav calcula incorrectamente el final de la cadena al eliminar los espacios iniciales y coloca un carácter NUL fuera del búfer, lo que provoca bloqueos aleatorios. Este código de análisis XML solo se utiliza con los módulos del proveedor DAV que admiten DeltaV, de los cuales el único proveedor publicado públicamente es mod_dav_svn.	Media
Apache HTTPD: mod_log_config crash (CVE-2014-0098) (apache-httpd-cve-2014-0098)	El activo afectado es vulnerable a esta vulnerabilidad SOLAMENTE si ejecuta uno de los siguientes módulos: mod_log_config. Revise la configuración de su servidor web para su validación. Se encontró una falla en mod_log_config. Un atacante remoto podría enviar una cookie truncada específica causando un bloqueo. Este bloqueo solo sería una denegación de servicio si se utiliza un MPM con hilos.	Media
Apache HTTPD: mod_cgid denegación de servicio (CVE-2014-0231) (apache-httpd-cve-2014-0231)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_cgid. Revise la configuración de su servidor web para su validación. Una falla fue encontrada en mod_cgid. Si un servidor que usa mod_cgid alojó scripts CGI que no consumieron entrada estándar, un atacante remoto podría hacer que los procesos secundarios se cuelguen indefinidamente, lo que provocaría una denegación de servicio.	Media
Apache HTTPD: bloqueo de mod_cache con el encabezado Content-Type vacío (CVE-2014-3581) (apache-httpd-cve-2014-3581)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_cache. Revise la configuración de su servidor web para su validación. Se encontró una deferencia de puntero NULL en mod_cache. Un servidor HTTP malintencionado podría provocar un bloqueo en una configuración de proxy de almacenamiento en caché. Este bloqueo solo sería una denegación de servicio si se utiliza un MPM con hilos.	Media
Apache HTTPD: ataque de contrabando de solicitudes HTTP contra analizador de solicitudes fragmentadas (CVE-2015-3183) (apache-httpd-cve-2015-3183)	Un ataque de contrabando de solicitudes HTTP fue posible debido a un error en el análisis de solicitudes fragmentadas. Un cliente malintencionado podría forzar al servidor a malinterpretar la longitud de la solicitud, permitiendo el envenenamiento de caché o el secuestro de credenciales si se está utilizando un proxy intermediario.	Media

Apache HTTPD: Relleno de Oracle en Apache mod_session_crypto (CVE-2016-0736) (apache-httpd-cve-2016-0736)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_session_crypto. Revise la configuración de su servidor web para su validación. Antes de la versión 2.4.25 de Apache HTTP, mod_sessioncrypto estaba cifrando sus datos / cookie utilizando los cifrados configurados con posiblemente los modos de operación CBC o ECB (AES256-CBC de forma predeterminada), por lo tanto, no hay cifrado autenticable integrado o seleccionable. Esto lo hizo vulnerable a los ataques de Oracle Oracle, particularmente con CBC. Ahora se agrega una etiqueta de autenticación (SipHash MAC) para evitar tales ataques.	Media
Apache HTTPD: Vulnerabilidad de DoS en mod_auth_digest (CVE-2016-2161) (apache-httpd-cve-2016-2161)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_auth_digest. Revise la configuración de su servidor web para su validación. La entrada maliciosa a mod_auth_digest causará que el servidor se bloquee, y cada instancia continúa fallando incluso para solicitudes subsiguientes válidas.	Media
Apache HTTPD: Mitigación de entorno HTTP_PROXY "httpoxy" (CVE-2016-5387) (apache-httpd-cve-2016-5387)	HTTP_PROXY es una variable de entorno bien definida en un proceso CGI, que colisionó con varias bibliotecas que no lograron evitar la colisión con este espacio de nombres CGI. Se proporciona una mitigación para el entorno CGI de httpd para evitar llenar la variable "HTTP_PROXY" desde un encabezado "Proxy:", que nunca ha sido registrado por IANA. Esta solución y el parche están documentados en el Aviso de ASF en asf-httpoxy-response.txt e incorporado en las versiones 2.4.25 y 2.2.32. Nota: Esto no tiene asignada una severidad de httpd, ya que es un defecto en otro software que sobrecargó las variables de entorno CGI bien establecidas y no refleja un error en el software del servidor HTTP.	Media

Apache HTTPD: Solicitud HTTP de Apache que analiza los defectos de los espacios en blanco (CVE-2016-8743) (apache-httpd-cve-2016-8743)	El servidor HTTP de Apache, antes de la versión 2.4.25 (2.2.32), aceptó un amplio patrón de patrones de espacio en blanco inusuales del agente de usuario, incluidos CR, FF y VTAB desnudos al analizar la línea de solicitud y las líneas de encabezado de solicitud, así como HTAB en el análisis de la línea de solicitud. Cualquier CR simple presente en las líneas de solicitud se trató como espacios en blanco y permaneció en el miembro del campo de solicitud "the_request", mientras que un CR simple en el nombre del campo del encabezado de la solicitud se consideraría como espacio en blanco, y se mantuvo un CR simple en el valor del campo del encabezado de la solicitud la matriz de encabezados de entrada. Los espacios en blanco adicionales implícitos se aceptaron en la línea de solicitud y antes del delimitador ':' de cualquier línea de encabezado de solicitud. RFC7230 Sección 3.5 llama a algunas de estas excepciones de espacios en blanco, y la sección 3.2. 3 eliminó y aclaró el papel de los espacios en blanco implícitos en la gramática de esta especificación. La Sección 3.1.1 requiere exactamente un solo SP entre el método y el objetivo de la solicitud, y entre el objetivo de la solicitud y la versión de HTTP, seguido inmediatamente por una secuencia de CRLF. Ninguno de estos campos permite ningún carácter CTL (no codificado) en absoluto. La Sección 3.2.4 prohibió explícitamente cualquier espacio en blanco del campo del encabezado de la solicitud antes del carácter ':', mientras que la Sección 3.2 no permite todos los caracteres CTL en la línea del encabezado de la solicitud que no sean el carácter HTAB como espacios en blanco. Estos defectos representan un problema de seguridad cuando httpd participa en cualquier cadena de proxies o interactúa con servidores de aplicaciones back-end, ya sea a través de mod_proxy o mediante mecanismos CGI convencionales. En cada caso en el que un agente acepta dichos caracteres CTL y no los trata como espacios en blanco, existe la posibilidad en una cadena de proxy de generar dos respuestas desde un servidor detrás del agente de proxy no cauteloso. En una secuencia de dos solicitudes, esto hace que la solicitud A al primer proxy se interprete como solicitudes A + A 'por el servidor de back-end, y si las solicitudes A y B se enviaron al primer proxy en una conexión de keepalive, el proxy puede interpretar la respuesta A 'como la respuesta a la solicitud B, contaminando la memoria caché o posiblemente entregando el contenido de A' a un agente de usuario intermedio diferente. Estos defectos se solucionan con el lanzamiento de Apache HTTP Server 2.4.25 y se coordinan mediante una nueva directiva; HttpProtocolOptions Strict, que es el comportamiento predeterminado de 2.4.25 y versiones posteriores. Cambiando de 'estricto' comportamiento al comportamiento "inseguro", algunas de las restricciones se pueden relajar para permitir que algunos clientes HTTP / 1.1 no válidos se comuniquen con el servidor, pero esto reintroducirá la posibilidad de los problemas descritos en esta evaluación. Tenga en cuenta que al reducir el comportamiento a "Inseguro" aún no se permitirán las CTL sin procesar que no sean HTAB (donde esté permitido), pero no se aplicarán otros requisitos de RFC, como exactamente dos caracteres SP en la línea de solicitud.	Media

Apache HTTPD: Escritura fuera de límite en mod_authnz_ldap cuando se usan valores de Accept-Language demasiado pequeños (CVE-2017-15710) (apache-httpd-cve-2017-15710)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_authnz_ldap. Revise la configuración de su servidor web para su validación. mod_authnz_ldap, si está configurado con AuthLDAPCharsetConfig, usa el valor del encabezado Accept-Language para buscar la codificación del juego de caracteres correcto al verificar las credenciales del usuario. Si el valor del encabezado no está presente en la tabla de conversión de caracteres, se utiliza un mecanismo de reserva para truncarlo en un valor de dos caracteres para permitir un reintento rápido (por ejemplo, "en-US" se trunca a "en"). Un valor de encabezado de menos de dos caracteres fuerza una escritura fuera de límite de un byte NUL a una ubicación de memoria que no forma parte de la cadena. En el peor de los casos, muy poco probable, el proceso se bloquearía, lo que podría usarse como un ataque de denegación de servicio.	Media
Apache HTTPD: uso después de usar cuando se usa <Limit> con un método no reconocido en .htaccess ("OptionsBleed") (CVE-2017-9798) (apache-httpd-cve-2017-9798)	Cuando se proporciona un Método HTTP no reconocido en una directiva <Límite {método}> en un archivo .htaccess, y ese archivo .htaccess es procesado por la solicitud correspondiente, la tabla de métodos globales está dañada en el proceso de trabajo actual, lo que resulta en un comportamiento errático . Este comportamiento se puede evitar enumerando todos los métodos HTTP inusuales en una directiva global httpd.conf RegisterHttpMethod en la versión 2.4d de httpd y posteriores. Para permitir otras directivas .htaccess mientras se deniega la directiva <Limit>, consulte la directiva AllowOverrideList. El parche del código fuente (2.4) está en; CVE-2017-9798-patch-2.4.patch El parche del código fuente (2.2) se encuentra en; CVE-2017-9798-patch-2.2.patch Nota 2.2 es el final de la vida útil, no se planea ninguna otra versión con esta solución. Se recomienda a los usuarios que migren a 2.4.28 o posterior para esta y otras correcciones.	Media
Apache HTTPD: posible lectura fuera de límite en mod_cache_socache (CVE-2018-1303) (apache-httpd-cve-2018-1303)	El activo afectado es vulnerable a esta vulnerabilidad SOLAMENTE si ejecuta uno de los siguientes módulos: mod_cache_socache. Revise la configuración de su servidor web para su validación. Un encabezado de solicitud HTTP especialmente diseñado podría haber estrellado el servidor HTTP Apache antes de la versión 2.4.33 debido a una lectura fuera de límite mientras preparaba los datos para ser almacenados en la memoria compartida. Podría usarse como un ataque de denegación de servicio contra usuarios de mod_cache_socache.	Media
Base de datos de acceso abierto (base de datos de acceso abierto)	La base de datos permite a cualquier sistema remoto la posibilidad de conectarse a él. Se recomienda limitar el acceso directo a los sistemas de confianza porque las bases de datos pueden contener datos confidenciales, y se descubren rutinariamente nuevas vulnerabilidades y vulnerabilidades para ellos. Por esta razón, es una violación de la sección 1.3.6 de PCI DSS tener bases de datos que escuchan en puertos accesibles desde Internet, incluso cuando están protegidos con mecanismos de autenticación seguros.	Media
Instalación predeterminada de Apache / página de bienvenida instalada (http-apache-default-install-page)	La instalación predeterminada de Apache o la página de "Bienvenida" se instala en este servidor. Por lo general, esto indica un servidor recién instalado que aún no se ha configurado correctamente y que puede no conocerse. En muchos casos, Apache se instala de forma predeterminada y es posible que el usuario no sepa que el servidor web se está ejecutando. Estos servidores rara vez están parcheados y rara vez son monitoreados, lo que brinda a los piratas informáticos un objetivo conveniente que probablemente no dispare ninguna alarma.	Media
Vulnerabilidad de PHP: CVE-2018-19396 (php-cve-2018-19396)	ext / standard / var_unserializer.c en PHP 5.x a 7.1.24 permite que los atacantes causen una denegación de servicio (bloqueo de la	Media

	aplicación) a través de una llamada unserialize para la clase com, dotnet o variante.	
Vulnerabilidad de PHP: CVE-2018-19935 (php-cve-2018-19935)	ext / imap / php_imap.c en PHP 5.xy 7.x antes de la versión 7.3.0 permite a los atacantes remotos causar una denegación de servicio (eliminación de puntero NULL y bloqueo de la aplicación) a través de una cadena vacía en el argumento del mensaje a la función imap_mail.	Media
Apache HTTPD: bloqueo de mod_cache (CVE-2013-4352) (apache-httpd-cve-2013-4352)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_cache. Revise la configuración de su servidor web para su validación. Se encontró una desreferencia de puntero NULL en mod_cache. Un servidor HTTP malintencionado podría provocar un bloqueo en una configuración de proxy de almacenamiento en caché. (Tenga en cuenta que esta vulnerabilidad se corrigió en la versión 2.4.7, pero el impacto en la seguridad no se reveló en el momento de la versión).	Media
Apache HTTPD: mod_proxy denegación de servicio (CVE-2014-0117) (apache-httpd-cve-2014-0117)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_proxy. Revise la configuración de su servidor web para su validación. Se encontró una falla en mod_proxy en las versiones 2.4d a 2.4.9 de httpd. Un atacante remoto podría enviar una solicitud cuidadosamente elaborada a un servidor configurado como un proxy inverso y provocar que el proceso secundario se bloquee. Esto podría dar lugar a una denegación de servicio contra un MPM con hilos.	Media
Apache HTTPD: mod_deflate denegación de servicio (CVE-2014-0118) (apache-httpd-cve-2014-0118)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_deflate. Revise la configuración de su servidor web para su validación. Se encontró un defecto de consumo de recursos en mod_deflate. Si se configuró la descompresión del cuerpo de la solicitud (utilizando el filtro de entrada "DESINFLAR"), un atacante remoto podría hacer que el servidor consumiera recursos significativos de memoria y / o CPU. El uso de la descompresión del cuerpo de solicitud no es una configuración común.	Media
Apache HTTPD: mod_lua múltiple "Require" el manejo de directivas no funciona (CVE-2014-8109) (apache-httpd-cve-2014-8109)	El activo afectado es vulnerable a esta vulnerabilidad SOLAMENTE si ejecuta uno de los siguientes módulos: mod_lua. Revise la configuración de su servidor web para su validación. Corrija el manejo de la línea Require en mod_lau cuando se usa un LuaAuthzProvider en varias directivas Require con diferentes argumentos. Esto podría llevar a reglas de autenticación diferentes a las esperadas.	Media
Apache HTTPD: ap_some_auth_required API inutilizable (CVE-2015-3185) (apache-httpd-cve-2015-3185)	Un error de diseño en la función "ap_some_auth_required" hace que la API sea inutilizable en httpd 2.4.x. En particular, la API está documentada para responder si la solicitud requirió autenticación, pero solo responde si hay líneas Requeridas en la configuración correspondiente. Dado que 2.4.x Require, las líneas también se utilizan para la autorización y pueden aparecer en las configuraciones incluso cuando no se requiere autenticación y la solicitud no tiene restricciones. Esto podría hacer que los módulos utilicen esta API para permitir el acceso cuando, de lo contrario, no deberían hacerlo. Los usuarios de la API deben usar la nueva API ap_some_authn_required agregada en 2.4.16 en su lugar.	Media
Apache HTTPD: inyección mod_userdir CRLF (CVE-2016-4975) (apache-httpd-cve-2016-4975)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_userdir. Revise la configuración de su servidor web para su validación. Posible inyección de CRLF que permite ataques de división de respuestas HTTP para sitios que usan mod_userdir. Este problema se mitigó con los cambios realizados en 2.4.25 y 2.2.32 que prohíben la inyección de CR o LF en la "Ubicación" u otra clave o valor de encabezado de salida.	Media

Apache HTTPD: manipulación de datos mod_session para aplicaciones CGI (CVE-2018-1283) (apache-httpd-cve-2018-1283)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_session. Revise la configuración de su servidor web para su validación. Cuando mod_session está configurado para reenviar sus datos de sesión a aplicaciones CGI (SessionEnv activado, no el predeterminado), un usuario remoto puede influir en su contenido utilizando un encabezado de "Sesión". Esto proviene del nombre de variable "HTTP_SESSION" utilizado por mod_session para reenviar sus datos a CGI, ya que el servidor HTTP Apache también utiliza el prefijo "HTTP_" para pasar los campos de encabezado HTTP, según las especificaciones CGI. La gravedad se establece en Moderada porque "SessionEnv on" no es una configuración por defecto ni común, sin embargo, debe considerarse más grave cuando este es el caso, debido a la posible explotación remota.	Media
Apache HTTPD: posible acceso fuera de enlace después de un error en la lectura de la solicitud HTTP (CVE-2018-1301) (apache-httpd-cve-2018-1301)	Una solicitud especialmente diseñada podría haber colapsado el servidor HTTP Apache antes de la versión 2.4.33, debido a un acceso fuera del límite después de alcanzar un límite de tamaño al leer el encabezado HTTP. Esta vulnerabilidad se considera muy difícil, si no imposible, de activar en modo sin depuración (tanto en el nivel de registro como en el de compilación), por lo que se clasifica como bajo riesgo de uso común del servidor.	Media
Apache HTTPD: mod_session_cookie no respeta el tiempo de caducidad (CVE-2018-17199) (apache-httpd-cve-2018-17199)	El activo afectado es vulnerable a esta vulnerabilidad SOLO si ejecuta uno de los siguientes módulos: mod_session_cookie. Revise la configuración de su servidor web para su validación. En la versión 2.4.37 de Apache HTTP Server 2.4 y anteriores, mod_session comprueba el tiempo de expiración de la sesión antes de decodificar la sesión. Esto hace que el tiempo de caducidad de la sesión se ignore para las sesiones mod_session_cookie, ya que la hora de caducidad se carga cuando se descodifica la sesión.	Media
Vulnerabilidad de PHP: CVE-2018-17082 (php-cve-2018-17082)	El componente Apache2 en PHP antes de 5.6.38, 7.0.x antes de 7.0.32, 7.1.x antes de 7.1.22 y 7.2.x antes de 7.2.10 permite a XSS a través del cuerpo de una solicitud de "Codificación de transferencia: fragmentada", porque la brigada del grupo se maneja mal en la función php_handler en sapi / apache2handler / sapi_apache2.c.	Media
Método HTTP OPTIONS habilitado (http-options-method-enabled)	Los servidores web que responden al método OPTIONS HTTP exponen qué otros métodos son compatibles con el servidor web, lo que permite a los atacantes limitar e intensificar sus esfuerzos.	Baja

Anexo 4: Vulnerabilidades encontradas en el escaneo realizado con Nexpose (asociadas al gestor de base de datos)

ANEXO 6

SOLUCIONES ESTABLECIDAS TANTO POR NESSUS Y NEXPOSE PARA LAS VULNERABILIDADES ENCONTRADAS LUEGO DEL ESCANEO DE LOS SISTEMAS GESTORES DE BASES DE DATOS.

ULNERABILIDAD	RECOMENDACIÓN
Métodos HTTP TRACE / TRACK permitidos	Desactiva estos métodos. Consulte la salida del complemento para obtener más información.
Cifras en modo CBC del servidor SSH habilitadas	Póngase en contacto con el proveedor o consulte la documentación del producto para deshabilitar el cifrado de cifrado en modo CBC y habilitar el cifrado de cifrado CTR o GCM.

Anexo 6: Solución a vulnerabilidades encontradas en MySQL con Nessus

VULNERABILIDAD	RECOMENDACIÓN
Vulnerabilidad de Oracle MySQL: CVE-2018-3185 (oracle-mysql-cve-2018-3185)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3187 (oracle-mysql-cve-2018-3187)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3247 (oracle-mysql-cve-2018-3247)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2019-2534 (oracle-mysql-cve-2019-2534)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3171 (oracle-mysql-cve-2018-3171)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3133 (oracle-mysql-cve-2018-3133)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3143 (oracle-mysql-cve-2018-3143)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3144 (oracle-mysql-cve-2018-3144)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3155 (oracle-mysql-cve-2018-3155)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3156 (oracle-mysql-cve-2018-3156)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de Oracle MySQL: CVE-2018-3161 (oracle-mysql-cve-2018-3161)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de Oracle MySQL: CVE-2018-3162 (oracle-mysql-cve-2018-3162)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de Oracle MySQL: CVE-2018-3173 (oracle-mysql-cve-2018-3173)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en MySQL de Oracle: CVE-2018-3200 (oracle-mysql-cve-2018-3200)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3277 (oracle-mysql-cve-2018-3277)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de Oracle MySQL: CVE-2018-3251 (oracle-mysql-cve-2018-3251)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3276 (oracle-mysql-cve-2018-3276)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en MySQL de Oracle: CVE-2018-3278 (oracle-mysql-cve-2018-3278)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en MySQL de Oracle: CVE-2018-3282 (oracle-mysql-cve-2018-3282)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3283 (oracle-mysql-cve-2018-3283)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2018-3284 (oracle-mysql-cve-2018-3284)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql

Vulnerabilidad en MySQL de Oracle: CVE-2019-2420 (oracle-mysql-cve-2019-2420)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2019-2434 (oracle-mysql-cve-2019-2434)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2019-2455 (oracle-mysql-cve-2019-2455)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2019-2481 (oracle-mysql-cve-2019-2481)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2019-2482 (oracle-mysql-cve-2019-2482)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2019-2486 (oracle-mysql-cve-2019-2486)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en Oracle MySQL: CVE-2019-2503 (oracle-mysql-cve-2019-2503)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en MySQL de Oracle: CVE-2019-2507 (oracle-mysql-cve-2019-2507)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de MySQL en Oracle: CVE-2019-2510 (oracle-mysql-cve-2019-2510)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en Oracle MySQL: CVE-2019-2528 (oracle-mysql-cve-2019-2528)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en MySQL de Oracle: CVE-2019-2529 (oracle-mysql-cve-2019-2529)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en MySQL de Oracle: CVE-2019-2531 (oracle-mysql-cve-2019-2531)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en MySQL de Oracle: CVE-2019-2532 (oracle-mysql-cve-2019-2532)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad en MySQL de Oracle: CVE-2019-2537 (oracle-mysql-cve-2019-2537)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de Oracle MySQL: CVE-2018-3174 (oracle-mysql-cve-2018-3174)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Vulnerabilidad de Oracle MySQL: CVE-2018-3174 (oracle-mysql-cve-2018-3174)	Descargue y aplique la actualización desde: http://dev.mysql.com/downloads/mysql
Apache HTTPD: Ap_get_basic_auth_pw () Omisión de autenticación (CVE-2017-3167) (apache-httpd-cve-2017-3167)	Apache HTTPD> = 2.2 y <2.2.34 Actualizar a Apache HTTPD versión 2.2.34 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo. Apache HTTPD> = 2.4 y <2.4.26 Actualizar a Apache HTTPD versión 2.4.26 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.26.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: Reflexión de la memoria sin inicializar en mod_auth_digest (CVE-2017-9788) (apache-httpd-cve-2017-9788)	Apache HTTPD> = 2.2 y <2.2.34 Actualizar a Apache HTTPD versión 2.2.34 Descargue y aplique la actualización desde:

	http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo. Apache HTTPD> = 2.4 y <2.4.27 Actualizar a Apache HTTPD versión 2.4.27 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.27.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: mod_status desbordamiento de búfer (CVE-2014-0226) (apache-httpd-cve-2014-0226)	Apache HTTPD> = 2.2 y <2.2.29 Actualizar a la versión de Apache HTTPD 2.2.29 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo. Apache HTTPD> = 2.4 y <2.4.10 Actualiza a Apache HTTPD versión 2.4.10 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.10.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: mod_cgid denegación de servicio (CVE-2014-0231) (apache-httpd-cve-2014-0231)	
Apache HTTPD: mod_deflate denegación de servicio (CVE-2014-0118) (apache-httpd-cve-2014-0118)	
Apache HTTPD: Derivación de procesamiento de HTTP Trailers (CVE-2013-5704) (apache-httpd-cve-2013-5704)	Apache HTTPD> = 2.2 y <2.2.29 Actualizar a la versión de Apache HTTPD 2.2.29 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.2.29.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo. Apache HTTPD> = 2.4 y <2.4.12 Actualiza a Apache HTTPD versión 2.4.12 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.12.tar.gz Muchas plataformas y distribuciones proporcionan paquetes

	binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: omitir <FilesMatch> con una nueva línea final en el nombre del archivo (CVE-2017-15715) (apache-httpd-cve-2017-15715)	Apache HTTPD> = 2.4 y <2.4.33 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.33.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: mod_dav crash (CVE-2013-6438) (apache-httpd-cve-2013-6438)	Apache HTTPD> = 2.2 y <2.2.27 Actualiza a Apache HTTPD versión 2.2.27 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.2.27.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo. Apache HTTPD> = 2.4 y <2.4.9 Actualiza a Apache HTTPD versión 2.4.9 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.9.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Vulnerabilidad de PHP: CVE-2015-9253 (php-cve-2015-9253)	Descargue y aplique la actualización desde: http://www.php.net/releases/
Método HTTP TRACE habilitado (http-trace-method-enabled)	Apache HTTPD Deshabilite el método HTTP TRACE para Apache Las versiones más recientes de Apache (1.3.34 y 2.0.55 y posteriores) proporcionan una directiva de configuración llamada TraceEnable. Para denegar las solicitudes TRACE, agregue la siguiente línea a la configuración del servidor: TraceEnable off Para versiones anteriores del servidor web Apache, use el módulo mod_rewrite para rechazar las solicitudes TRACE: RewriteEngine On RewriteCond% {REQUEST_METHOD} ^ TRACE RewriteRule. * - [F] IIS, PWS, Microsoft-IIS, servicios de información de Internet, servicios de información de Internet, Microsoft-PWS Deshabilite el método HTTP TRACE para Microsoft IIS Para los Servicios de Internet Information Server (IIS) de Microsoft, puede usar la herramienta URLScan, disponible gratuitamente en http://www.microsoft.com/technet/security/tools/urlscan.mspx Servidor web del sistema Java, servidor web SunONE,

	servidor web Sun-ONE, iPlanet Desactive el método HTTP TRACE para SunONE / iPlanet Para Sun ONE / iPlanet Web Server v6.0 SP2 y posterior, agregue la siguiente configuración a la parte superior del objeto predeterminado en el archivo 'obj.conf': <Método del cliente = "RASTREO"> AuthTrans fn = "set-variable" remove-headers = "codificación de transferencia" set-headers = "content-length: -1" error = "501" </Client> A continuación, debe reiniciar el servidor para que los cambios surtan efecto. Para el servidor web Sun ONE / iPlanet antes de v6.0 SP2, siga las instrucciones provistas en la sección 'Ayuda / Solución' del aviso oficial de Sun: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc= fsalert% 2F50603 Lotus Domino Deshabilite el método HTTP TRACE para Domino Siga las instrucciones de IBM para deshabilitar los métodos HTTP en el servidor Domino agregando la siguiente línea al archivo NOTES.INI del servidor: HTTPDisableMethods = TRACE Después de guardar NOTES.INI, reinicie el servidor web de Notes emitiendo el comando de la consola "decirle a http reinicio".
Apache HTTPD: bloqueo de mod_cache con el encabezado Content-Type vacío (CVE-2014-3581) (apache-httpd-cve-2014-3581)	Apache HTTPD> = 2.4 y <2.4.12 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.12.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: ataque de contrabando de solicitudes HTTP contra analizador de solicitudes fragmentadas (CVE-2015-3183) (apache-httpd-cve-2015-3183)	Apache HTTPD> = 2.2 y <2.2.31 Actualizar a Apache HTTPD versión 2.2.31 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.2.31.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo. Apache HTTPD> = 2.4 y <2.4.16 Actualizar a Apache HTTPD versión 2.4.16 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.16.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.

Apache HTTPD: Mitigación de entorno HTTP_PROXY "httpoxy" (CVE-2016-5387) (apache-httpd-cve-2016-5387)	Apache HTTPD> = 2.2 y <2.2.32 Actualizar a Apache HTTPD versión 2.2.32 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.2.32.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo. Apache HTTPD> = 2.4 y <2.4.25 Actualiza a Apache HTTPD versión 2.4.25 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: Relleno de Oracle en Apache mod_session_crypto (CVE-2016-0736) (apache-httpd-cve-2016-0736)	Apache HTTPD> = 2.4 y <2.4.25 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.25.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: uso después de usar cuando se usa <Limit> con un método no reconocido en .htaccess ("OptionsBleed") (CVE-2017-9798) (apache-httpd-cve-2017-9798)	Apache HTTPD> = 2.4 y <2.4.28 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.28.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Base de datos de acceso abierto (base de datos de acceso abierto)	Configure el servidor de base de datos para permitir solo el acceso a sistemas confiables. Por ejemplo, el estándar PCI DSS requiere que coloque la base de datos en una zona de red interna, segregada de la DMZ
Instalación predeterminada de Apache / página de bienvenida instalada (http-apache-default-install-page)	El servidor web Apache debe estar deshabilitado hasta que esté configurado correctamente. Consulte la documentación del servidor HTTP Apache para obtener instrucciones sobre cómo deshabilitar, configurar y volver a habilitar el servidor.
Vulnerabilidad de PHP: CVE-2018-19396 (php-cve-2018-19396)	Actualizar a la versión de PHP 5.6.37 Descargue y aplique la actualización desde: http://www.php.net/releases/ Actualizar a la versión de PHP 7.1.25 Descargue y aplique la actualización desde: http://www.php.net/releases/
Vulnerabilidad de PHP: CVE-2018-19935 (php-cve-2018-19935)	Actualizar a la versión de PHP 5.6.39 Descargue y aplique la actualización desde: http://www.php.net/releases/

	Actualizar a la versión 7.3.0 de PHP Descargue y aplique la actualización desde: http://www.php.net/releases/
Apache HTTPD: bloqueo de mod_cache (CVE-2013-4352) (apache-httpd-cve-2013-4352)	Apache HTTPD> = 2.4 y <2.4.7 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.7.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: mod_proxy denegación de servicio (CVE-2014-0117) (apache-httpd-cve-2014-0117)	Apache HTTPD> = 2.4 y <2.4.10 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.10.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: mod_lua múltiple "Require" el manejo de directivas no funciona (CVE-2014-8109) (apache-httpd-cve-2014-8109)	Apache HTTPD> = 2.4 y <2.4.12 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.12.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: ap_some_auth_required API inutilizable (CVE-2015-3185) (apache-httpd-cve-2015-3185)	Apache HTTPD> = 2.4 y <2.4.16 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.16.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Apache HTTPD: mod_session_cookie no respeta el tiempo de caducidad (CVE-2018-17199) (apache-httpd-cve-2018-17199)	Apache HTTPD> = 2.4 y <2.4.38 Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.4.38.tar.gz Muchas plataformas y distribuciones proporcionan paquetes binarios precompilados para el servidor HTTP Apache. Estos paquetes precompilados generalmente se personalizan y optimizan para una distribución particular, por lo tanto, le recomendamos que utilice los paquetes si están disponibles para su sistema operativo.
Vulnerabilidad de PHP: CVE-2018-17082 (php-cve-2018-17082)	Actualizar a la versión de PHP 5.6.38 Descargue y aplique la actualización desde: http://www.php.net/releases/ Actualizar a la versión de PHP 7.0.32 Descargue y aplique la actualización desde: http://www.php.net/releases/ Actualizar a la versión de PHP 7.1.22

	Descargue y aplique la actualización desde: http://www.php.net/releases/ Actualizar a PHP versión 7.2.10 Descargue y aplique la actualización desde: http://www.php.net/releases/
Método HTTP OPTIONS habilitado (http-options-method-enabled)	Deshabilitar el método de OPCIONES HTTP Desactive el método de OPCIONES HTTP en su servidor web. Consulte el manual de instrucciones de su servidor web sobre cómo hacer esto. Los servidores web que responden al método OPTIONS HTTP exponen qué otros métodos son compatibles con el servidor web, lo que permite a los atacantes limitar e intensificar sus esfuerzos. Apache HTTPD Desactivar el método HTTP OPTIONS para Apache Deshabilite el método OPCIONES incluyendo lo siguiente en la configuración de Apache: <Limite las OPCIONES> Orden negar, permitir Negar todo </Limit> Microsoft IIS Deshabilite el método de OPCIONES HTTP para IIS Deshabilite el método OPCIONES haciendo lo siguiente en el administrador de IIS Seleccione el sitio relevante Seleccione Solicitar filtrado y cambie a la pestaña de verbo HTTP Seleccione Denegar verbo en el panel de acciones Escriba OPCIONES en el cuadro de texto provisto y presione OK nginx nginx Deshabilite el método de OPCIONES HTTP para nginx Deshabilite el método OPCIONES agregando la siguiente línea a su bloque de servidor, puede agregar otros métodos HTTP para que se puedan ejecutar después de la POST limit_except GET POST {deny all; }

Anexo 6: Solución a vulnerabilidades encontradas en MySQL con Nexpose

VULNERABILIDAD	RECOMENDACIÓN
MS16-047: Actualización de seguridad para los protocolos remotos SAM y LSAD (3148527) (bloqueo) (verificación sin credenciales)	Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.
No se requiere firma SMB	Imponer la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de política 'Servidor de red de Microsoft: firmar comunicaciones digitalmente (siempre)'. En Samba, la configuración se llama 'firma de servidor'. Vea los enlaces 'ver también' para más detalles.

Anexo 6: Solución a vulnerabilidades encontradas en SQL Server con Nessus

VULNERABILIDAD	RECOMENDACIÓN
Firma de SMB deshabilitada (cifs-smb-signature-disabled)	• Microsoft Windows Configurar la firma SMB para Windows Configure el sistema para habilitar o requerir la firma SMB según corresponda. El método y el efecto de hacer esto es específico del sistema, así que consulte este artículo de TechNet para obtener más información. Nota: asegúrese de que la configuración de firma SMB se realiza para las conexiones entrantes (Servidor). • Samba Configurar la firma SMB para Samba Configure Samba para habilitar o requerir la firma SMB según corresponda. Para habilitar la firma SMB, coloque lo siguiente en el archivo de configuración de Samba, generalmente smb.conf, en la sección global: firma de servidor = auto Para requerir la firma SMB, coloque lo siguiente en el archivo de configuración de Samba, generalmente smb.conf, en la sección global: firma del servidor = obligatorio
Windows Autologin habilitado (Windows-Autologin-habilitado)	Vaya al Panel de control de Usuarios y Contraseñas. Asegúrese de que la casilla que dice "Los usuarios deben ingresar un nombre de usuario y una contraseña para usar esta casilla de verificación de la computadora" esté marcada. Haga clic en la pestaña Avanzado. Asegúrese de que esté marcada la casilla que dice "Requerir a los usuarios que presionen Ctrl-Alt-Del antes de iniciar sesión". Haga clic en Aceptar para aplicar la configuración y salir del panel de control. NOTA: Si su computadora es miembro de un dominio, esta opción no aparecerá en su panel de control. Para deshabilitar la característica, debe editar el registro: Abra su editor de registro (regedit.exe) y busque: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon Asegúrese de que el valor REG_SZ de "AutoAdminLogon" esté establecido en "0". Los valores "DefaultUser" y "DefaultPassword" deben eliminarse.

Firma de SMB no requerida (cifs-smb-firmando-no-requerida)	• Microsoft Windows Configurar la firma SMB para Windows Configure el sistema para habilitar o requerir la firma SMB según corresponda. El método y el efecto de hacer esto es específico del sistema, así que consulte este artículo de TechNet para obtener más información. Nota: asegúrese de que la configuración de firma SMB se realiza para las conexiones entrantes (Servidor). • Samba Configurar la firma SMB para Samba Configure Samba para habilitar o requerir la firma SMB según corresponda. Para habilitar la firma SMB, coloque lo siguiente en el archivo de configuración de Samba, generalmente smb.conf, en la sección global: firma de servidor = auto Para requerir la firma SMB, coloque lo siguiente en el archivo de configuración de Samba, generalmente smb.conf, en la sección global: firma del servidor = obligatorio

No se requiere la firma SMBv2 (cifs-smb2-signature-no-required)	• Microsoft Windows Configurar la firma SMB para Windows Configure el sistema para habilitar o requerir la firma SMB según corresponda. El método y el efecto de hacer esto es específico del sistema, así que consulte este artículo de TechNet para obtener más información. Nota: asegúrese de que la configuración de firma SMB se realiza para las conexiones entrantes (Servidor). • Samba Configurar la firma SMB para Samba Configure Samba para habilitar o requerir la firma SMB según corresponda. Para habilitar la firma SMB, coloque lo siguiente en el archivo de configuración de Samba, generalmente smb.conf, en la sección global: firma de servidor = auto Para requerir la firma SMB, coloque lo siguiente en el archivo de configuración de Samba, generalmente smb.conf, en la sección global: firma del servidor = obligatorio

Firma de SMB no requerida (cifs-smb-firmando-no-requerida)	• Microsoft Windows Configurar la firma SMB para Windows Configure el sistema para habilitar o requerir la firma SMB según corresponda. El método y el efecto de hacer esto es específico del sistema, así que consulte este artículo de TechNet para obtener más información. Nota: asegúrese de que la configuración de firma SMB se realiza para las conexiones entrantes (Servidor). • Samba Configurar la firma SMB para Samba Configure Samba para habilitar o requerir la firma SMB según corresponda. Para habilitar la firma SMB, coloque lo siguiente en el archivo de configuración de Samba, generalmente smb.conf, en la sección global: firma de servidor = auto Para requerir la firma SMB, coloque lo siguiente en el archivo de configuración de Samba, generalmente smb.conf, en la sección global: firma del servidor = obligatorio
Amplificación del tráfico NetBIOS NBSTAT (amplificación netbios-nbstat)	NetBIOS puede ser importante para el correcto funcionamiento de una red de Windows dependiendo del diseño. Restrinja el acceso al servicio NetBIOS solo a activos de confianza.

Anexo 6: Solución a vulnerabilidades encontradas en SQL Server con Nexpose.

ANEXO 7

DESCRIPCIÓN Y VALORACIÓN DE LAS MEJORAS POR CADA AMENAZA DETECTADA

CÓDIGO	AMENAZA	SALVAGUARDAS	DETALLE	COSTO
I. 5	Avería de origen físico o lógico	Disponer de sensores de monitoreo del estado del hardware, esto permitirá verificar el tiempo de vida útil para así elaborar un plan de renovación para el mismo y para el estado del software con escaneo permitirá verificar su vulnerabilidad	La revisión física de los equipos se aplicará 3 veces al año, con un costo de $750,00 la lógica mediante Nessus con un costo anual es de $2495,00	**$2750,00**
I.8	Fallo de servicio de comunicaciones	Realizar una evaluación de los sistemas, con el fin de elaborar un plan de gestión para mitigar los riesgos	El plan de gestión se realiza una vez y tiene un costo estimado de $3000,00	**$3,000**
		Disponer de sistemas de comunicación redundantes con el fin de dar continuidad a los procesos en caso de fallos. (RAID, Tarjetas de red, fuentes de alimentación)	Adquirir sistemas de comunicación redundantes significa un costo de $3500,00	**$3,500**
		Elaborar documentos de respaldo de la configuración de los dispositivos y del acceso al sistema	La elaboración de respaldos de configuración se realiza diariamente con un costo estimado de $2,00 diarios	**$520,00**
I.10	Degradación de los soportes de almacenamiento de la información	Elaborar inventarios actualizados cada 3 meses de los recursos con los que se cuenta	La elaboración de inventarios y control de vida útil se hará cada 3 meses con un costo estimado de $25,00	**$100,00**
		Disponer de elementos redundantes que permitan la continuidad de las operaciones sin pérdidas de tiempo en caso de fallos.	Contar con elementos redundantes de comunicación estima un costo de $2000,00	**$2000,00**
E. 1	Errores de los usuarios	Capacitar al personal sobre la importancia de cuidar sus claves de acceso y demás datos que puedan comprometer el buen desempeño de las actividades de las instituciones.	Por capacitación permanente en seguridad y sentido de pertenencia a una institución, se considera un costo de $1500,00	$**1500,00**
E.2	Errores del Administrador	Presentar al personal un manual de políticas de responsabilidades y procedimientos de operación en caso de errores	En la elaboración de manuales de políticas de responsabilidades se estima un costo de $100,00	**$100,00**
		Asignar a cada usuario un orden especifico de tareas claras y directas para evitar errores de omisión o que las tareas se realicen de forma redundante.	Capacitar al personal en su rol a cumplir dentro de la institución $150,00	**$150,00**
		Documentar los permisos de accesos y privilegios por roles de cada usuario de la información.	La documentación de los permisos de usuario se realizará en cada contratación o ascenso del empleado $20,00	**$20,00**
E.3	Errores de monitorización (Log)	Capacitar al personal sobre la importancia de cuidar sus claves de acceso y demás datos que puedan	Las capacitaciones se realizarán de forma bimensual con un costo de	**$1200, 00**

		comprometer el buen desempeño de las actividades de las instituciones. Concienciación, educación y capacitación en seguimiento de la información	$200,00 cada una además de campañas digitales.	
E. 4	Errores de configuración	Realizar pruebas de actualizaciones previo a la instalación.	Las pruebas de actualización se realizan mensualmente con un costo de $20,00	**$240,00**
		Realizar pruebas mensuales del cortafuegos.	Las pruebas a cortafuegos suponen un costo de $45,00 mensuales	**$540,00**
		Definir procesos de configuración de los equipos según el rol que desempeñe el usuario dentro de la institución.	La definición de procesos de roles de usuario se lo hará 2 veces al año con un costo de $200,00	**$400,00**
		Disponer de equipos alternos para realizar pruebas de concepto, con el fin adaptar y mejorar las ideas y lograr una mejor aceptación.	En adquisición de equipos alternos se estima un costo de $8000,00	**$8000,00**
E.8	Difusión de Software dañino	Realizar semanal o mensualmente controles contra códigos maliciosos.	En la adquisición de antivirus se estima un costo de $3000,00	**$3000,00**
E.9	Errores de (re)encaminamiento	Realizar una adecuada configuración de los switches.	En la adquisición de antivirus se estima un costo de $3000,00	**$3000,00**
		Disponer de personal capacitado para la administración de los equipos.	Adquirir switches origina un costo de $1700,00 con instalación y mantenimiento por 1 año	**$1700,00**
E. 10	Errores de secuencia	Disponer de plan de recuperación de la información integra para evitar su alteración.	Disponer de un plan de recuperación de la información tiene un costo de $300,00	**$300,00**
E.15	Alteración accidental de la información	Crear perfiles de usuario con los permisos correspondientes para cada empleado. Realizar diariamente copias de seguridad de la información, para su verificación en caso de cambios inesperados.	Las copias de seguridad se realizarán diariamente con un costo de $1,00 diario	**$360,00**
E. 20	Vulnerabilidades de los programas (software)	Evitar el uso de cualquier dispositivo de almacenamiento en los equipos de la institución. Evitar la instalación o uso de aplicaciones no autorizadas en los equipos de la institución.	Se capacita al personal en temas de seguridad del uso de programas cada 3 meses con un costo de $200,00 por capacitación	**$800,00**

		Utilizar protocolos de seguridad para proteger las comunicaciones.		
E.21	Errores de Mantenimiento / Actualización de Equipos	Creación de perfiles de seguridad. Creación de puntos de recuperación de la información para evitar cambios no deseados en los equipos.	Crear perfiles y puntos de recuperación de información se realizará 2 veces al año con un costo de $250,00	**$500,00**
E.24	Caída del sistema por agotamiento de recursos	Disponer de elementos redundantes, para suplir en caso de agotamiento de los recursos disponibles en la institución. Realizar periódicamente mantenimiento preventivo de los equipos, para evitar la pérdida del recurso.	El mantenimiento de los equipos se lo hará 2 veces al año con un costo de $500,00 cada uno	**$1000,00**
		Mantenimiento correctivo de los equipos, en caso de fallos en el mismo.		
A. 3	Manipulación de registro de actividades (log)	Contar con políticas de control de acceso. Realizar copias de seguridad de la información para el análisis, gestión de logs y control de acceso lógico.	Las políticas de control de acceso y sus copias de seguridad se harán una vez al año con un costo de $500,00	$**500,00**
A. 4	Manipulación de los ficheros de configuración	Asignación de privilegios de acceso de los usuarios.	La capacitación para el asignar acceso al sistema se revisará 2 veces al año con un costo de $80,00	**$160,00**
A.5	Suplantación de identidad del usuario	Cifrado de información sensible.	Cifrado de información sensible se lo hará diariamente con un costo de $2,0	**$720,00**
		Solicitar el uso de información confidencial para la autenticación.	La capacitación en seguridad se hará dos veces al año con un costo de $500,00	**$500,00**
A.6	Abuso de privilegios de acceso	Aplicar perfiles de seguridad de usuarios. Revisión de los derechos de acceso de los usuarios.	Contratar a un experto en seguridad que verifique los procesos llevados a cabo supone un costo de $400,00 al año	**$400,00**
A.7	Uso no previsto	Formación y concientización del personal en cuanto a seguridad Uso aceptable de los activos, según la normativa institucional.	Capacitar al personal en una vez cada 3 meses representa un costo de $600,00	**$600,00**

A. 8	Difusión de Software dañino	Implementar procesos de hardering de servidores con el fin de reducir las vulnerabilidades a las que se expone el sistema. Revisar y actualizar periódicamente los incidentes que se presenten y la solución aplicada.	La actualización de protocolos de seguridad estima un costo de $850,00 al año	**$850,00**
A. 9	(re) encaminamiento de mensajes	Crear políticas y procedimientos de intercambio de información. Capacitar al personal sobre el adecuado uso y envío de la información	Crear políticas de seguridad y capacitar al personal supone un costo anual de $650,00	**$650,00**
A. 10	Alteración de secuencia	Realizar controles de acceso a la información de acuerdo al orden establecido.	Revisión mensual del plan de controles de acción establecido supone un costo de $30,00 mensuales	**$360,00**
A. 11	Acceso no autorizado	Cambiar siempre las configuraciones por defecto de los equipos.	Elaborar el plan de políticas de acceso supone un costo anual de $100,00	**$100,00**
		Implementación de sistema de detección de intrusos.	La configuración de los equipos supone un costo de $80,00 se lo hace al momento de la compra.	**$80,00**
A. 14	Interceptación de información (escucha)	Establecer políticas para el control de la seguridad de la información y capacitar al personal para su correcta aplicación.	Crear políticas de seguridad y capacitar al personal supone un costo anual de $650,00	**$650,00**
		Aplicar políticas de seguridad a la red.	La instalación de sensores el tráfico de información representa un costo de $750,00	**$750,00**
		Utilizar cifrado de datos para evitar que sean leídos por todos.	Capacitación en seguridad de información se hará 3 veces al año con un costo de $500,00 cada una	**$1500,00**
A. 22	Manipulación de programas	Uso de herramientas de administración de sistemas, para hacer un seguimiento de las actividades que realiza cada empleado.	La aplicación genera un costo de $600,00	**$600,00**
A.24	Denegación de Servicio	Configurar correctamente el firewall para que analice de forma exhaustiva el tráfico tanto de entrada como de salida.	La actualización del firewall genera un costo de $450,00 al año	**$450,00**

Anexo 7: plan de mejoras por amenaza con valoración económica