UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS

PROGRAMA DE MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

COHORTE 2022

Tema: AUTOMATIZACIÓN DEL DESPLIEGUE DE APLICACIONES WEB JAVA EE EN SERVIDORES LINUX DE X64, BASADO EN LA NORMA ISO/IEC 27001:2018, UTILIZANDO CONTENEDORES DE SOFTWARE.

Trabajo de Titulación, previo a la obtención del Título de Cuarto Nivel de Magister en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones.

Modalidad del Trabajo de Titulación: Componente de Investigación Aplicada y de Desarrollo.

Autor: Ingeniero Fernando Alexander Moya Chiluiza.

Director: Ingeniero Oscar Fernando Ibarra Torres, Magister

Ambato – Ecuador

2023

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por: Ingeniero Héctor Fernando Gómez Alvarado PhD, e integrado por los señores: *Ingeniera Lorena Isabel Barona López PhD e Ingeniera Esthela Maribel Cabezas Molina Magister*, designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: *Automatización del despliegue de aplicaciones web Java EE en servidores Linux de x64, basado en la norma ISO/IEC 27001:2018, utilizando contenedores de software* elaborado y presentado por el señor Ingeniero Fernando Alexander Moya Chiluiza, para optar por el Título de cuarto nivel de Magíster en Tecnologías de la Información mención Seguridad de Redes y Comunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Héctor Fernando Gómez Alvarado PhD
Presidente y Miembro del Tribunal

Ing. Lorena Isabel Barona López PhD
Miembro del Tribunal

Ing. Esthela Maribel Cabezas Molina Mg
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Automatización del despliegue de aplicaciones web Java EE en servidores Linux de x64, basado en la norma ISO/IEC 27001:2018, utilizando contenedores de software, le corresponde exclusivamente a: Ingeniero Fernando Alexander Moya Chiluiza, Autor bajo la Dirección de Ingeniero Oscar Fernando Ibarra Torres, Mg., Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniero Fernando Alexander Moya Chiluiza
c.c.: 1722146261
AUTOR

Ingeniero Oscar Fernando Ibarra Torres, Magister
c.c.: 1804003497
DIRECTOR

DERECHOS DE AUTOR

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

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

Ingeniero Fernando Alexander Moya Chiluiza
c.c.: 1722146261

INDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

A todas y cada una de las personas que estuvieron presentes en este proceso continuo de enseñanza aprendizaje, no solo en la parte académica sino en el día de día.

A la Universidad Técnica de Ambato que me abrió sus puertas para continuar con mis estudios y mi formación académica.

A los docentes de la Maestría en Tecnologías de la Información quienes impartieron sus conocimientos con empeño y ahincó.

Fernando Alexander Moya Chiluiza

DEDICATORIA

A mis padres Alfredo y Fanny quienes con mucho esfuerzo y dedicación me demostraron que todo es posible.

A mi hermano Fabricio quien con sus ocurrencias me saca una sonrisa de la nada.

A José Gabriel quien recién comienza a dar sus primeros pasos.

Fernando Alexander Moya Chiluiza

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
COHORTE 2022

TEMA:

AUTOMATIZACIÓN DEL DESPLIEGUE DE APLICACIONES WEB JAVA EE EN SERVIDORES LINUX DE x64, BASADO EN LA NORMA ISO/IEC 27001:2018, UTILIZANDO CONTENEDORES DE SOFTWARE.

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con Componente de Investigación Aplicada y de Desarrollo.*
AUTOR: *Ingeniero Fernando Alexander Moya Chiluiza*.
DIRECTOR: *Ingeniero Oscar Fernando Ibarra Torres, Magister*
FECHA: *Veinte y seis de Julio de dos mil veinte y tres.*

RESUMEN EJECUTIVO

Este proyecto presenta una investigación sobre la automatización del despliegue de aplicaciones web Java EE en servidores Linux de x64, basado en la norma ISO/IEC 27001:2018, utilizando contenedores de software.

El objetivo principal es optimizar el uso de recursos informáticos en un entorno de pruebas para aplicaciones Java EE, usando contenedores de software y aplicando controles de seguridad de la información, basados en la norma ISO/IEC 27001:2018, y la metodología Magerit versión 3.0 con la finalidad de mejorar la gestión de la seguridad de la información y la administración de los activos de información mediante la identificación, clasificación, valoración de amenazas, vulnerabilidades, riesgos por degradación y probabilidad de ocurrencia para asegurar la confidencialidad, integridad, disponibilidad con el propósito de aplicar diferentes tipos de controles a futuro para garantizar que los riesgos dentro de la organización sean mínimos aplicando diferentes tipos de controles en cada uno de los procesos.

Para la fundamentación teórica se utilizó bases de datos indexadas, artículos científicos, libros y tesis que se alinean con el área de investigación, el enfoque aplicado fue cuantitativo y cualitativo a nivel explicativo, donde se utilizó diferentes

tipos de instrumentos como la entrevista, encuesta a los directivos de la organización y al personal del área de TI.

Este documento se encuentra estructurado por seis capítulos, en los cuales se describen los diferentes temas tratados para el desarrollo del trabajo de investigación, además de los anexos que contienen una guía para la implementación, matrices las cuales se obtuvieron previo a un análisis en base a la información obtenida y encuestas que permitieron conocer de primera mano la situación actual de la organización y cuál fue el grado de satisfacción de la solución planteada.

El proyecto es viable debido a que se cuenta con el apoyo de los directivos y técnicos de la organización en donde la propuesta planteada puede ser aplicada en otras organizaciones y/o empresas consultoras en el área de desarrollo e infraestructura.

DESCRIPTORES: *CONTENEDORES, DOCKER, ESTÁNDARES, ISO/IEC 27001, NORMAS, SERVIDORES, VIRTUALIZACIÓN.*

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Introducción

En el mercado tecnológico existen varias opciones para trabajar con infraestructura en la nube, como Azure de Microsoft, AWS de Amazon, Google Cloud Platform de Google entre otros, y cada una de las empresas proporciona planes empresariales que permiten migrar de tipo de infraestructura, otra forma es trabajar por medio de la virtualización, que consiste en tener varias máquinas virtuales con diferentes prestaciones que interactúan unas con otras y que generan una infraestructura bastante sólida y con casos de éxito.

Una de las principales limitantes al momento de trabajar ya sea con un servidor en la nube o por medio de la virtualización es la capacidad de almacenamiento y procesamiento, que en determinado momento muchos procesos que se encuentren ejecutando se bloquearán hasta que no terminen y si esto sucede en entornos de producción las repercusiones pueden ser graves a corto y largo plazo.

Toda nueva funcionalidad que se cree dentro de una empresa de desarrollo de software debe pasar por controles de calidad, para lo cual se debe generar un entorno similar al de producción que se lo conoce como el ambiente de pruebas, los jefes de desarrollo al percatarse que los productos de software son multiempresa proponen que deben existir varios o un único ambiente e intercalar cada una de las pruebas pertinentes, lo que para los directivos se traduce en tiempo y el tiempo en dinero.

Cada una de las organizaciones debe aplicar una serie de controles desde etapas iniciales, medias y finales aplicando en cada una de ellas la mejora continua para lo cual es importante incorporar la norma ISO/IEC 27001:2018 en la cual se aplica criterios de seguridad de la información como son: Confidencialidad, Integridad y Disponibilidad.

Por tal motivo el presente proyecto tiene como objetivo optimizar el uso de recursos informáticos en un entorno de pruebas para aplicaciones Java EE (Enterprise Edition) usando contenedores de software aplicando controles de seguridad de la información, basado en la norma ISO/IEC 27001:2018.

El trabajo de investigación está estructurado en los siguientes capítulos:

El Capítulo I se enfoca en la introducción y la justificación del tema de investigación considerando aspectos científicos teóricos y experimentales. Además, se describen los objetivos planteados tanto el general como los específicos a cumplir.

El Capítulo II describe los antecedentes investigativos con la revisión de la literatura, el estado del arte del cual se obtiene información valiosa referente al tema de investigación.

El Capítulo III describe a detalle el marco metodológico, ubicación, equipos y materiales a usar, tipos de investigación, prueba de hipótesis, población muestra, recolección de información, procesamiento de información y análisis estadístico, variables respuesta y los resultados alcanzados.

El Capítulo IV describe el análisis y validación de los resultados con conjunto con la verificación de la hipótesis.

El Capítulo V detalla las conclusiones y recomendaciones, fruto de la investigación, dando cumplimiento a los objetivos planteados, además de la bibliografía y anexos que sustentan la investigación.

El Capítulo VI describe la propuesta planteada, la modalidad de titulación, proyecto de titulación, con componente de investigación aplicada y desarrollo.

1.2. Justificación

En la actualidad uno de los activos más importantes para todo tipo de empresa u organización es la información, lo cual la convierte en un insumo de gran utilidad para bien y para mal, lo que obliga a optar por protegerla de cualquier ataque aplicando normas, protocolos, mejorando la infraestructura de red y servidores tanto físicos como en la nube, garantizando aspectos tan importantes como lo es la confidencialidad, integridad y disponibilidad.

Al no trabajar con normas o estándares dentro de una organización se genera una brecha que no permite estar a la vanguardia frente a otras organizaciones, lo que conlleva no solo la pérdida de clientes, prestigio, contratos, etc., y ante una eventualidad o contingencia

no existen los procedimientos necesarios para poder afrontar este tipo de situaciones, lo que se traduce en tiempo, dinero, recursos y ante todo ello es necesario trabajar y crear un esquema de buenas prácticas en el cual se aplique toda la norma o parte de ella con la finalidad de generar un clima de confianza con los clientes y usuarios.

La metodología de trabajo comprende el desarrollo de aplicaciones web Java EE, un servidor de aplicaciones y un motor de bases de datos PostgreSQL en ambientes locales de desarrollo lo cual implica un ambiente ideal de pruebas, por cuestiones de interoperabilidad interna se optó por un SVN (Apache Subversion) a fin de integrar todos los desarrollos en un solo lugar, un servidor que permitan realizar pruebas pertinentes de los sistemas independientemente del equipo donde fue desarrollado.

En el servidor de pruebas coexisten VMs (Máquinas virtuales) cada una configurada con diferentes recursos de memoria, disco, red y cuya principal limitación radica en que las pruebas a realizar no consuman más allá de los recursos asignados en cada VMs, para reducir o amentar recursos entre VMs se debe detener todos los procesos que se encuentren ejecutando lo que conlleva tiempos de espera hasta volver a tener arriba los servicios.

La contratación de un nuevo servidor incurre en gastos adicionales que la organización estará o no dispuesta a invertir, además de posibles vulnerabilidades inherentes propias de la configuración inicial lo que implica aplicar normas y estándares vigentes.

Por los expuesto, surge la necesidad de aplicar la norma ISO/IEC 27001:2018 - Gestión de la seguridad de la información y nuevas tecnologías como lo son los contenedores de software que permiten realizar pruebas de implementación rápidas y continuas, que en conjunto presentarán una alternativa de solución en el trabajo del día a día optimizando tiempo, recursos y costos con la finalidad de que muestre un constante crecimiento, actualización en uso de las TIC y una ventaja frente a otros competidores.

- **Factibilidad técnica:**

  Este proyecto es técnicamente factible de realizar ya que se cuenta con los recursos tecnológicos requeridos como lo es la infraestructura, herramientas tecnológicas, software, datos e información, además de que se enmarcará en lo establecido en la norma ISO/IEC 27001:2018 para sistemas de gestión de seguridad de la información.

- **Factibilidad Operativa:**

  Este proyecto es factible operativamente porqué se dispone de los conocimientos del investigador, el apoyo y apertura de la empresa consultora que se encuentra interesada en aplicarlo a futuro.

- **Factibilidad Económica:**

  Este proyecto es factible económicamente ya que los costos que implican, la búsqueda, análisis, desarrollo y tiempo empleado son asumidos por parte del investigador.

1.3. Objetivos

1.3.1. General

Optimizar el uso de recursos informáticos en un entorno de pruebas para aplicaciones Java EE usando contenedores de software aplicando controles de seguridad de la información, basado en la norma ISO/IEC 27001:2018.

1.3.2. Específicos

- Analizar la norma ISO/IEC 27001:2018 y relacionarla con el fundamento teórico para el desarrollo del proyecto.
- Investigar los diferentes ambientes de contenedores de software que trabajan en servidores Linux x64.
- Definir un ambiente de pruebas para aplicaciones Java EE basado en contenedores de software.
- Evaluar el nivel de aceptación y confianza de la propuesta de solución para el caso de estudio práctico basado en la norma ISO/IEC 27001:2018.

CAPÍTULO II

MARCO TEORICO

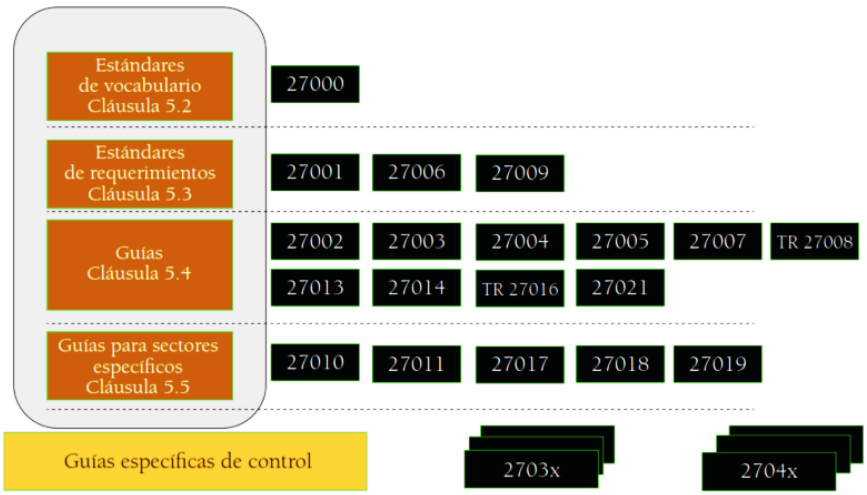
a) ANTECEDENTES INVESTIGATIVOS

Para el autor (Cepeda & De La Cruz, 2018) la norma internacional ISO/IEC 27000 muestra una breve descripción de los pasos a seguir para el establecimiento, monitoreo, mejora de un SGSI (Sistema de Gestión de Seguridad de la Información) y establecer los requisitos mínimos que pueden ser aplicados en cualquier organización.

(Valencia, 2021), lista la relación la relación entre las diecinueve normas principales de la familia de la ISO/IEC 27000, clasificadas en cuatro categorías como se muestra en la Figura 1.

Figura 1

Norma ISO/IEC 27000



Nota. La figura representa la relación entre las diferentes normas de la familia ISO/IEC 27000. Tomado de (Valencia, 2021)

(Cordero, 2022; De la Cruz & Segura, 2017; Guacanés & Vilatuña, 2022) en sus trabajos de titulación mencionan que la norma ISO/IEC 27001 es un estándar publicado por la Organización Internacional de Normalización, el cual pertenece a la familia de normas ISO/IEC 27000 en donde se establecen un modelo de evaluación de creación,

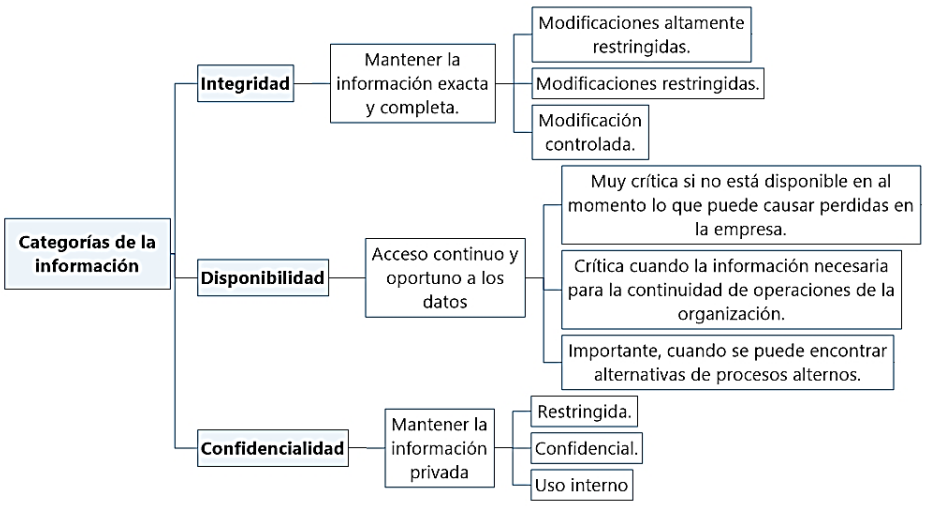
implementación, mantenimiento, operación, supervisión, revisión, mantenimiento de un SGSI de acuerdo al tamaño y necesidades de la empresa.

En la revista científica publica por los autores (Pazmiño et al., 2020), se conceptualiza un activo de información como cualquier elemento que contenga información de los cuales la organización debe tener conocimiento, deben estar clasificados de acuerdo con el grado de sensibilidad o función que cumplen, a fin de dar un tratamiento y protección adecuada.

Para los autores (G. Fernández, 2021; Mendoza & Naranjo, 2020) la seguridad de la información según la norma ISO/IEC 27001 tiene como pilares básicos la confidencialidad, integridad y disponibilidad como se muestra en la Figura 2, que son importantes para mantener los niveles de competitividad, rentabilidad e imagen a fin de cumplir con los objetivos de la organización.

Figura 2

Categorías de la clasificación de la información



Nota. La figura muestra las categorías de la clasificación de la información basado en la triada CID (Confidencialidad, Integridad y Disponibilidad). Tomado de (G. Fernández, 2021).

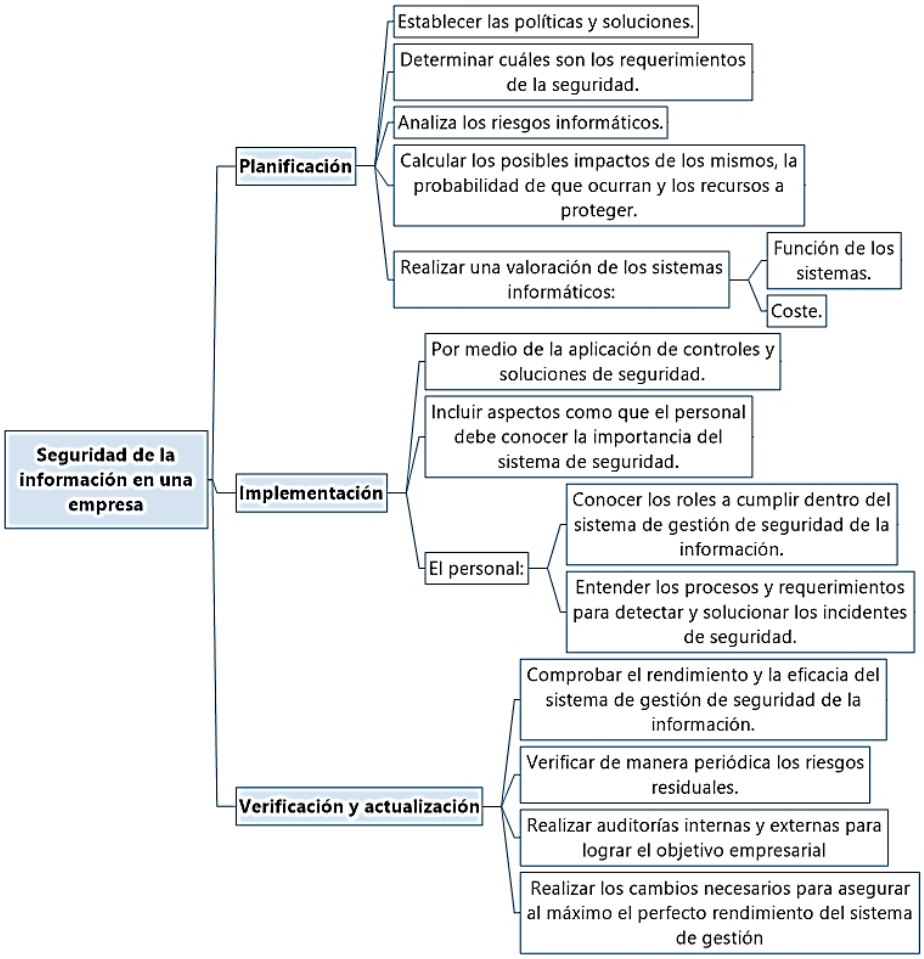
En su proyecto de investigación (Cordero, 2022), describe dos objetivos sobre la seguridad de la información, el objetivo primario es mantener al mínimo los riesgos sobre los recursos informáticos y garantizar la continuidad de la organización mientras se administra el riesgo a un costo aceptable, mientras que el objetivo secundario

garantiza que los documentos, registros y archivos informáticos de la organización mantengan confiabilidad.

Para los autores (G. Fernández, 2021; Mendoza & Naranjo, 2020) la solución más optima es un sistema de gestión de seguridad de la información (SGSI) el cual es un medio eficaz para minimizar los riesgos y que deberá ser sostenible en el tiempo con la capacidad de incorporar mejora continua, además de basarse en cuatro procesos bien diferenciados como lo es la planificación, implementación, verificación y actualización como se detalla en la Figura 3.

Figura 3

Procesos diferenciados de seguridad de la información



Nota. La figura representa los tres procesos bien diferenciados con los que cuenta un SGSI que va desde la planificación, implementación, verificación y actualización. Tomado de *(Mendoza & Naranjo, 2020)*

(Lucano, 2019) lista una serie de beneficios acerca del uso de un SGSI de los que se destacan:

1. El poder contar con procedimientos y procesos para la continuidad y disponibilidad de las operaciones.
2. La existencia de una reducción de costos generados por los incidentes de seguridad de la información.
3. Establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.
4. Prevenir y detectar de manera eficiente y anticipada incidentes de seguridad de la información.

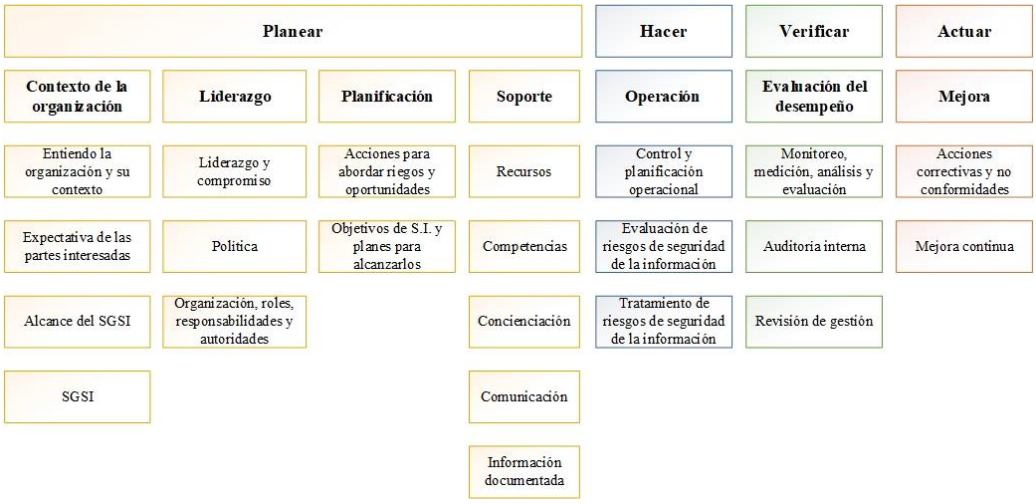
5. Una evaluación continua de la seguridad de la información, con el objetivo de implementar cambios, según se requiera.

En el trabajo de titulación publicado por (Quiñonez Quintero, 2022), se muestra que la norma ISO/IEC 27001 “a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados”.

Por su parte (Guacanés & Vilatuña, 2022) muestran que la norma ISO/IEC 27001 hace referencia al ciclo de Deming o ciclo PDCA (Plan, Do, Check, Act) el cual describe los cuatro pasos esenciales descritos en la Figura 4 para la gestión de la mejora continua y la relación que tiene con la estructura de la norma ISO/IEC 27001.

Figura 4

Ciclo PDCA



Nota. La figura representa al ciclo PDCA y su relación con la estructura general de la norma ISO/IEC 27001.

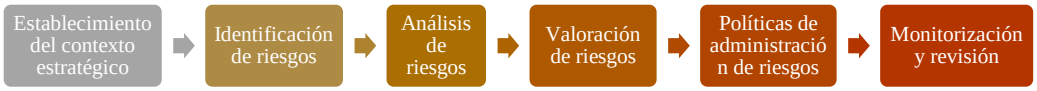
Para los autores (De la Cruz & Segura, 2017) describen que toda empresa debe aplicar el ciclo PDCA de manera sistemática independientemente del tipo, tamaño o naturaleza para lograr la mejora continua, con lo cual se prevé eficiencia, eficacia, disminución de fallos, prevención y eliminación del riesgo hacia los activos de la empresa que son más críticos, al contar con indicadores, métricas y datos reales se convierten en alertas que requerirán su respectiva corrección y mejora.

Los autores (Guano & Jaramillo, 2021) describen a la gestión del riesgo como un proceso estructurado y que comprende una serie de acciones preventivas y correctivas que

permiten la identificación, análisis, cuantificación de la probabilidad de que una amenaza se materialice para posteriormente mitigar, controlar o eliminar las amenazas y así reducir sus efectos negativos, en la Figura 5 se muestran las fases para una correcta gestión del riesgo.

Figura 5

Gestión de riesgo



Nota. La figura representa las fases secuenciales y ordenadas del proceso técnico de la gestión del riesgo.

(Guacanés & Vilatuña, 2022) lista una serie de beneficios sobre la gestión de riesgos y de los cuales se destacan:

1. Reducir el número de incidentes e impactos que pueden causar daños dentro de la organización.
2. Se genera una mejora continua en los procesos de análisis y tratamientos de los riesgos.
3. Se genera conciencia sobre la seguridad y da tranquilidad a las partes interesadas.
4. Da una visión completa sobre los riesgos con lo cual se puede generar una planificación estratégica para la toma de decisiones.

Para el análisis y gestión de riesgos existen varias metodologías como lo son OCTAVE, MAGERIT, CRAMM con similitudes, diferencias, las razones por las cuales es importante su aplicación y cuál es el mejor modelo para la toma de decisiones frente a un riesgo inminente dependen una comprensión sólida de las necesidades de la organización y en una evaluación cuidadosa de las características y enfoques de cada metodología.

En su trabajo de titulación (Balcázar, 2020) describe a OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation) como una metodología que se encarga de evaluar y proponer un plan de mitigación de riesgos de seguridad de la información dentro de una organización. Esta metodología persigue dos objetivos en específico:

1. Concientizar a la organización que la seguridad de la información no solo es un asunto técnico.
2. Presentar a la organización cuales son los estándares internacionales que guían la implementación de la seguridad a los aspectos no técnicos.

Según (Bravo, 2018; Guacanés & Vilatuña, 2022; Quilachamín, 2020) la metodología MAGERIT fue desarrollada por el Consejo Superior de Administración del Gobierno de España en 1997 y se encarga de analizar los riesgos de manera sistemática para estimar la magnitud de los riesgos a los que están expuestos una organización. MAGERIT en su tercera versión es compatible y se ha adaptado al cambio e implementación de la norma ISO/IEC 27001 alineando la gestión de riesgos a un marco de trabajo organizacional y persigue los siguientes objetivos:

1. Concientizar a los responsables de las organizaciones sobre la existencia del riesgo y de la necesidad de gestionarlos.
2. Proporcionar un análisis sistemático de los riesgos derivados del uso de las tecnologías de la información y comunicación.
3. Ayudar a las detección oportuna y planificación del tratamiento para mantener los riesgos controlados.
4. Preparar a la Organización para procesos de auditorías, evaluación, certificación o acreditación, según corresponda.

La versión 3 de MAGERIT se encuentra estructurada en dos libros y en una guía técnica:

- **Libro I** – Método.
- **Libro II** – Catálogo de elementos.
- **Libros II** – Guía de Técnicas

En lo expuesto en la guía de MAGERIT hay cinco pasos a seguir como se muestra en la Figura 6 para analizar los riesgos dentro de una organización abarcando diferentes situaciones que se pueden presentar.

Figura 6

Análisis de riesgos

Nota. La figura representa las fases para el análisis de riesgos dentro de una organización.

Para los autores (Guacanés & Vilatuña, 2022) CRAMM (CCTA Risk Analysis and Management Method) es una metodología de análisis de riesgos desarrollada y enfocada a grandes organizaciones, el mantenimiento como la gestión están cargo de la empresa privada Insight Consulting, se compone de tres fases:

1. Establecimiento de los objetivos de seguridad.
2. Evaluación de riesgos.
3. Identificación y selección de contramedidas.

Según (Hinojosa, 2021), en su tesis de "Modelado Funcional de Contenedores Virtuales Docker", muestra que los contenedores virtuales son una gran opción frente al problema de portabilidad, facilitando un desarrollo rápido y ágil de aplicaciones de software de manera fácil y uniforme, independiente del entorno ya sea este un centro de datos, nube pública o privada o incluso una laptop.

Según (Dziurzanski et al., 2020; Ortiz, 2022) los contenedores de software son una tecnología relativamente nueva con su lanzamiento en 2013 cambió la forma de ejecutar y orquestar software, se encuentra disponible para todos los sistemas operativos como se muestra en la Tabla 1. Desarrollado por Golang y parte del proyecto de código abierto Moby, permite crear, empaquetar todo lo necesario para probar e implementar aplicaciones o microservicio rápidamente.

Tabla 1

Sistemas operativos compatibles

Linux	Ubuntu, Debian, CentOS y Fedora, Red Hat Enterprise Linux, Oracle Linux y SUSE Linux Enterprise Server.
Windows	Microsoft Windows 10 (Pro, Enterprise o Education con 64 Bit), Microsoft Azure, Microsoft Windows Server 2016
macOS	macOS Big Sur (11), Monterey (12), Ventura (13)
Amazon	Amazon Web Services (AWS)

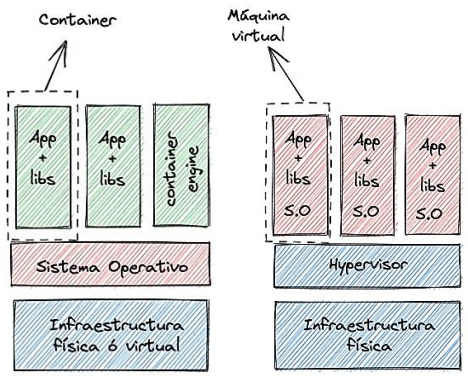
Nota. Esta tabla muestra los diferentes tipos de sistemas operativos con los que son compatibles los contenedores de software.

En sus trabajos (Hinojosa, 2021; López, 2020) muestran una de las principales diferencias entre las máquinas virtuales y los contenedores de software como se muestra

en la Figura 7, que para la virtualización está presente el uso del hipervisor para emular un sistema operativo frente al uso contenedores de software que se ejecutan sobre el mismo sistema operativo anfitrión de forma aislada sin la necesidad de un sistema operativo propio ya que comparten el kernel (núcleo del sistema operativo) lo que los hace más ligero.

Figura 7

Arquitectura de contenedores de software y máquinas virtuales



Nota. La figura muestra la diferencias estructurales entre una máquina virtual y un contenedor de software.

En recopilación de varios autores (Blial & Mamoun, 2017; Elmenreich et al., 2019; Hinojosa, 2021; Kwon & Lee, 2020; You & Sun, 2022) en la Tabla 2 se listan y se describen las ventajas y desventajas de los contenedores de software.

Tabla 2

Ventajas y desventajas contenedores de software

Ventajas	Desventajas
Portátil e independiente de las plataformas.	Se requiere mínimo la versión de Kernel 3.8.
Consta con un repositorio de imágenes**.**	Solo soporta a sistemas operativos Linux de arquitectura de x64.
Puede realizar pruebas de implementación rápidas y continuas.	No cuenta con herramientas de monitoreo de los recursos compartidos.
Posee un alto nivel de utilización de recursos puesto que solo involucran procesos de la aplicación y nada más.	Herramientas limitadas para el monitoreo y la administración de contenedores.
Portable entre ambientes lo que permite replicarlo varias veces.	No posee una interfaz gráfica de usuario (GUI), el usuario debe familiarizarse con la línea de comandos.

Soporta el desarrollo y la arquitectura modernos.	Si un contenedor se encuentra infectado con un software malicioso este puede infectar a la maquina anfitrión.
Son escalables lo que permite tener varias réplicas de un mismo contenedor con el mínimo esfuerzo.	Existen herramientas de software que no son de código abierto
Son seguros al aplicar buenas prácticas.	Requiere tener un conocimiento del sistema operativo subyacente
Automatización de los despliegues de infraestructura.	No son eficientes al momento de almacenar grandes volúmenes de datos.
Trabajan en base a la ISO/CEI JTC 1/SC 38 - Cloud computing and distributed platforms	No proporciona información de las aplicaciones que se encuentran ejecutándose dentro del contenedor.

Nota. Esta tabla lista las ventajas y desventajas de los contenedores de software.

Según la investigación de (Hinojosa, 2021; Javed & Toor, 2021) para el año 2020 existe un crecimiento del 40% en la adopción de uso de contenedores con una tendencia que va en aumento por la facilidad de despliegue y desarrollo como se muestra en la siguiente lista:

1. Un crecimiento del 145% año tras año en el número de descargas en la plataforma Docker Hub.
2. Un 45% en la creación de nuevas cuentas de usuario.
3. Un 40% en la creación de nuevas imágenes.
4. Un 38% en instalaciones de Docker Desktop

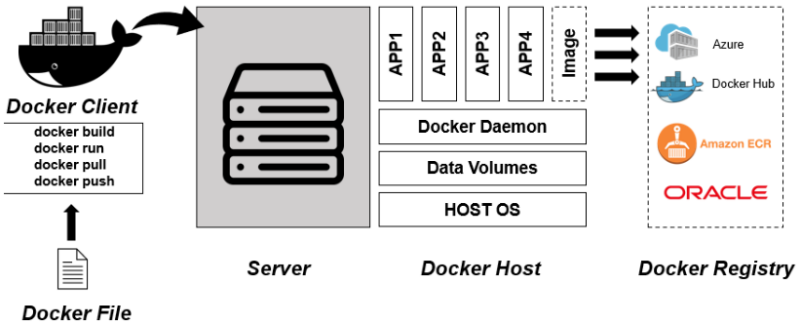
Como lo señalan (Hinojosa, 2021; Martínez, 2022) Docker se presenta como una plataforma que aplica LXC con un kernel (Núcleo del sistema operativo) y una API (Interfaz de programación de aplicaciones) a nivel de aplicación en la cual se pueden combinar distintas tecnologías que van alineadas bajo un único idioma de configuración eliminando por completo la necesidad de mantenimiento y configuración personalizada.

(Kim et al., 2022; Rivadeneira, 2022) señalan que con Docker se puede separar la aplicación de su infraestructura con el fin de que sea más rápida la prueba, entrega y puesta en producción de la aplicación sobre cualquier sistema operativo compatible. Para la construcción de un contenedor Docker se contemplan una serie de elementos que en la Figura 8 se aprecia de manera gráfica y se describen en la siguiente lista:

1. Un Docker File es un archivo de texto configurado para crear una imagen Docker, mediante comandos, se agregan y copian archivos de imágenes, se ejecutan comandos y se exponen los puertos.
2. Docker client crea una nueva imagen mediante un comando de compilación propio de Docker e interactúa con más un daemon o demonio a través de Docker CLI.
3. Docker Daemon se encarga de administrar las solicitudes de la API de Docker y de los objetos de Docker como imágenes, contenedores, redes y volúmenes.
4. Los Data volumes o volúmenes de datos son la parte de datos del contenedor y se inicializan cuando se crea el contenedor.
5. Docker Registry es un repositorio Apache de código abierto que almacena y distribuye imágenes.

Figura 8

Flujo de construcción de un contenedor Docker



Nota. La figura representa los diferentes elementos que intervienen en la construcción de un contenedor Docker. Tomado de (Kim et al., 2022)

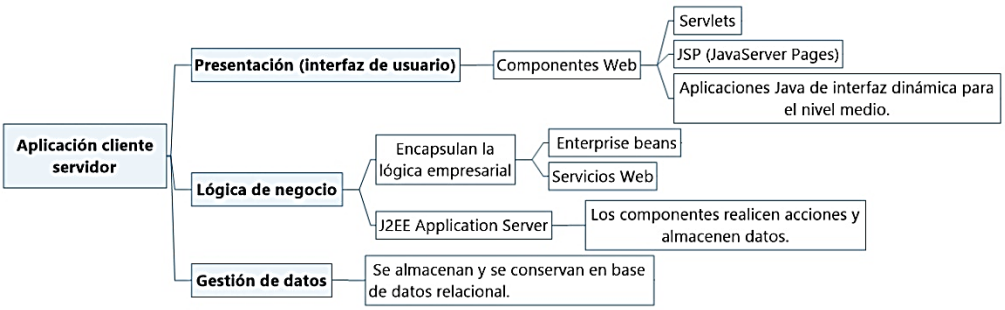
Como lo mencionan (Rosero, 2019; Vergara, 2019), una aplicación web es un sistema informático con interfaces similares a las aplicaciones de escritorio, se crean en respuestas a varias necesidades y procesos dentro de una organización, se puede acceder por medio del internet o una intranet gracias a su accesibilidad por medio de un navegador web, una de las ventajas que presentan es la facilidad de actualización y mantenimiento sin la instalación software en miles de clientes.

Una aplicación cliente servidor consta de tres componentes: presentación (interfaz de usuario), lógica de negocio y la gestión de datos como se muestra en la

Figura 9, cada uno de estos componentes puede estar a nivel de cliente o de servidor

Figura 9

Componentes aplicaciones web



Nota. La figura representa la estructura de una aplicación cliente servidor.

De acuerdo con (Rosero, 2019; Vergara, 2019) un servidor web es un sistema que tiene la característica de ser potente, modular, atender y responder a varias peticiones de los navegadores por medio de los protocolos HTTP o HTTPs siendo este el más seguro, y se encarga de gestionar la disponibilidad de las aplicaciones web a las cuales acceden los clientes, en la Tabla 3 se listan los diferentes tipos de servidores web.

Tabla 3

Servidores de aplicaciones web

Servidor de aplicaciones	Fabricante
JBoss	Red Hat
Oracle Application Server	Oracle
SAP NetWeaver AS Java	SAP
Tomcat EE	Apache Software Foundation
WebLogic	Oracle
WebSphere	IBM

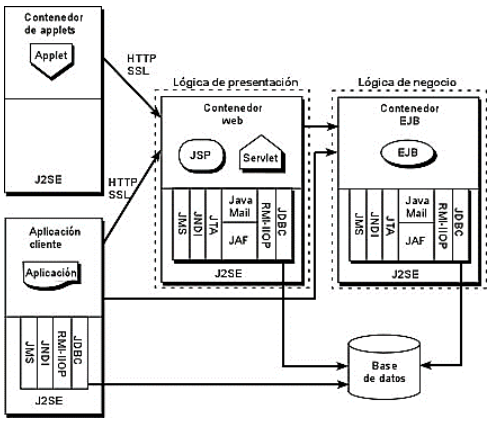
Nota. Esta tabla muestra una lista de servidores de aplicaciones de diferentes fabricantes

La plataforma J2EE "ha sido pensada para escribir aplicaciones distribuidas basadas en componentes", además que una aplicación empresarial se la conoce como aquella que "utiliza concurrentemente más que unos pocos usuarios, así como recursos distribuidos (Bases de datos compartidas entre aplicaciones), delega responsabilidades entre distintos objetos distribuidos y utiliza la tecnología J2EE" (Sarmiento, 2020).

Para los autores (Subrahmanyam et al., 2002) un archivo EAR (Enterprise Application ARchive) se utiliza para empaquetar uno o más módulos J2EE en un único módulo del modo que puedan cargar de clases y desplegarse en servidores de aplicaciones JEE, en la Figura 10 se muestra la arquitectura J2EE en términos de sus contenedores y APIs.

Figura 10

Arquitectura J2EE



Nota. La figura representa la arquitectura de una aplicación J2EE. Tomado de

La arquitectura vista en la Figura 7 consta de cuatro contenedores como lo describen (Subrahmanyam et al., 2002).

1. **Contenedor Web** que alberga los servelts Java y paginas JSP.
2. **Contenedor EJB** que alberga los componentes Enterprise JavaBean.
3. **Contenedor applet** que alberga los applets Java.
4. **Contenedor de aplicación cliente** que alberga las aplicaciones Java estándar.

b) FUNDAMENTACIÓN CIENTIFICA

Operacionalización de variables

La Tabla 4 y Tabla 5 se muestra la operacionalización de variables tanto independiente como dependiente en base a dimensiones, indicadores, ítems y técnicas e instrumentos a aplicar.

Variable independiente

Tabla 4

Variable independiente

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems	Técnicas e Instrumentos
Aplicando la norma ISO/IEC 27001 Para (Valencia, 2021; Villegas, 2019) la norma ISO/IEC 27001 proporciona los requisitos para establecer, implementar, mantener y mejorar un SGSI basado en las dimensiones básicas de la seguridad como la integridad, disponibilidad y confidencialidad de la información en una organización mediante la aplicación de un proceso de gestión de riesgos.	Solución basada en procesos estructurados y normados.	Precio. Tiempo. Nivel de aceptación.	¿Los técnicos implementadores tiene conocimiento sobre la Norma ISO/IEC 27001? ¿Los procesos internos dentro de la organización mantienen los principios de integridad, disponibilidad y confidencialidad de la información? ¿Los técnicos implementadores tienen conocimiento de que son los	**Grupo:** Directivos **Técnica:** Encuestas a los directivos de la organización. **Instrumento:** Cuestionario

Al aplicar la norma ISO/IEC 27001 los autores (De la Cruz & Segura, 2017) recomiendan que "durante la implementación, es necesario la presencia del personal de custodio de la información, durante todo el proceso debido a que son quienes conocen donde y como se encuentra almacenada la información".			activos de información? Durante una implementación ¿Los técnicos implementadores se encuentran presentes?	
Sin aplicar la norma ISO/IEC 27001 (Mendoza & Naranjo, 2020) recomiendan "realizar un levantamiento formal de los controles actuales que se tienen en la organización de manera que se definan procedimientos, responsables, alcance, etc. Para que estos controles no se los realice de forma empírica o por solo la necesidad, sino que sean algo constante y	Soluciones ad hoc	Complejidad. Precio. Tiempo.	¿Dentro de la organización los procesos se encuentran normados o aplican alguna norma internacional? ¿El personal conoce la importancia de la seguridad de la información? Frente a la salida del personal ¿Existen protocolos a seguir con los activos de	**Grupo:** Directivos **Técnica:** Encuestas a los directivos de la organización. **Instrumento:** Cuestionario

de conocimiento de todo el personal”. Según (Villegas, 2019) “la falta de personal oficialmente encargado dentro de la estructura organizacional limita la implementación de SGSI y resta importancia a la seguridad de la información de la institución”.			información que estaban a su cargo?	

Nota. Esta tabla muestra la operacionalización de variable independiente.

Variable dependiente

Tabla 5

Variable dependiente

Conceptualización o Descripción	**Dimensiones**	**Indicadores**	**Ítems**	**Técnicas e Instrumentos**
(Quiñonez Quintero, 2022) señala dentro de sus conclusiones que "los ambientes de pruebas virtualizados permiten diseñar, organizar y experimentar las ventajas e inconvenientes que se pueden presentar en una infraestructura antes de ponerla en equipo físicos y ocasionar eventos adversos con altos tiempos de recuperación, paralización de servicios y pérdida de recursos económicos".	Usabilidad Accesibilidad Disponibilidad Integridad Confidencialidad	Tiempos de instalación, configuración y despliegue.	¿Se han reducido los tiempos de implementación, configuración y despliegue de aplicaciones Java EE?	**Grupo:** Técnicos **Técnica:** Encuestas a los técnicos implementadores. **Instrumento:** Cuestionario

Nota. Esta tabla muestra la operacionalización de variable dependiente

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Tipo de investigación

Experimental: se crearán diferentes casos de prueba a fin de verificar los resultados en cada uno de los escenarios.

Cuantitativa: permitirá el análisis de los datos una vez finalizado los casos de prueba.

Bibliográfica: el fundamento teórico vendrá de tesis, revistas, artículos científicos de bases indexadas y cuya información permitirá elaborar un marco teórico vasto.

De Campo: se recolectará la información primaria por medio de encuesta y/o entrevista.

3.2. Población o muestra

Para la elección de la población del proyecto se tomarán en consideración dos escenarios, el primero utilizando contenedores Docker y el segundo sin la utilización de contenedores Docker, siendo el objeto de estudio si se mejora los tiempos de instalación, configuración del entorno de trabajo y el despliegue de la aplicación web Java EE.
En virtud de la población a ser investigada es pequeña se trabajará con la totalidad del universo sin que sea necesario sacar muestras representativas.

3.3. Prueba de Hipótesis - pregunta científica – idea a defender

¿Mediante la utilización de contenedores de software se mejora la automatización del despliegue de aplicaciones web Java EE en servidores Linux de X64, basado en la norma ISO/IEC 27001:2018?

3.4. Recolección de información

En primera instancia se recopilará la mayor cantidad de información basados en documentación oficial, trabajos de investigación, artículos científicos, tesis del repositorio Universidad Técnica de Ambato y de otras universidades que vayan alineados al tema propuesto.

Se realizará una entrevista con los directivos de la empresa para ver la problemática existente y si el tema de investigación ayudará a solucionar dicho problema. Para la recolección de información se utilizará una encuesta inicial para saber el nivel de conocimiento y si en algún momento se ha presentado una solución a corto, mediano o largo plazo, y como punto final la tabulación y posterior interpretación de los resultados obtenidos de los diferentes casos de prueba.

3.5. Procesamiento de la información y análisis estadístico:

Diseño de prueba previa y posterior: Comprobar si los grupos son diferentes antes del comienzo de la manipulación y del efecto de la manipulación (Explorable, 2022).\

Para un mayor control en el manejo y análisis de datos se realizaron en orden cronológico los siguientes pasos:

1. Decidir qué información buscar y sitios de fuentes confiables.
2. Dar un peso en específico a cada una de las fuentes de información según el contenido que aporta en la investigación.
3. Recolectar la información y generar un repositorio base.
4. Analizar la información recolectada en base a los lineamientos del tema de investigación planteado.
5. Exponer y explicar los resultados obtenidos.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1. Selección del contenedor de software

Para (Rivadeneira, 2022) dentro del análisis de herramientas DevOps para contenedores en base a la comparativa entre Docker, LXC, Podman, determina que Docker es la mejor opción por las siguientes razones:

1. Docker es la herramienta más usada por proveedores en la nube.
2. LXC, Podman carecen de un repositorio digital de imágenes.
3. LXC, Podman se encuentran enfocados en trabajar con VM.
4. Docker es una herramienta de DevOps más usada para trabajar con contenedores en la nube.

(Pacheco, 2018) en su trabajo de titulación destaca que Docker dentro de las estadísticas de utilización ha logrado lo siguiente:

1. 2/3 de las empresas que utilizan Docker en los ambientes de pruebas y desarrollo y con un tiempo estimando de 30 días lo utilizaron en producción.
2. Con una tasa de crecimiento del 35% en la adopción de Docker.
3. Diferentes lenguajes de programación y frameworks de desarrollo utilizan contenedores Docker.

(Montalvo Ochoa, 2020) concluye que Docker como contenedor de software ha demostrado agilizar procesos de despliegue de aplicaciones y servicios en entornos de prueba y/producción, además de la posibilidad de crear aplicaciones portables que se pueden ejecutar en otro equipo o entorno de trabajo que se encuentre instalado Docker.

4.2. Selección del servidor de aplicación

Como lo mencionan los autores (L. Fernández, 2020; Subrahmanyam et al., 2002), el hardware y la arquitectura del sistema son también importantes a la hora de decidir que servidor de aplicación es más adecuado para un determinado proyecto, que generalmente está direccionado a trabajar con sistemas de diferentes magnitudes y que estén relacionados en un entorno Web.

“Los servidores de aplicación son la principal representación de productos para especificaciones J2EE; proporciona contenedores Web y contenedores EJB que resultan claves para cualquier implementación J2EE” (Subrahmanyam et al., 2002).

Para los autores (Cortez, 2020; L. Fernández, 2020; Guayasamin, 2022) Wildfly es un servidor de aplicaciones de código abierto multiplataforma que evoluciona a partir de Jboss, al estar basado en JAVA lo hace compatible con los sistemas operativos que tengan instalado JVM (Java Virtual Machine) y entre sus características principales se destaca:

1. Rápida puesta en marcha.
2. Fácil configuración.
3. Modular.
4. Basado en proyectos Open Source.
5. Los procesos de arrancan altamente optimizados.
6. Posee subsistemas que se pueden agregar o eliminar según sea necesario.
7. Soporta implementaciones de los últimos estándares empresariales como Java EE8.

4.3. Selección del gestor de bases de datos

En sus trabajos (Jaramillo & Puchaicela, 2022; Ruano, 2020), explican que PostgreSQL en un gestor de bases de datos Open Source de alto nivel orientado a objetos, conocido por su alto grado de confiabilidad, integridad y precisión de datos, maneja una gran variedad de sentencias SQL además de consultas SQL complejas, Triggers, Views, etc., y entre las ventajas que posee se destacan:

1. No hay un costo de licencia.
2. Cumple con los estándares SQL.
3. Escalable y de alto rendimiento.
4. Fiable, PostgreSQL es ACID lo que significa que puede tolerar fallos de hardware.
5. Una comunidad activa que permite encontrar y resolver problemas en el menor tiempo posible.
6. Permite a los desarrolladores ejecutar tareas como: Describir objetos de bases de datos, exportar e importar datos, backups y restore de datos de datos.

4.4. Selección del gestor de monitoreo

Al trabajar con servidores es necesario monitorear cada una de las tareas que se encuentran ejecutando en base a diferentes métricas como lo es el consumo de CPU, RAM, disco duro, red, entre otros.

Una de las herramientas que viene integrada en los servidores con base Linux x64 es htop que es un visor estándar de procesos interactivo en texto plano que permite monitorear a través de un terminal de acceso, la limitante que presenta esta herramienta es que muestra los procesos que se encuentran ejecutando en ese momento y no tiene un registro histórico, la terminal siempre debe estar abierta lo cual no permite un monitoreo centralizado.

Para el caso de estudio se seleccionó la herramienta open source Netdata que permite visualizar diferentes métricas en tiempo real de los sistemas operativos, servidores, contenedores, hardware y aplicaciones que se ejecutan en una variedad de entornos, incluidos locales, en la nube e híbridos.

4.5. Tiempos de instalación, configuración y despliegue

Para determinar los tiempos de instalación, configuración y despliegue en cada uno de los escenarios, el primero utilizando contenedores Docker y el segundo sin la utilización de contenedores Docker, para ello se tomará en cuenta los siguientes aspectos:

1. Hardware base, un procesador AMD Opteron Octa-Core, 8x2.4 Turbo 2,40 GHz con16GB en RAM y 500 GB HDD
2. Conexión de internet a una velocidad de Internet a100 Mbps a través de fibra óptica.
3. Sistema operativo Ubuntu-22.04.2-live-server-amd64.

La Tabla 6 y Tabla 7 se muestran los tiempos de instalación, configuración y despliegue en los escenarios propuestos el primero usando contenedores Docker y el segundo sin el uso de contenedores Docker.

1. **Entorno de pruebas con Docker**

Tabla 6

Tiempos de implementación con Docker

Servicio/Aplicativo	Tiempo

Instalación Ubuntu Server 22.04.2	13 min
Instalación Docker - Docker compose	3 min
Configuración DockerFile	5 min
Configuración docker-compose	5 min
Despliegue Postgres – Pgadmin4 – Wildfly - JDK	4 min
Restauración de bases de datos	2 min
Despliegue aplicativo Java EE	1min 11 seg
Total	33 min 11 seg

Nota. Esta tabla muestra los tiempos de instalación y configuración de un entorno con Docker.

2. Entorno de pruebas sin Docker

Tabla 7

Tiempos de implementación sin Docker

Servicio/Aplicativo	**Tiempo**
Instalación Ubuntu Server 22.04.2	33 min
Instalación de actualizaciones	3 min
Instalación y configuración JDK	5 min
Descarga e instalación Postgres	3 min
Descarga e instalación PgAdmin	4 min
Restauración de bases de datos	4 min
Descarga Wildfly	2 min
Configuración y despliegue Wildfly	15 min
Despliegue aplicativo Java EE	3 min
Total	1 hora 12 min

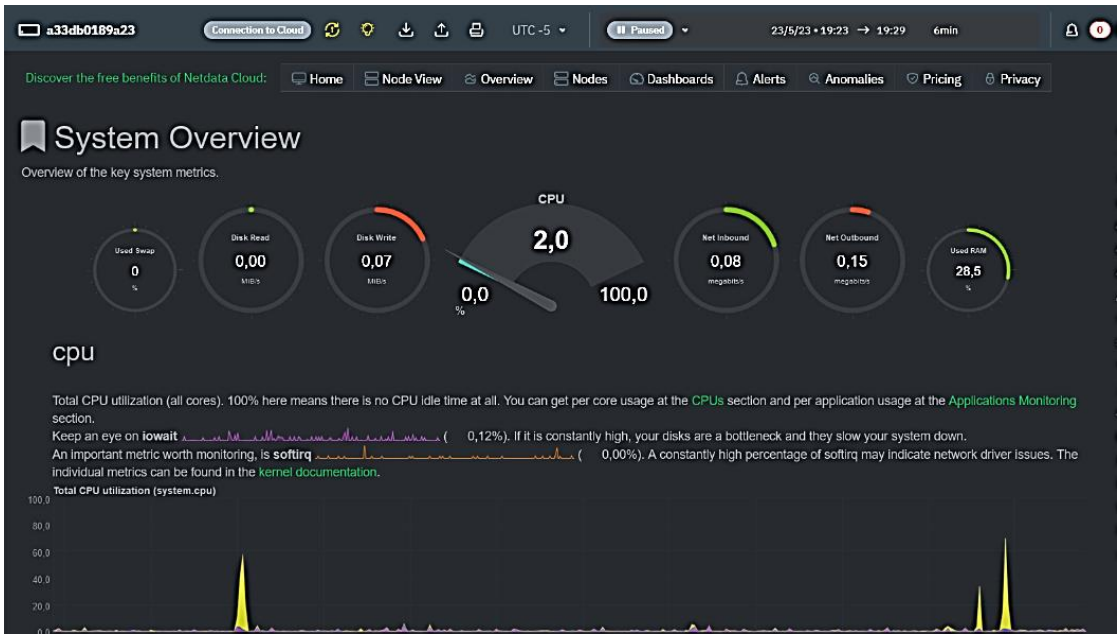
Nota. Esta tabla muestra los tiempos de instalación y configuración de un entorno sin Docker.

Como se muestra en Tabla 6 y Tabla 7 cada uno de los ítems presentados tiene un tiempo estimado de instalación, configuración y/o despliegue, a pesar de trabajar bajo una misma arquitectura de servidor, en comparativa entre un entorno y otro, el resultado final muestra que entorno de pruebas con Docker el tiempo es de 33 min 11 seg frente a la 1 hora 12 min del entorno de pruebas sin Docker , lo que muestra una diferencia de 38 min 49 seg que para una configuración, implementación y despliegue es aceptable.

En la Figura 11 y Figura 12 se muestra un dashboard en donde se muestra una descripción general de las métricas clave del sistema, lo cual permitirá monitorear de mejor manera el consumo de recursos para los dos escenarios expuestos.

Figura 11

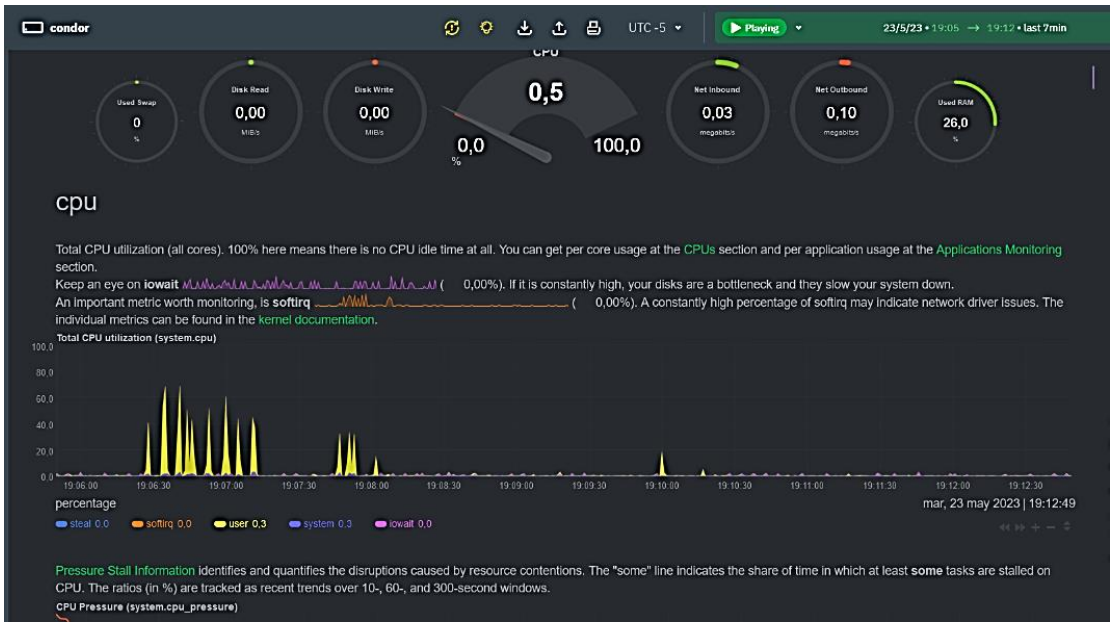
Consumo de recursos CPU, RAM y almacenamiento usando Docker



Nota. La figura muestra un dashboard en Netdata con Docker

Figura 12

Consumo de recursos CPU, RAM y almacenamiento sin usar Docker



Nota. La figura muestra un dashboard Netdata sin Docker

4.6. Selección de la metodología de gestión de riesgo

Cabe destacar que como base y guía se usó la norma ISO/IEC 27001:2013 la cual recibió una actualización el 25 de octubre de 2022 en la que se destaca los siguientes cambios:

1. Paso de ser “ISO/IEC 27001:2013, Tecnología de información-técnicas de seguridad-sistemas de gestión de seguridad de la información-Requerimientos” a “ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad”.
2. Cambios en el Anexo A, se redujo en número de controles de 114 a 93.
3. Actualizaciones en las cláusulas obligatorias de 4 a la 10.
4. Los 93 controles pasaron de estar distribuidos de 14 a 4 secciones.
5. Dentro del Anexo A, se añadieron 11 nuevos controles.
6. Las empresas que ya se encuentran certificadas en la norma ISO/IEC 27001:2013 pueden aplicar a la nueva norma, pueden hacer esa transición hasta el 31 de octubre del 2025.

Para (Valencia, 2021) la norma ISO/IEC 27000:2018 muestra una visión general, los principales términos que se utilizan para la implementación de un SGSI, los cuales se requieren

para evitar ambigüedades y en la cual se delimitan los términos y las definiciones que se utilizan en las diferentes normas de la familia ISO/IEC 27000.

(Guacanés & Vilatuña, 2022) describen la relación que existe entre MAGERIT y la ISO/IEC 27001 en la cual muestra como un sistema de seguridad requiere de una metodología para una posterior evaluación de la información de una manera consistente y que puede ser empleada en todas las etapas de la gestión de riesgos.

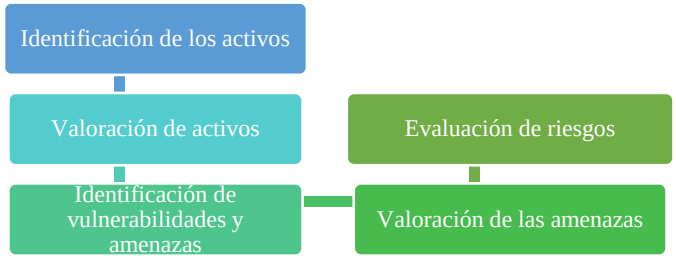
En su trabajo de titulación (Mendoza & Naranjo, 2020) describe a MAGERIT como una metodología de alto nivel que cubre todos los elementos de TI hardware, software, bases de datos, redes y comunicaciones, recursos humanos y servicios con la finalidad de que las empresas tomen buenas decisiones.

"La versión 3.0 es compatible con las normas ISO/IEC 27001:2013 alineando la gestión de riesgos a un marco de trabajo de la organización" (Bravo, 2018).
Dentro de las ventajas que presenta MAGERIT se destacan:

1. Permite identificar las amenazas y vulnerabilidades.
2. Es una metodología fácil de implementar dado que es una guía completa y detallada.
3. Se puede tomar como punto de partida para mejorar los sistemas de gestión de información y posterior certificación.

Figura 13

Metodología de análisis y gestión de riesgos



Nota. La figura representa un flujograma de la metodología de análisis y gestión de riesgos.

Como base para la aplicación de la metodología MAGERIT, se tomó de ejemplo la propuesta del autor (Camacho, 2021) y se armó un flujograma que se muestra en la Figura 13 para el caso de estudio.

4.7. Estado inicial del negocio

En la Tabla 8 se muestra el resultado del estado inicial del negocio en base a una serie de preguntas que abarcan diferentes áreas dentro de la organización.

Tabla 8

Resultado de la entrevista

Preguntas	Respuestas
POLÍTICAS DE SEGURIDAD:	
¿Existen documento(s) de políticas de seguridad de Sistema de Información?	NO
¿Existe normativa relativa a la seguridad del Sistema de Información?	NO
¿Existen procedimientos relativos a la seguridad de Sistema de Información?	NO
¿Existe un responsable de las políticas, normas y procedimientos?	NO
¿Existen mecanismos para la comunicación a los usuarios de las normas?	NO
¿Existen controles regulares para verificar la efectividad de las políticas?	NO
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN:	
¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?	NO
¿Existe un responsable encargado de evaluar la adquisición y cambios de Sistema de Información?	NO
¿Participan la Dirección y las áreas de la Organización en temas de seguridad?	NO
¿Existen condiciones contractuales de seguridad con terceros y outsourcing?	NO
¿Existen criterios de seguridad en el manejo de terceras partes?	NO
¿Existen programas de formación en seguridad para los empleados, clientes y terceros?	NO
¿Existe un acuerdo de confidencialidad de la información que se accede?	NO
¿Se revisa la organización de la seguridad de forma periódica por una empresa externa?	NO
GESTIÓN DE ACTIVOS:	
¿Existen un inventario de activos actualizado?	NO

¿El Inventario contiene activos de datos, software, equipos y servicios?	NO
¿Se dispone de una clasificación de la información según la criticidad de la misma?	NO
¿Existe un responsable de los activos?	NO
¿Existen procedimientos para clasificar la información?	NO
¿Existen procedimientos de etiquetado de la información?	NO

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS:

¿Se tienen definidas responsabilidades y roles de seguridad?	NO
¿Se tiene en cuenta la seguridad en la selección y baja del personal?	NO
¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?	NO
¿Se imparte la formación adecuada de seguridad y tratamiento de activos?	NO
¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?	NO
¿Se recogen los datos de los incidentes de forma detallada?	NO
¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?	NO
¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?	NO
¿Existe un proceso disciplinario de la seguridad de la información?	NO

SEGURIDAD FÍSICA Y AMBIENTAL:

¿Existe perímetro de seguridad física (una pared, puerta con llave)?	SI
¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado?	NO
¿Un área segura ha de estar cerrada, aislada y protegida de eventos naturales?	NO
¿En las áreas seguras existen controles adicionales al personal propio y ajeno?	NO
¿Las áreas de carga y expedición están aisladas de las áreas de SI?	SI
¿La ubicación de los equipos está de tal manera para minimizar accesos innecesarios?	NO
¿Existen protecciones frente a fallos en la alimentación eléctrica?	NO
¿Existe seguridad en el cableado frente a daños e intercepciones?	NO
¿Se asegura la disponibilidad e integridad de todos los equipos?	NO

¿Existe algún tipo de seguridad para los equipos retirados o ubicados en el exterior?	NO
¿Se incluye la seguridad en equipos móviles?	NO

SEGURIDAD EN LAS TELECOMUNICACIONES:

¿Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados?	NO
¿Están establecidas responsabilidades para controlar los cambios en equipos?	NO
¿Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?	NO
¿Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas?	NO
¿Existe una separación de los entornos de desarrollo y producción?	SI
¿Existen contratistas externos para la gestión de los Sistemas de Información?	NO
¿Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento?	NO
¿Existen criterios de aceptación de nuevos Sistema de Información, incluyendo actualizaciones y nuevas versiones?	SI
¿Controles contra software maligno?	NO
¿Realizar copias de backup de la información esencial para el negocio?	SI
¿Existen logs para las actividades realizadas por los operadores y administradores?	NO
¿Existen logs de los fallos detectados?	SI
¿Existen rastro de auditoría?	SI
¿Existe algún control en las redes?	NO
¿Se ha establecidos controles para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)?	NO
¿Eliminación de los medios informáticos?	NO
¿Existe seguridad de la documentación de los Sistemas?	NO
¿Existen acuerdos para intercambio de información y software?	NO
¿Existen medidas de seguridad de los medios en el tránsito?	NO
¿Existen medidas de seguridad en el comercio electrónico?	NO

¿Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada?	NO
¿Existen medidas de seguridad en las transacciones en línea?	NO
¿Se monitorean las actividades relacionadas a la seguridad?	NO

CONTROL DE ACCESOS:

¿Existe una política de control de accesos?	NO
¿Existe un procedimiento formal de registro y baja de accesos?	SI
¿Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario?	SI
¿Existe una gestión de los password de usuarios?	NO
¿Existe una revisión de los derechos de acceso de los usuarios?	SI
¿Existe el uso del password?	SI
¿Se protege el acceso de los equipos desatendidos?	NO
¿Existen políticas de limpieza en el puesto de trabajo?	NO
¿Existe una política de uso de los servicios de red?	NO
¿Se asegura la ruta (path) desde el terminal al servicio?	NO
¿Existe una autenticación de usuarios en conexiones externas?	SI
¿Existe una autenticación de los nodos?	NO
¿Existe un control de la conexión de redes?	NO
¿Existe un control del routing de las redes?	NO
¿Existe una identificación única de usuario y una automática de terminales?	NO
¿Existen procedimientos de log-on al terminal?	NO
¿Se ha incorporado medidas de seguridad a la computación móvil?	NO
¿Está controlado el teletrabajo por la organización?	NO

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS:

¿Se asegura que la seguridad está implantada en los Sistemas de Información?	SI
¿Existe seguridad en las aplicaciones?	SI
¿Existen controles criptográficos?	SI
¿Existe seguridad en los ficheros de los sistemas?	NO
¿Existe seguridad en los procesos de desarrollo, testing y soporte?	NO
¿Existen controles de seguridad para los resultados de los sistemas?	NO
¿Existe la gestión de los cambios en los Sistemas Operativos?	NO

¿Se controlan las vulnerabilidades de los equipos?	NO

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN:

¿Se comunican los eventos de seguridad?	SI
¿Se comunican las debilidades de seguridad?	NO
¿Existe definidas las responsabilidades antes un incidente?	SI
¿Existe un procedimiento formal de respuesta?	NO
¿Existe la gestión de incidentes?	NO

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO:

¿Existen procesos para la gestión de la continuidad?	NO
¿Existe un plan de continuidad del negocio y análisis de impacto?	NO
¿Existe un diseño, redacción e implantación de planes de continuidad?	NO
¿Existe un marco de planificación para la continuidad del negocio?	NO
¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?	NO
CUMPLIMIENTO:	
¿Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas?	NO
¿Existe el resguardo de la propiedad intelectual?	SI
¿Existe el resguardo de los registros de la organización?	NO
¿Existe una revisión de la política de seguridad y de la conformidad técnica?	NO
¿Existen consideraciones sobre las auditorías de los sistemas?	NO

Nota. Esta tabla muestra el resultado de la entrevista del estado inicial del negocio.

4.8. Evaluación de riesgos

1. Identificación de los activos

Para la identificación de los activos se realizará el levantamiento inicial de todos los activos involucrados en el desarrollo del trabajo de investigación, en base al formato

que se muestra en la Tabla 9, en el Anexo III se encuentra más a detalle todo el inventario realizado.

Tabla 9

Identificación de los activos

Código	Tipo	Equipo	Características					Ubicación	Responsable
			Marca	Modelo	Procesador	Memoria	S.O.		
AHW	[pc]	Laptop	Toshiba	S55	i7-4700MQ	16 GB	Ubuntu	Área de desarrollo	Fernando Moya

Nota. Esta tabla muestra la matriz de identificación de activos.

1.1. Clasificación de activos

Para la clasificación de los activos se tomó en cuenta al Libro II – Catálogo de Elementos de MAGERIT – versión 3.0 como se muestra en la Tabla 10 (Amutio et al., 2012).

Tabla 10

Clasificación de activos

Tipo	Descripción	Activos
Hardware [AHW]	Todos los equipos físicos con los que trabaja y cuenta la organización.	• Laptops • Servidores Físicos – Virtualizados • Router
Software [ASW]	Todos los programas de software libre y software de paga, desarrollos propios con los que trabaja la organización.	• Sistema Operativo Ubuntu • Sistema Operativo Windows

		• Sistema Administrativo - Financiero
Datos/Información [AD]	Es toda la información con la cuenta la organización esta sea física, digital o almacenada en una base de datos.	• Bases de datos • Código fuente • Diagrama de red • Backups
Personal [AP]	Todo el personal involucrado dentro de la organización	• Personal administrativo, técnico.
Soporte de información [AMedia]	Todos los dispositivos físicos que almacenan información a corto, mediana y largo plazo.	• Discos duros externos • Memorias USB
Equipos auxiliares [AAUX]	Dispositivos que dan soporte a equipos e infraestructura.	• Reguladores de voltaje • Disipadores de calor

Nota. Esta tabla muestra la categorización, descripción y nomenclatura de activos.

2. Valoración de activos

La valoración de activos permite asignar un valor al o los activos ya sea este cuantitativo o cualitativo y alinearlo con las dimensiones propuesta por Magerit como lo es la **confidencialidad [C]**, **integridad [I]**, **disponibilidad [D]**, tomando en cuenta que "la valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión" (Amutio et al., 2012).

2.1. Criterios de valoración

Para la valoración de los activos se tomo como base la escala propuesta en el libro II – Catálogo de Elementos de MAGERIT – versión 3.0 como se muestra en la Tabla 11 (Amutio et al., 2012, p. 19), siguiendo las siguientes recomendaciones:

- Utilizar una escala en común a usar para todas las dimensiones.
- Usar una escala logarítmica, centrada en diferencias relativas de valor.
- Usar un criterio homogéneo para comparar los análisis que se han realizado por separado.

Tabla 11

Criterios de valoración

Valor	**Criterios**	
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Nota. Esta tabla muestra los Criterios de valoración de activos

Con lo expuesto en la Tabla 11 en conjunto con las dimensiones de valoración (confidencialidad, integridad, disponibilidad), se procedió a valorar los activos de la organización y a sacar un promedio de las dimensiones antes expuestas.

En la Tabla 12 se muestra un ejemplo de valoración de activos, en el Anexo IV se encuentra más a detalle toda la valoración realizada.

Tabla 12

Valoración de activos

Activo	Ubicación	Valoración			Promedio
		[C]	[I]	[D]	
AHW_01	Área de desarrollo	4	8	8	6.66

Nota. Esta tabla muestra la valoración de activos en base a las dimensiones (confidencialidad, integridad, disponibilidad).

3. Identificación de vulnerabilidades y amenazas

Para la identificación de vulnerabilidades y amenazas se tomó como base la lista de amenazas que se describen en el libro II – Catálogo de Elementos de MAGERIT – versión 3.0, más la clasificación de activos de la Tabla 10.

En la Tabla 13 se muestra un ejemplo de identificación de vulnerabilidades y amenazas de activos, en el Anexo V se encuentra más a detalle toda la identificación realizada.

Tabla 13

Identificación de vulnerabilidades y amenazas

Activo	Tipo	Vulnerabilidades	Amenazas	Dimensiones
Hardware [AHW]	[pc]	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	Disponibilidad

Nota. Esta tabla muestra la identificación de vulnerabilidades y amenazas que pueden afectar a los activos de la organización.

4. Valoración de las amenazas

Identificadas las vulnerabilidades y amenazas a las cuales pueden estar expuestos los activos de la organización se procedió a crear una escala de valoración para la degradación y probabilidad de ocurrencia, como se muestra en la Tabla 14.

Tabla 14

Criterios de valoración de las amenazas

Valor	Degradación	Probabilidad de ocurrencia
10	Extremo	Sucede a diario.
9	Muy alto	Sucede varias veces a la semana.
6 – 8	Alto	Sucede una vez al mes.
3 – 5	Medio	Sucede una vez al año.
1 – 2	Bajo	Sucede muy rara vez.
0	Despreciable	Irrelevante a efectos prácticos.

Nota. Esta tabla muestra los criterios de valoración de las amenazas por degradación y probabilidad de ocurrencia.

Con la escala de valoración de las amenazas por degradación y probabilidad de ocurrencia, se procedió a valorar las vulnerabilidades y amenazas en conjunto con la justificación.

En la Tabla 15 se muestra un ejemplo de la valoración de vulnerabilidades y amenazas de activos, en el Anexo VI se encuentra más a detalle toda la identificación realizada.

Tabla 15

Evaluación de vulnerabilidades y amenazas por degradación y probabilidad de ocurrencia.

Activo	Vulnerabilidad	Amenaza	Degradación	Probabilidad de ocurrencia	Justificación
AHW_01	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	2	3	Fallas en las instalaciones eléctricas.

Nota. Esta tabla muestra la valoración de vulnerabilidades y amenazas por degradación y probabilidad de ocurrencia.

5. Evaluación de riesgos

En base a la información recopilada desde la identificación de los activos hasta la valoración de las amenazas el procedió a calcular el riesgo por impacto y probabilidad de ocurrencia.

5.1. Impacto

“Es la medida de daño sobre el activo derivado de la materialización de una amenaza, o cambio adverso importante en el nivel de los objetivos de negocio logrados”(Villegas, 2019), aplicando diferentes criterios de valoración como se muestra en la Tabla 16.

Tabla 16

Criterios de valoración del impacto

Valor	Criterio	Descripción
10	Extremo [E]	Cuando la amenaza se ha materializado y causa daños irreparables dentro de la organización.
9	Muy alto [MA]	Cuando la amenaza se ha materializado y causa daños que la organización puede controlar en un periodo largo de tiempo.
6 – 8	Alto[A]	Cuando la amenaza se ha materializado y causa daños que la organización puede controlar en un periodo significativo de tiempo.
3 – 5	Medio[M]	Cuando la amenaza se ha materializado y causa daños fáciles de controlar en muy poco tiempo.
1 – 2	Bajo[B]	Cuando la amenaza se ha materializado y los daños que causa no afectan al normal funcionamiento de la organización.
0	Despreciable [D]	Cuando la amenaza se ha materializado, pero no afecta en absoluto al funcionamiento de la organización.

Nota. Esta tabla muestra la valoración del impacto (0 - Despreciable a 10 - Extremo)

Con la escala de valoración de la Tabla 16, se procedió a valorar el impacto y la magnitud del impacto, en la Tabla 17 muestra un ejemplo de la valoración del impacto de activos, en el Anexo VII se encuentra más a detalle toda la identificación realizada.

Tabla 17

Valoración y magnitud del impacto

Activo	Vulnerabilidad	Amenaza	Valoración impacto				Magnitud del impacto			
			[C]	[I]	[D]	Prom	[C]	[I]	[D]	Prom
AHW_01	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	2	5	5	4	[B]	[M]	[M]	[M]

Nota. Esta tabla muestra la valoración y magnitud del impacto en base a las dimensiones (confidencialidad, integridad, disponibilidad).

5.2. Probabilidad de ocurrencia

En la Tabla 18 se muestra los criterios para la degradación y probabilidad de ocurrencia en base la escala propuesta en el libro II – Catálogo de Elementos de MAGERIT – versión 3.0.

Tabla 18

Criterios de valoración de probabilidad de ocurrencia

Valor	Degradación	Probabilidad de ocurrencia
10	Extremo [E]	Sucede a diario.
9	Muy alto [MA]	Sucede varias veces a la semana.
6 – 8	Alto[A]	Sucede una vez al mes.
3 – 5	Medio[M]	Sucede una vez al año.
1 – 2	Bajo[B]	Sucede muy rara vez.
0	Despreciable [D]	Irrelevante a efectos prácticos.

Nota. Esta tabla muestra la valoración del riesgo por degradación y probabilidad de ocurrencia

En la Tabla 19 se muestra un ejemplo de la valoración la degradación y probabilidad de activos, en el Anexo VIII se encuentra más a detalle toda la identificación realizada.

Tabla 19

Valoración del riesgo por degradación y probabilidad de impacto

Activo	Vulnerabilidad		Valoración	Magnitud

		Amenaza	Degradación	Probabilidad	Total	Probabilidad	Degradación	Probabilidad	Probabilidad de ocurrencia
AHW_01	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	3	2	5	2	[M]	[B]	[B]

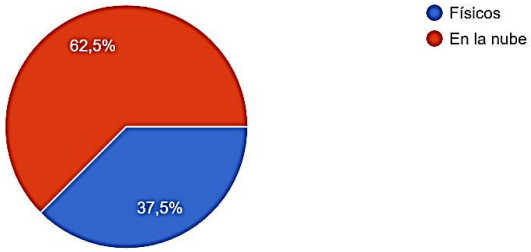
Nota. Esta tabla muestra la valoración y magnitud del riesgo por degradación y probabilidad de ocurrencia.

La siguiente encuesta se aplicó a los directivos del área de TIC de diferentes organizaciones con el propósito de conocer sus diferentes puntos de vista sobre los contenedores de software y la norma ISO/IEC 27001.

1. **¿Qué tipo de servidores utiliza la organización?**

Figura 14

Primera pregunta



Nota. La figura muestra el resultado de la primera pregunta.

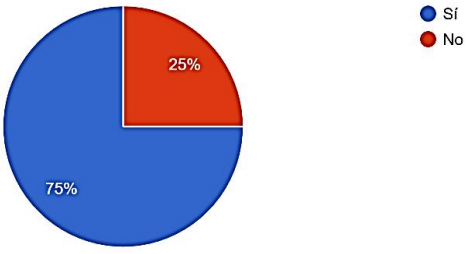
Análisis e interpretación

Del total de encuestados, el 37.5% no trabajan con servidores en la nube, y un porcentaje importante del 62.5% sigue trabajando con servidores en la nube. Se determina que, las organizaciones tienen la tendencia a utilizar servidores en la nube como se observa en la Figura 14.

2. **¿Conoce usted sobre la tecnología de contenedores de software?**

Figura 15

Segunda pregunta



Nota. La figura muestra el resultado de la segunda pregunta.

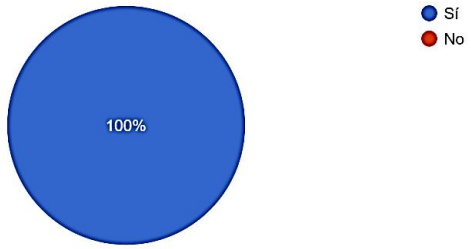
Análisis e interpretación

Del total de encuestados, el 75% conoce sobre la tecnología de Docker, y un 25% no tiene conocimiento. Se determina que, existe conocimiento previo sobre la tecnología como se observa en la Figura 15.

3. **Piensa usted que la virtualización de servidores ayudaría a mejorar la infraestructura de la organización.**

Figura 16

Tercera pregunta



Nota. La figura muestra el resultado de la tercera pregunta.

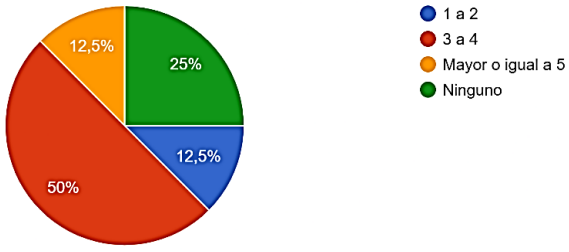
Análisis e interpretación

Del total de encuestados, el 100% como se muestra en la Figura 16 piensa que la virtualización de servidores ayudaría a mejorar la infraestructura dentro de una organización. Se determina que, la tendencia de migrar servidores físicos a la nube va en crecimiento.

4. **¿Con cuántos servidores virtualizados se encuentra trabajando en la actualidad?**

Figura 17

Cuarta pregunta



Nota. La figura muestra el resultado de la cuarta pregunta.

Análisis e interpretación

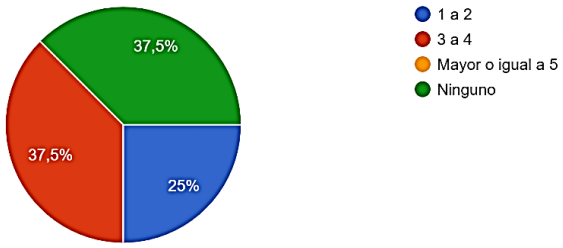
Del total de encuestados como se muestra en la Figura 17, el 50% trabaja entre 3 a 4 servidores en virtualizados, un 12.5 mayor o igual a 5, un 12.5% de 1 a 2 y un 25% no trabaja con ninguno. Se determina que, las organizaciones en su mayoría trabajan en

la nube dependiente de la inversión que realicen y una minoría trabaja con servidores físicos.

5. **¿Para trabajar en ambientes de pruebas ¿con cuántos servidores cuenta?**

Figura 18

Quinta pregunta



Nota. La figura muestra el resultado de la quinta pregunta.

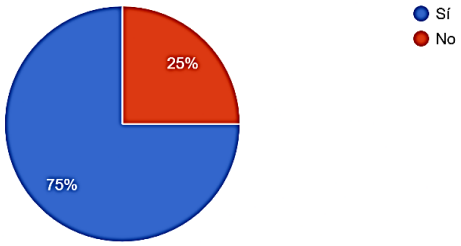
Análisis e interpretación

Del total de encuestados, el 37.5% no trabaja con ambientes de pruebas, un 37.5% entre 3 a 4 y un 25% de 1 a 2 como se observa em la Figura 18. Se determina que, las organizaciones poseen ambientes de pruebas mientras que otras no los tienen.

6. **Los ambientes de pruebas con los que trabaja la empresa utilizan sistemas de virtualización.**

Figura 19

Sexta pregunta



Nota. La figura muestra el resultado de la sexta pregunta.

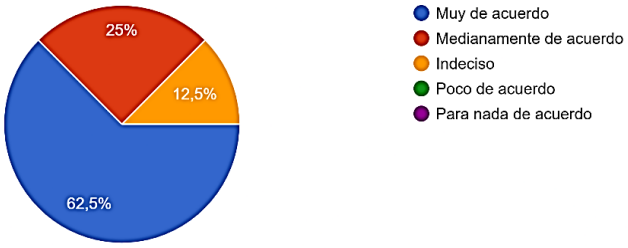
Análisis e interpretación

Del total de encuestados, el 75% sus ambientes de pruebas trabajan con sistemas virtualización mientras que un 25% no. Se determina que en las organizaciones los ambientes de pruebas se encuentran virtualizados y otros siguen siendo en servidores físicos tal como se observa en la Figura 19.

7. **¿Cree usted que los contenedores de software ayudan a mejorar el trabajo de infraestructura dentro de una consultora?**

Figura 20

Séptima pregunta



Nota. La figura muestra el resultado de la séptima pregunta.

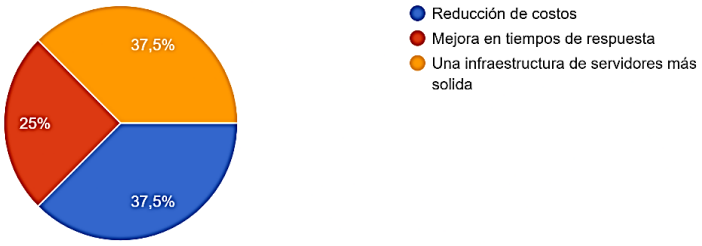
Análisis e interpretación

Del total de encuestados, el 62.5% está muy de acuerdo en que los contenedores de software mejoran el trabajo de infraestructura, un 12.5 se encuentra indeciso y un 25% mediamente de acuerdo. Se determina que, dentro de una organización la idea de mejora en infraestructura está presente como se muestra en la Figura 20.

8. **¿Qué beneficio a futuro cree usted que aportaría el uso de contenedores de software dentro de la organización?**

Figura 21

Octava pregunta



Nota. Resultado de la octava pregunta.

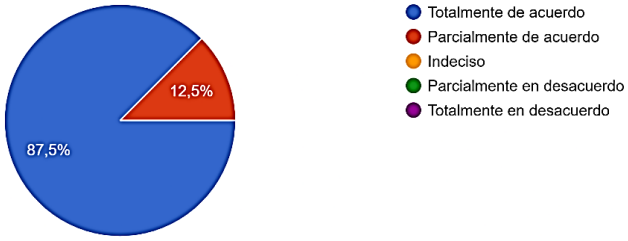
Análisis e interpretación

Del total de encuestados, el 37.5% cree que el uso de contenedores software reducirá costos, un 25% cree que el uso de contenedores software mejora los tiempos de respuesta y un 37.5% cree que se tendrá una infraestructura de servidore más sólida como se muestra en la Figura 21. Se determina que, las opiniones son variadas, pero con un único objetivo que es una mejora continua.

9. **Si se presenta una alternativa de solución en la cual se aplique Docker como contenedor de software para mejorar el trabajo en infraestructura de servidores, estaría dispuesto a implementar dentro de la organización.**

Figura 22

Novena pregunta



Nota. La figura muestra el resultado de la novena pregunta.

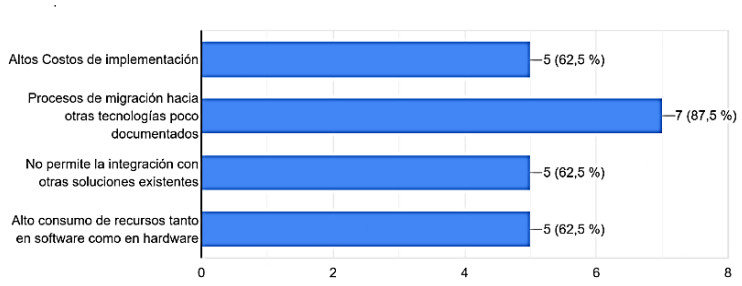
Análisis e interpretación

Del total de encuestados, el 87.5% considera que aplicaría dentro de su organización Docker como contenedor de Software para mejorar su infraestructura de servidores mientras que el 12.5 % está parcialmente de acuerdo como se muestra en la Figura 22. Se determina que, dentro de las organizaciones están dispuestas a aplicar una alternativa de solución.

10. **¿Qué desventajas considera usted que tendría la tecnología de contenedores?**

Figura 23

Décima pregunta



Nota. La figura muestra el resultado de la décima pregunta.

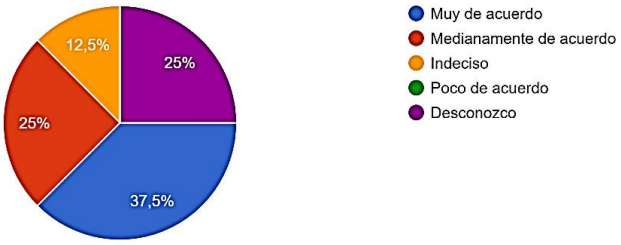
Análisis e interpretación

Del total de encuestados, el 87.5 % concuerda que una de las principales desventajas es el proceso de migración hacia otras tecnologías, con un 62.5% los altos costos de implementación, un 62.5% piensa que no permitirá la integración con otras tecnologías, y un 62.5% los altos consumos de software y hardware. Se determina que, las desventajas son variadas con respecto al uso de contenedores de software como se observa en la Figura 23.

11. ¿Cree usted que los contenedores de software presentan características como son la Integridad, Confidencialidad y Disponibilidad, descritos en la ISO 27001?

Figura 24

Décima primera pregunta



Nota. La figura muestra el resultado de la décimo primera pregunta.

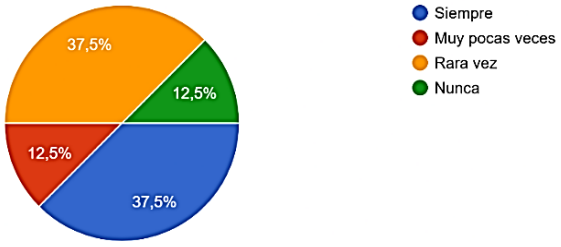
Análisis e interpretación

Del total de encuestados, el 37.5% está muy de acuerdo en que los contenedores de software presentan características como son la Integridad, Confidencialidad y Disponibilidad, un 25% medianamente de acuerdo, un 12.5% se encuentra indeciso y un 25% desconoce totalmente. Se determina que, dentro de las organizaciones concuerdan que se aplica las características expuestas en la Figura 24.

12. **Dentro de la organización aplican el ciclo de mejora continua de Deming (Planificar-Hacer-Comprobar-Actuar), descrito en la ISO 27001.**

Figura 25

Décima segunda pregunta



Nota. La figura muestra el resultado de la décimo segunda pregunta.

Análisis e interpretación

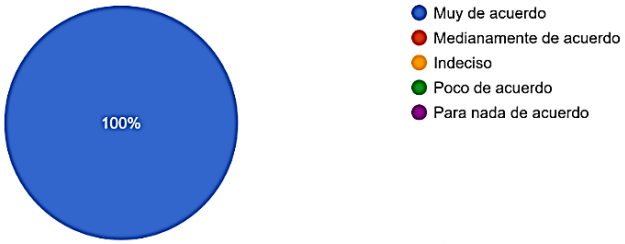
Del total de encuestados, el 37.5% siempre aplican el ciclo de mejora continua, un 37.5% rara vez, un 12.5% pocas veces y un 12.5% nunca. Se determina que, las organizaciones de manera imperativa necesitan conocer más o fondo la Norma ISO 27001 y aplicarlo en cada uno de sus procesos como se observa en la Figura 25.

La siguiente encuesta se aplicó a los directivos y técnicos del área de TIC de la organización con el propósito de conocer el grado de aceptación de la propuesta de investigación ya ejecutada.

1. **¿La propuesta de solución aplicada con contenedores Docker, cubre las necesidades actuales dentro la organización?**

Figura 26

Primera pregunta



Nota. La figura muestra el resultado de la primera pregunta.

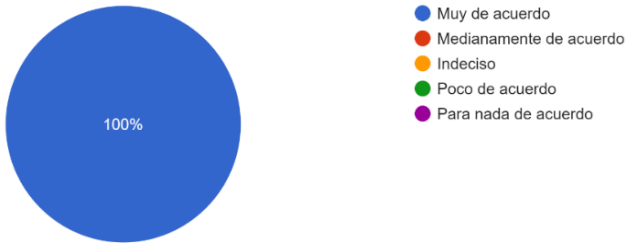
Análisis e interpretación

Del total de encuestados, el 100% está muy de acuerdo en aplicar la solución planteada. Se determina que, la propuesta cumple y cubre las necesidades de la organización por medio de contenedores Docker como se observa en la Figura 26.

2. **Con respecto a forma tradicional de instalar, configurar y desplegar aplicaciones Java EE en entornos de pruebas ¿Cree usted la propuesta de solución aplicada con contenedores Docker mejoró sustancialmente los tiempos de trabajo?**

Figura 27

Segunda pregunta



Nota. La figura muestra el resultado de la segunda pregunta.

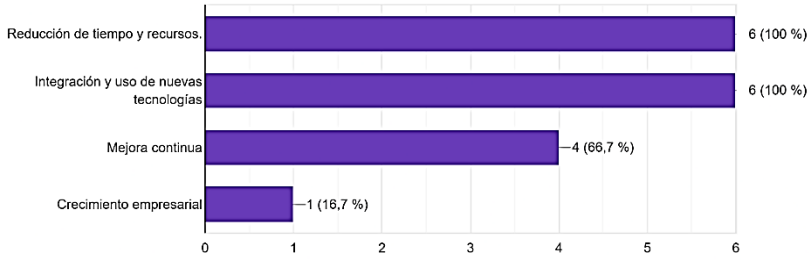
Análisis e interpretación

Del total de encuestados, el 100% está muy de acuerdo en que se redujo el tiempo de trabajo. Se determina que, la solución planteada cumple con el objetivo general planteado dentro de la investigación como se observa en la Figura 27.

3. **¿Cuál cree que es uno de los principales beneficios de aplicar contenedores Docker en el despliegue de aplicaciones Java EE?**

Figura 28

Tercera pregunta



Nota. La figura muestra el resultado de la tercera pregunta.

Análisis e interpretación

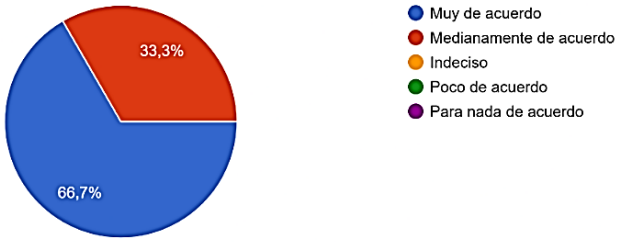
Del total de encuestados, el 100 % concuerda que uno de los principales beneficios es la reducción de tiempo y recursos, con un 100% la integración y uso de nuevas tecnologías, un 66.7% concuerda que se aplica la mejora continua, y un 16.7%

considera el crecimiento empresarial. Se determina que, la solución planteada se alinea a las necesidades de la organización aplicando nuevas tecnologías como se observa en la Figura 28.

4. **¿Crees usted que al aplicar una o varias metodologías que se alinean con la Norma ISO 27001 en conjunto con la propuesta de solución aplicada con contenedores Docker ayudó a mejorar la forma en que se venía trabajando?**

Figura 29

Cuarta pregunta



Nota. La figura muestra el resultado de la cuarta pregunta.

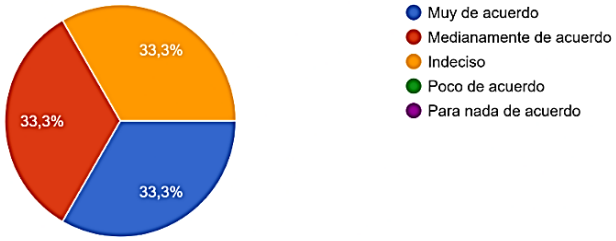
Análisis e interpretación

Del total de encuestados, el 33.3% está medianamente de acuerdo dado que es mejor cubrir toda la organización y no en partes, un 66.7% está muy de acuerdo que al abarcar parte de un proceso dentro de la organización permitirá observar que mejoras se pueden ir añadiendo a futuro. Se determina que, el uso de metodologías que se encuentran alineadas con la Norma ISO/IEC 27001 en diferentes procesos dentro de la organización permitió trabajar de manera más ordena y aplicando siempre la mejora continua como se observa en la Figura 29.

5. **Estaría de acuerdo a futuro implementar un SGSI (Sistema de Gestión de Seguridad de la Información) que abarque a toda la organización.**

Figura 30

Quinta pregunta



Nota. La figura muestra el resultado de la quinta pregunta.

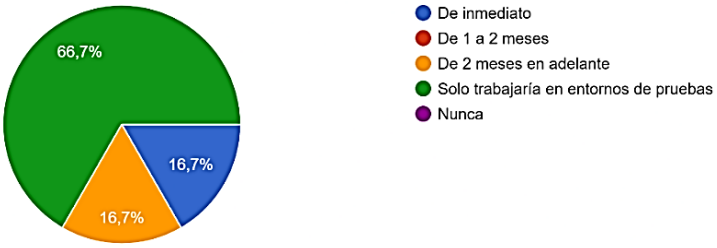
Análisis e interpretación

Del total de encuestados, el 33.3% está muy de acuerdo en implementar un SGSI, un 33.3% medianamente de acuerdo, un 33.3% indeciso. Se determina que, si bien es cierto la implementación de un SGSI aporta valor a la organización es una decisión que la toman los directivos y sin el consentimiento de ellos es poco probable que se llega a dar como se observa en la Figura 30.

6. ¿Cuál sería el tiempo estimado en aplicar la propuesta de solución con contenedores Docker para ambientes de producción?

Figura 31

Sexta pregunta



Nota. La figura muestra el resultado de la sexta pregunta.

Análisis e interpretación

Del total de encuestados, el 66.7% está de acuerdo en que la solución planteada se aplique solo en entornos de pruebas, un 16.7% que se aplique de inmediato y, un 16.7% que se aplique de 2 en adelante. Se determina que, la solución planteada para trabajar en entornos de pruebas está bien ya que si existe algún fallo no afectaría a terceros, pero para que entre a funcionar en producción es necesario realizar pruebas una y otras vez para descartar cualquier eventualidad como se observa en la Figura 31.

CAPÍTULO V

CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA, ANEXOS.

5.1. Conclusiones

- Se propuso que desde el inicio se aplique controles de la norma ISO/IEC 27001, como la identificación y valoración de activos, identificación de vulnerabilidades y amenazas, valoración de las amenazas y la evaluación de riesgos. En adición se trabaje en un ambiente de pruebas configurado con Docker y que se realice todas y cada una de las pruebas de funcionalidad, usabilidad y de rendimiento y ver cuál es el comportamiento del servidor, con lo que se pudo concluir que el funcionamiento de la aplicación Java EE no vario, lo que fue más evidente y palpable fue la reducción del tiempo de configuración y despliegue, que el consumo de recursos en RAM y almacenamiento se redujo considerablemente.

- Con base a la investigación realizada de la norma ISO/IEC 27001 permitió comprobar que la aplicabilidad de esta norma se realiza de manera sistemática independientemente del tipo, tamaño o naturaleza de una organización, proporcionando los mecanismos necesarios para la protección y optimización de recursos, un ciclo de mejora continua para alcanzar los objetivos propuestos y a futuro la posibilidad de obtener una certificación internacional.

- En el análisis de los ambientes de contenedores de software podemos destacar que, en base a la revisión de la literatura para el desarrollo del trabajo de investigación existen varias tecnologías que permiten trabajar con contenedores de software en diferentes sistemas operativos con arquitectura X64 ya sea software libre o de paga, Docker al ser una opción open source y al contar con una amplia documentación y un repositorio de imágenes bien documentadas permitió que el desarrollo del trabajo de investigación se cumpla de inicio a fin con los resultados esperados.

- Al trabajar en un ambiente de pruebas utilizando contenedores de software permitió aplicar desde un inicio el ciclo de Deming, el cual se alinea con la norma ISO/IEC 27001 y para ello en cada nueva configuración hecha en el Dockerfile se fue mejorando de manera sustancial, logrando que al final el aplicativo Java EE

se despliegue y funcione con toda normalidad, presntando fluidez en cada una de sus opciones.

- Para evaluar el nivel de aceptación y confianza de la propuesta de solución, se procedió a aplicar una encuesta posterior al finalizar el trabajo de investigación, la cual arrojo resultados satisfactorios lo que demuestra que la propuesta aplicando contenedores de software en el despliegue de aplicaciones web Java EE utilizando contenedores de software es aceptada por los miembros de organización.

5.2. Recomendaciones

- Se debe considerar que si bien el trabajo de investigación abarca temas relevantes de la norma ISO/IEC 27001 y dentro de la documentación se exponen una serie de matrices que se encuentran catalogadas con los activos que se utilizaron para el desarrollo del trabajo se recomienda abarcar a toda la organización y generar un SGSI que a futuro traerá beneficios y control más ordenado.

- Es recomendable capacitar al personal técnico de manera permanente sobre el uso de nuevas tecnologías que se encuentran en auge en los últimos tiempos y en ello incluir normativas tanto nacionales como internacionales para que conozcan sobre la importancia de aplicarlas en el día a día dentro de la organización.

- Tomar en consideración que es necesario que previo a la configuración y despliegue de los contenedores Docker en el ambiente de pruebas se realicen las pruebas pertinentes en ambientes locales dado que existe una gama amplia de imágenes en Docker Hub de las cuales se debe escoger la más adecuada y que se alinee al tema de estudio con el fin de evitar errores y prolongar los tiempos de trabajo.
- Es muy importante que la alta dirección antes de poner en marcha la implementación de un SGSI, primero demuestre liderazgo y compromiso, se asegure que todos los recursos estén disponibles, que cada uno de los procesos dentro de la organización se integren, que cada uno de los roles y responsabilidades estén bien definidos y sobre todo que exista un compromiso de mejora continua para obtener los resultados esperados.

5.3. Bibliografía

Amutio, M., Candau, J., & Mañas, J. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*.

Balcázar, M. del C. (2020). *Propuesta metodológica para mitigar el riesgo de seguridad informática con el uso de técnicas OSINT*. http://repositorio.espe.edu.ec/xmlui/handle/21000/22805?locale-attribute=de

Blial, O., & Mamoun, M. Ben. (2017). DockFlex: A Docker-based SDN Distributed Control Plane Architecture. *International Journal of Future Generation Communication and Networking*, *10*(12), 35–46. https://doi.org/10.14257/ijfgcn.2017.10.12.04

Bravo, M. J. (2018). *Desarrollo de un Sistema de Gestión de Seguridad de la Información para bibliotecas basado en una metodología mejorada para análisis de riesgos compatible con la norma ISO/IEC 27001:2013*. https://bibdigital.epn.edu.ec/handle/15000/19880

Camacho, V. (2021). *Diseño de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO/IEC 27001:2013, para una fábrica de cuero y calzado*. https://bibdigital.epn.edu.ec/handle/15000/21975

Cepeda, M., & De La Cruz, C. (2018). *Herramientas de gestión de tecnologías de información y comunicación TIC y su incidencia en los sistemas de evaluación y control interno de las empresas del sector servicios reguladas por la superintendencia de compañías en la provincia de Cotopaxi periodo 2012-2016*. https://repositorio.espe.edu.ec/handle/21000/14617

Cordero, M. G. (2022). *Políticas de seguridad de la información basadas en normas internacionales para garantizar controles ante amenazas y vulnerabilidades en el departamento de tecnología de la cooperativa de ahorro y crédito San Francisco LTDA*. https://repositorio.uta.edu.ec/handle/123456789/34814

Cortez, E. (2020). *Desarrollo de una aplicación web utilizando el IDE de desarrollo NETBEANS para la gestión de los procesos de solicitudes complementarias en la atención médica del hospital de especialidades de las FF. AA N°1*. http://repositorio.espe.edu.ec/xmlui/handle/21000/24921

De la Cruz, D. A., & Segura, K. G. (2017). *Diseño de un plan de SGSI para un caso de estudio en el área de TI*. https://bibdigital.epn.edu.ec/handle/15000/17328

Dziurzanski, P., Zhao, S., Przewozniczek, M., Komarnicki, M., & Indrusiak, L. S. (2020). Scalable distributed evolutionary algorithm orchestration using Docker containers. *Journal of Computational Science*, *40*. https://doi.org/10.1016/j.jocs.2019.101069

Elmenreich, W., Moll, P., Theuermann, S., & Lux, M. (2019). Making simulation results reproducible-Survey, guidelines, and examples based on gradle and docker. *PeerJ Computer Science*, *2019*(12), 1–27. https://doi.org/10.7717/peerj-cs.240

Fernández, G. (2021). *Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la*

disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí. http://repositorio.espe.edu.ec/xmlui/handle/21000/26482

Fernández, L. (2020). *Sistematización de la gestión del Procedimiento Oncológico y Parte Operatorio del Hospital de Especialidades Fuerzas Armadas Nº 1. A través de un sistema orientado a la web*. http://repositorio.espe.edu.ec/bitstream/21000/24923/1/M-ESPEL-sit-0094.pdf

Guacanés, M., & Vilatuña, J. (2022). *Propuesta de diseño de un SGSI basado en la norma ISO/IEC 27001. Caso de estudio la empresa Ultralink.* https://bibdigital.epn.edu.ec/handle/15000/22812

Guano, M., & Jaramillo, M. (2021). *Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio*. https://bibdigital.epn.edu.ec/handle/15000/21472

Guayasamin, C. (2022). *Sistema de Doctorados para la Universidad Central del Ecuador*. http://www.dspace.uce.edu.ec/handle/25000/29595

Hinojosa, M. (2021). *Modelado Funcional de Contenedores Virtuales Docker*. https://www.tamps.cinvestav.mx/descargables/tesis/2021/6_2021_Mariana_Magdalena_Hinojosa_Tijerina_M_2019.pdf

Jaramillo, A., & Puchaicela, W. (2022). *Evaluación comparativa de rendimiento de PostgreSQL y Cassandra en operaciones CRUD*. http://repositorio.espe.edu.ec/xmlui/handle/21000/32544

Javed, O., & Toor, S. (2021). *Understanding the Quality of Container Security Vulnerability Detection Tools*. https://arxiv.org/abs/2101.03844

Kim, B. S., Lee, S. H., Lee, Y. R., Park, Y. H., & Jeong, J. (2022). Design and Implementation of Cloud Docker Application Architecture Based on Machine Learning in Container Management for Smart Manufacturing. *Applied Sciences*, *12*(13), 6737. https://doi.org/10.3390/app12136737

Kwon, S., & Lee, J. H. (2020). DIVDS: Docker Image Vulnerability Diagnostic System. *IEEE Access*, *8*, 42666–42673. https://doi.org/10.1109/ACCESS.2020.2976874

López, A. (2020). *Despliegue de aplicaciones escalables con Kubernetes*. http://repositorio.ual.es/bitstream/handle/10835/9871/LOPEZ%20GARCIA%2C%20ANTONIO.pdf

Lucano, L. F. (2019). *Diagnóstico y diseño de un sistema de gestión de seguridad de la información (SGSI), basado en la norma ISO/IEC 27001:2013, en un banco público*. http://www.dspace.uce.edu.ec/handle/25000/18451

Martínez, A. (2022). *Implementación de un servidores con herramientas DevOps: Implementación de un servidor NGINX en Docker con vhost.* https://bibdigital.epn.edu.ec/handle/15000/23046

Mendoza, P., & Naranjo, D. (2020). *Plan de gestión de seguridad de la información para la empresa ALPHA TECHNOLOGIES CIA. LTDA con la norma ISO/IEC 27001:2011*. https://bibdigital.epn.edu.ec/handle/15000/20959

Montalvo Ochoa, F. G. (2020). *Análisis, diseño y desarrollo de un sistema para la gestión del seguimiento de pasantías y prácticas pre-profesionales a través de la implementación de microservicios en Docker para la Universidad Politécnica Salesiana*. https://dspace.ups.edu.ec/handle/123456789/19483

Ortiz, R. (2022). *PROTOTIPO DE SISTEMA DE FIDELIZACIÓN DE COMERCIO ELECTRÓNICO USANDO TECNOLOGÍA DOCKER Y SERVICIOS DE AMAZON* .

Pacheco, J. (2018). *Estudio comparativo entre una arquitectura con microservicios y contenedores dockers y una arquitectura tradicional (monolítica) con comprobación aplicativa*. http://repositorio.ug.edu.ec/handle/redug/32755

Pazmiño, C., Serrano, A., & González, M. (2020). *Las Tics como herramienta para la gestión de riesgos*. https://recimundo.com/index.php/es/article/view/793

Quilachamín, A. (2020). *Despliegue de un sistema de gestión de eventos e información de seguridad de código abierto*. https://bibdigital.epn.edu.ec/handle/15000/20870

Quiñonez Quintero, J. M. (2022). *Elaboración y evaluación de un sistema que permita mejorar la disponibilidad y seguridad en los servicios web de la Universidad Técnica Luis Vargas Torres, mediante el uso de herramientas de software libre.* http://dspace.espoch.edu.ec/handle/123456789/15706

Rivadeneira, A. (2022). *Implementación de contenedores alojados en la nube*. https://bibdigital.epn.edu.ec/handle/15000/23044

Rosero, M. (2019). *REESTRUCTURACIÓN E IMPLEMENTACIÓN DE NUEVOS SERVICIOS AL SISTEMA DE GESTIÓN DE VISITAS MÉDICAS DEL LABORATORIO GENESIS DE LA CIUDAD DE AMBATO*. https://repositorio.uti.edu.ec/handle/123456789/1125

Ruano, M. D. L. Á. (2020). *Sistema de registro de bienes inmuebles ancestrales de la parroquia San Antonio de Ibarra utilizando el framework laravel y un visor geográfico*. http://repositorio.utn.edu.ec/handle/123456789/10361

Sarmiento, L. (2020). *Diseño y desarrollo de una aplicación web para la gestión de la bodega de suministros mediante el uso de software libre, en el Comando Logístico N °25 "Reino de Quito."* http://repositorio.espe.edu.ec/xmlui/handle/21000/24957

Subrahmanyam, A., Cedric, B., & John, D. (2002). *Programación Java Server con J2EE Edición 1.3*. ANAYA MULTIMEDIA.

Tusa, E. (2021). *Evaluación Técnica Informática al Subsistema de Matriculación Vehicular de la Mancomunidad de Tránsito del Norte con base en COBIT 2019*. https://repositorio.espe.edu.ec/bitstream/21000/25461/1/T-ESPE-044667.pdf

Valencia, J. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000*. http://www.fadmon.unal.edu.co/fileadmin/user_upload/extension/cursos/imagenes_cursos/digitales_septiembre/sistema_de_gestion_de_seguridad-1.pdf

Vergara, P. (2019). *"Sivenlac" sistema web de inventario para control de existencias en la bodega de materiales, de la empresa "PASTOLAC."* http://repositorio.espe.edu.ec/xmlui/handle/21000/20648

Villegas, J. (2019). *Evaluación técnica informática al sistema de gestión de seguridad de la información del GAD provincial de Imbabura en base de la norma ISO/IEC 27001:2013*. http://repositorio.espe.edu.ec/xmlui/handle/21000/21529

You, L., & Sun, H. (2022). Research and Design of Docker Technology Based Authority Management System. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/5325694

5.4. Anexos

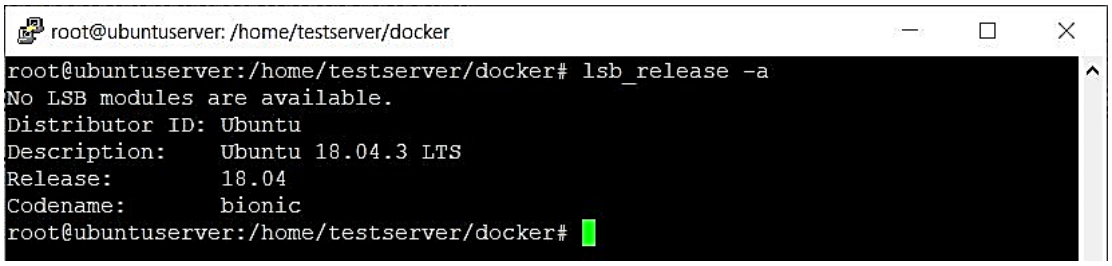
Anexo I

Prerrequisitos

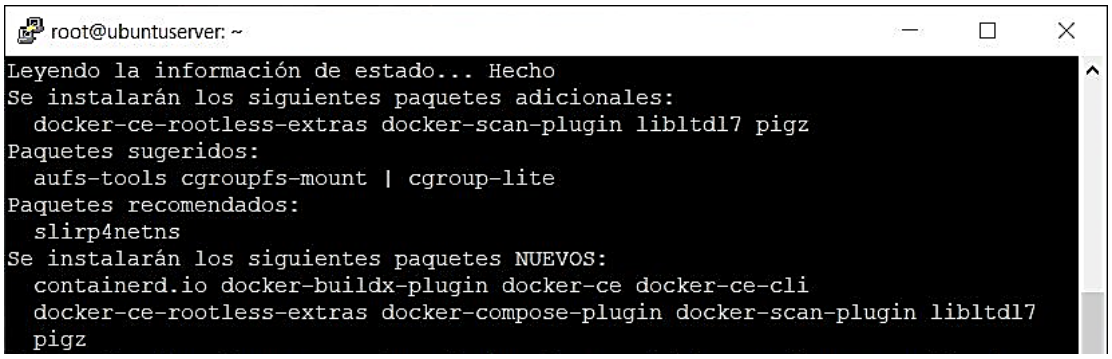
Para completar la instalación, necesitará lo siguiente:

1. Un servidor de **Ubuntu Server 22.04.2** con la arquitectura x64.
2. Acceso a internet.
3. Conexión por medio de SSH.

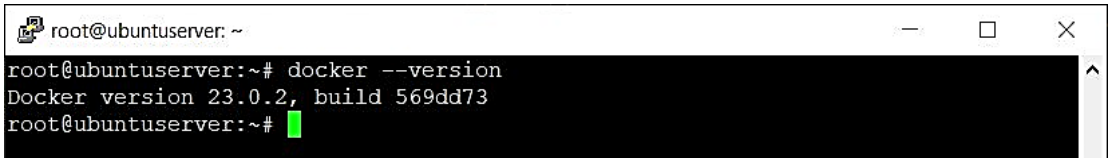
Una vez instalado Ubuntu Server se necesitará que se encuentre actualizado.



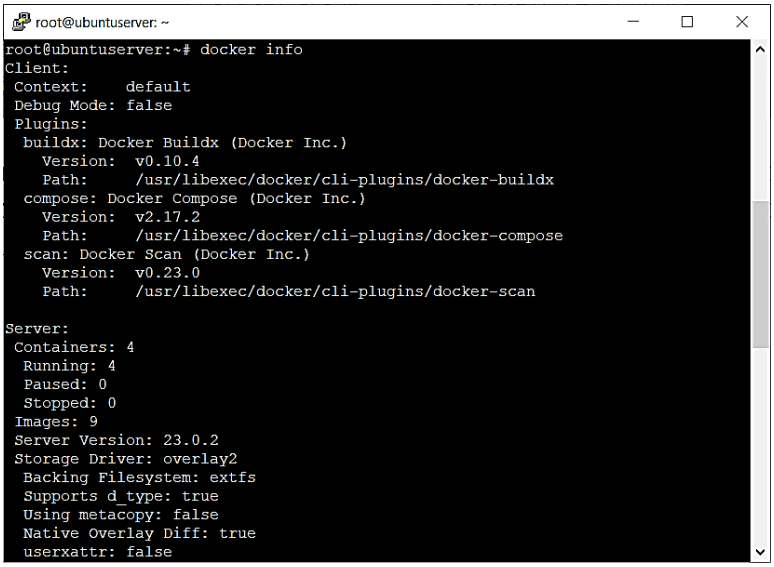
Instalar la versión más actual de Docker.



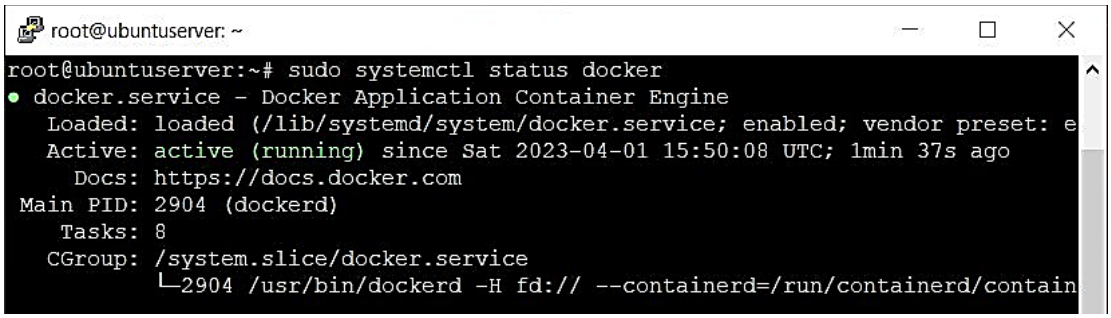
Verificar la versión instalada de Docker.



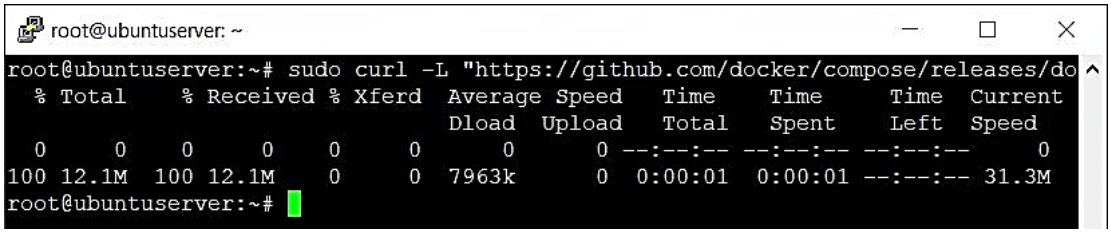
Para visualizar la información de todo el sistema sobre la instalación de Docker como: la cantidad de contenedores e imágenes, el nombre del grupo, el archivo de datos, archivo de metadatos, espacio de datos utilizado, controlador de ejecución y la versión del kernel.



Verificar que el servicio de Docker se encuentre activo en el servidor.

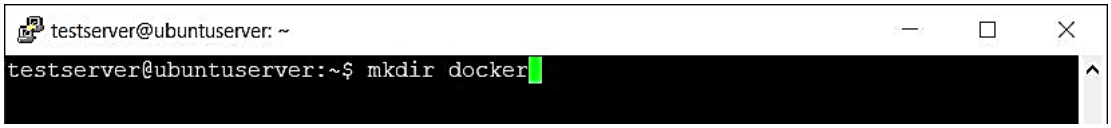


Instalar la versión más actual de Docker Compose.

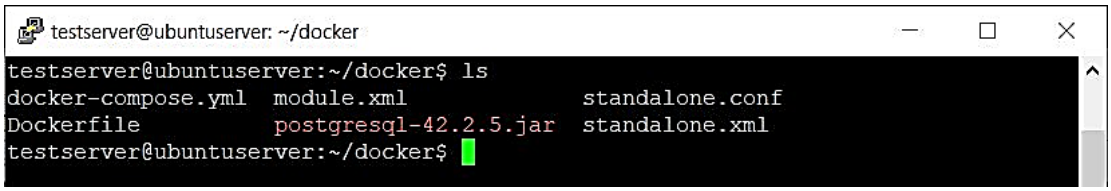


Verificar la versión instalada de Docker Compose.

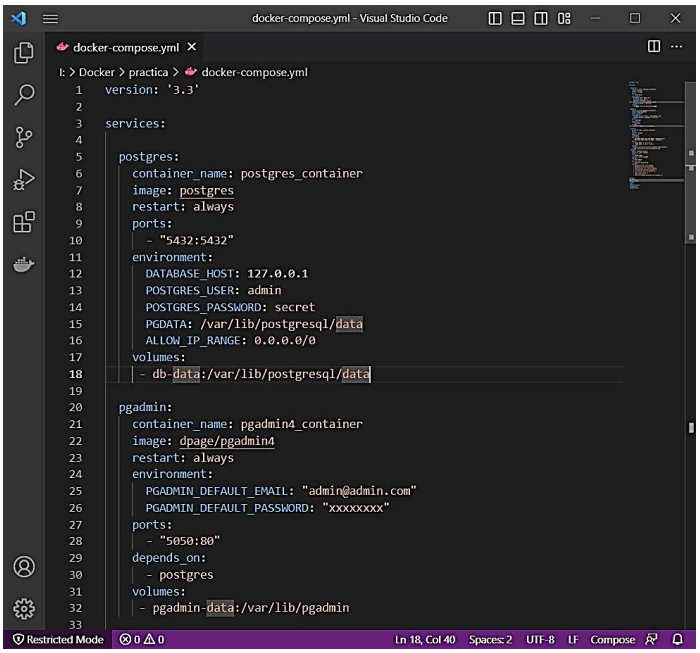
Crear un directorio donde se alojarán los archivos de configuración.



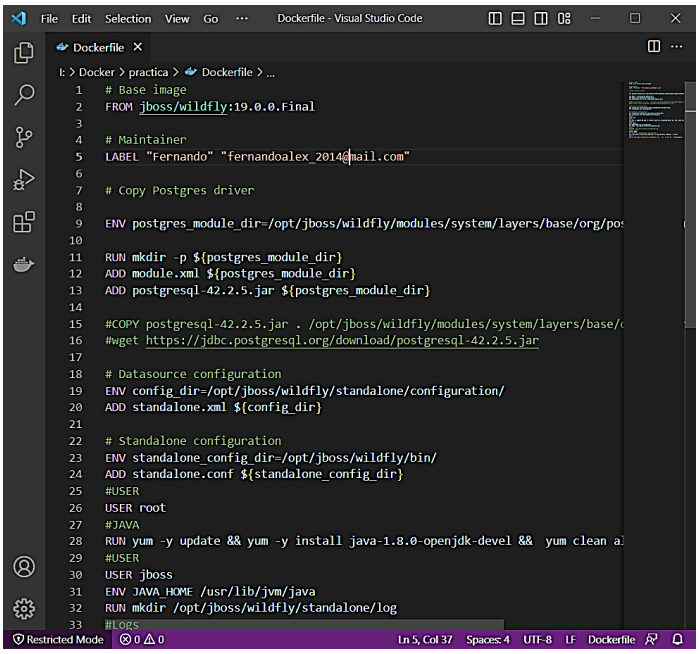
Copiar todos los archivos de configuración en el directorio creado.



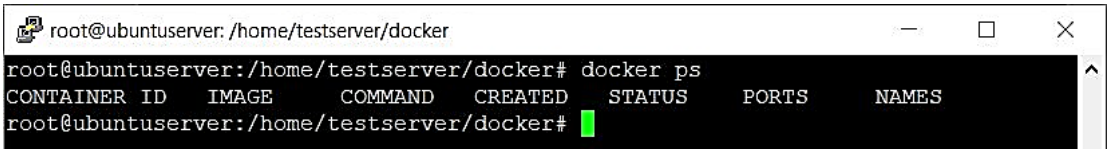
Crear un archivo docker-compose.yml con cada una de las imágenes (postgres, pgadmin4, wildfly, netdata) y su configuración respectiva como lo es usuarios, contraseñas, puertos de escucha del host y del contenedor para tener comunicación hacia el exterior.



Docker Hub presenta un gran repositorio de imágenes oficiales y otra serie de imágenes creadas por terceros las cuales pueden tener o no soporte. Si se desea trabajar desde cero se puede crear una nueva a partir de la configuración de un Dockefile.



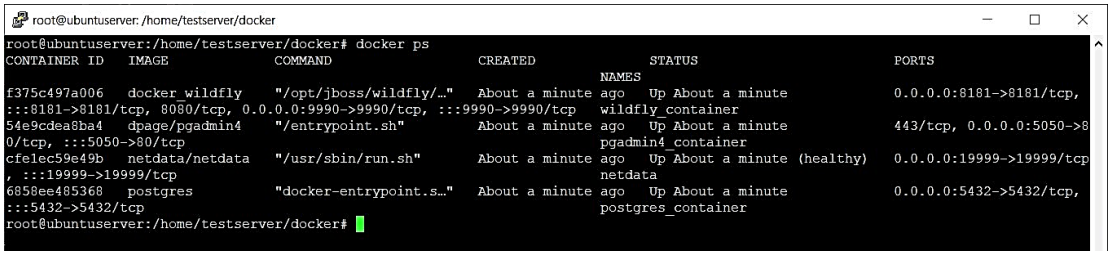
Verificar que contenedores se encuentran ejecutando.



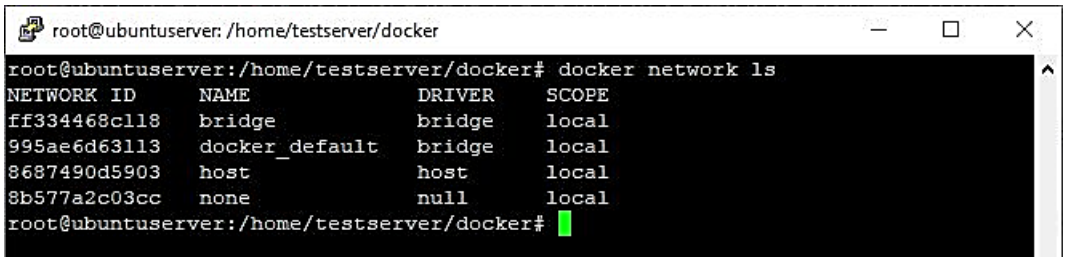
Construir la imagen que se encuentre referenciada en el docker-compose.yml a partir de un Dockerfile.

Crear el o los contenedores (servicio) que se encuentran configurados en el archivo docker-compose.yml en modo detach lo que significa que dentro de la terminal se ve visualizará los logs.

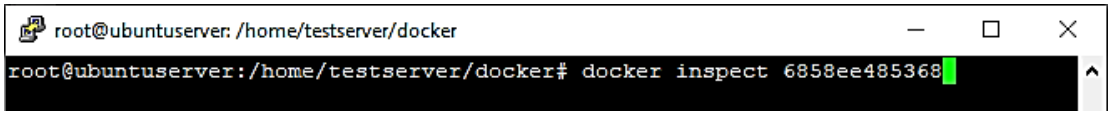
Verificar que contenedores se encuentran ejecutando.



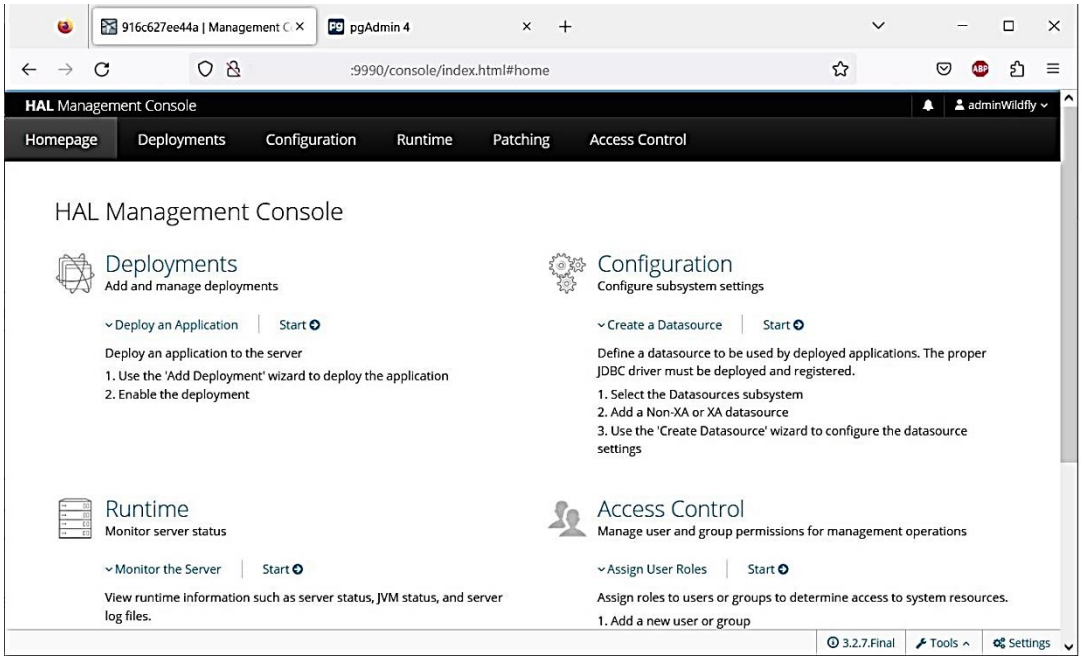
Para conectar cada uno de los contenedores verificar que tipo de red se encuentra creada.

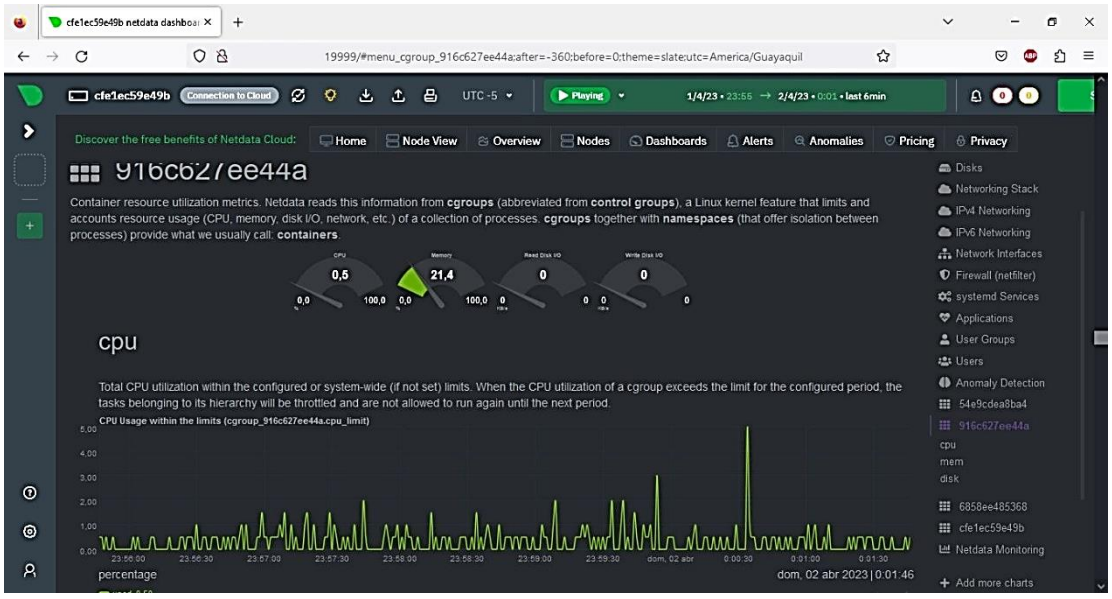


Verificar las direcciones IP de cada uno de los contenedores.

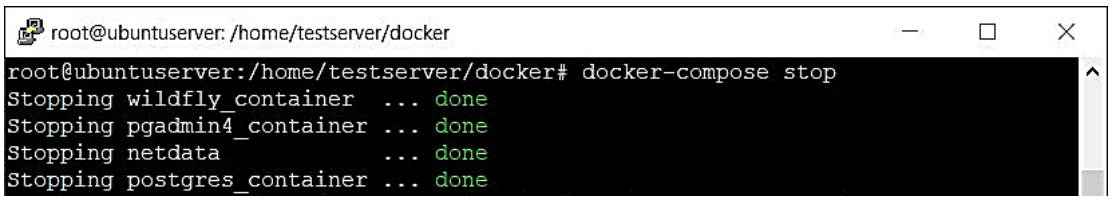


Por medio de la dirección IP y los puertos de escucha del host ingresar a un navegador web y verificar que cada uno de los contenedores configurados tengan acceso.

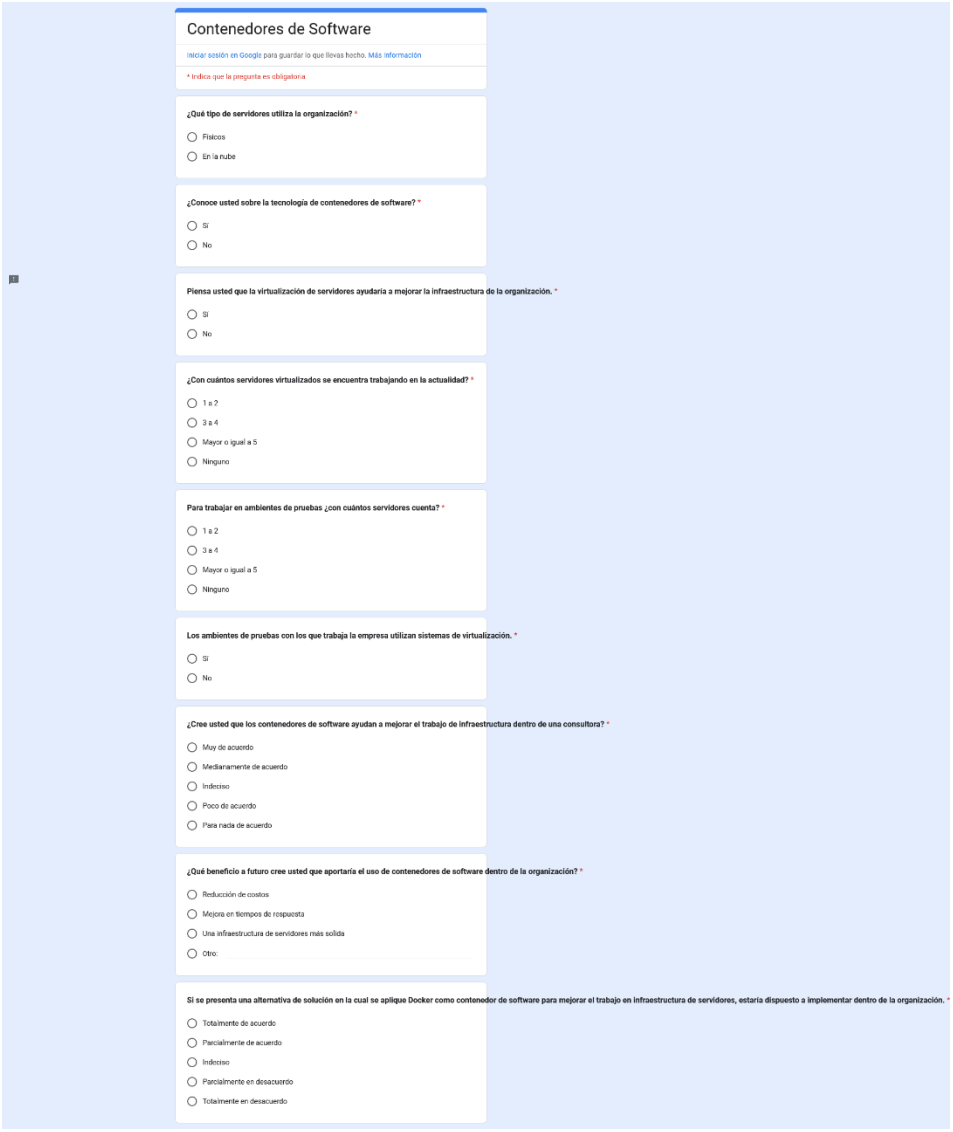




Para detener todos los contenedores que se hayan ejecutado con anterioridad.



Anexo II



Contenedores de Software

Iniciar sesión en Google para guardar lo que llevas hecho. Más información

* Indica que la pregunta es obligatoria

¿Qué tipo de servidores utiliza la organización? *
- Físicos
- En la nube

¿Conoce usted sobre la tecnología de contenedores de software? *
- Sí
- No

Piensa usted que la virtualización de servidores ayudaría a mejorar la infraestructura de la organización. *
- Sí
- No

¿Con cuántos servidores virtualizados se encuentra trabajando en la actualidad? *
- 1 a 2
- 3 a 4
- Mayor o igual a 5
- Ninguno

Para trabajar en ambientes de pruebas ¿con cuántos servidores cuenta? *
- 1 a 2
- 3 a 4
- Mayor o igual a 5
- Ninguno

Los ambientes de pruebas con los que trabaja la empresa utilizan sistemas de virtualización. *
- Sí
- No

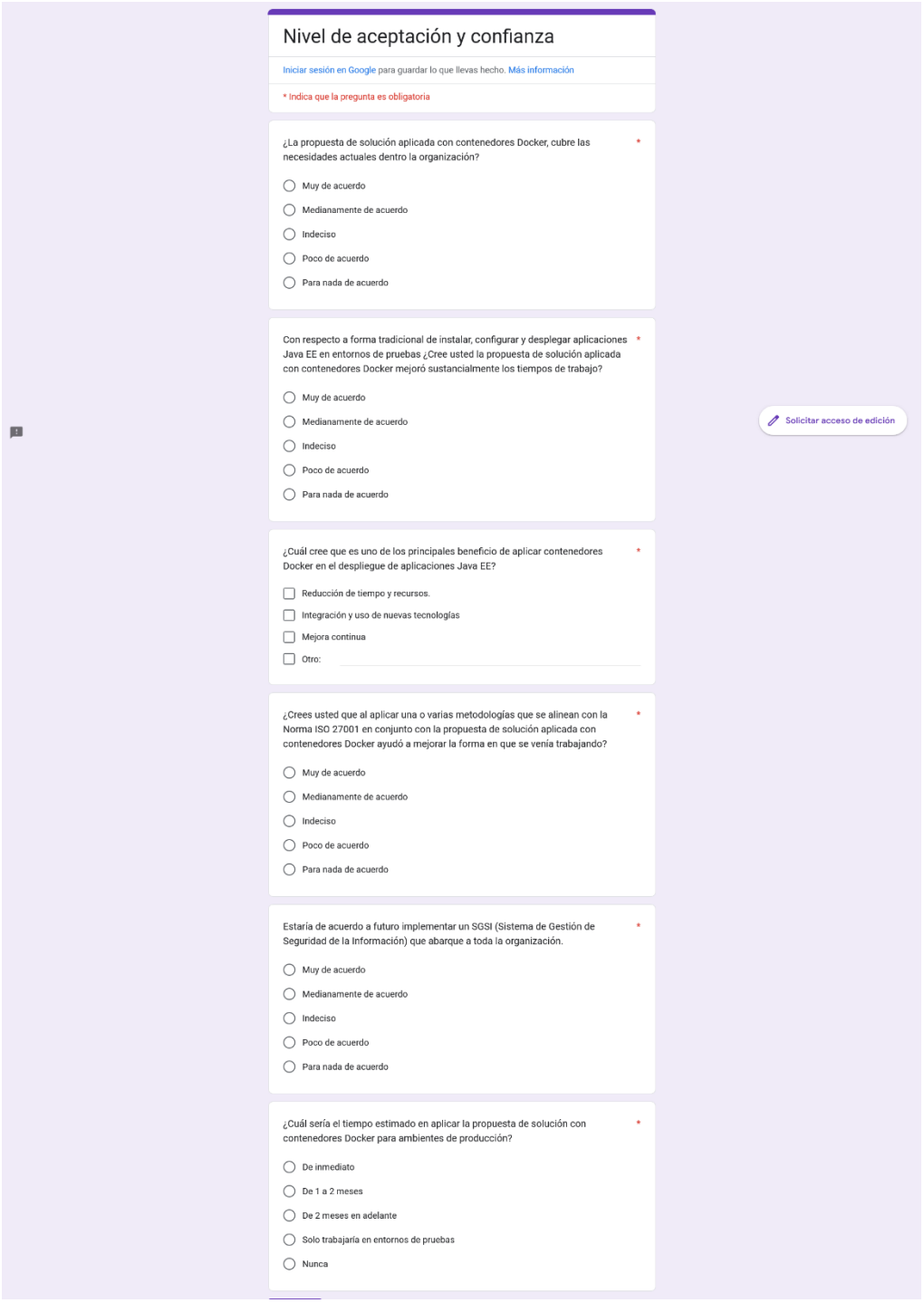
¿Cree usted que los contenedores de software ayudan a mejorar el trabajo de infraestructura dentro de una consultora? *
- Muy de acuerdo
- Medianamente de acuerdo
- Indeciso
- Poco de acuerdo
- Para nada de acuerdo

¿Qué beneficio a futuro cree usted que aportaría el uso de contenedores de software dentro de la organización? *
- Reducción de costos
- Mejora en tiempos de respuesta
- Una infraestructura de servidores más solida
- Otro:

Si se presenta una alternativa de solución en la cual se aplique Docker como contenedor de software para mejorar el trabajo en infraestructura de servidores, estaría dispuesto a implementar dentro de la organización. *
- Totalmente de acuerdo
- Parcialmente de acuerdo
- Indeciso
- Parcialmente en desacuerdo
- Totalmente en desacuerdo

La encuesta completa la encuentra en el siguiente enlace:

https://forms.gle/7Njb6oHLhm4b2AYz5



La encuesta completa la encuentra en el siguiente enlace:

https://forms.gle/H9s1ySSZq3hUYmce6

Anexo III

Identificación y clasificación de activos

Activos de Hardware

Código	**Tipo**	**Equipo**	**Características**					**Ubicación**	**Responsable**
			Marca	**Modelo**	**Procesador**	**Memoria**	**S.O.**		
AHW_01	[pc]	Laptop	Toshiba	S55-a5164	Core i7-4700MQ 2.4GHz	16 GB	Ubuntu 18.04.6	Área de desarrollo	Fernando Moya
AHW_02	[vhost]	Servidor			AMD Opteron Octa-Core, 8x2.4 Turbo 2,40 GHz	16 GB	Ubuntu Server	En la nube	Fernando Moya
AHW_03	[modem]	Modem						Área de desarrollo	

Activos de Software

Código	Tipo	Fabricante	Características		
			Software	**Versión**	**Costo**
ASW_01	[os]	Windows	Sistema operativo	10 Home 22H2	Licencia Original
ASW_02	[os]	Ubuntu	Sistema operativo	18.04.6 LTS	Licencia GNU GPL
ASW_03	[os]	Ubuntu	Sistema operativo servidor	18.04.3-live-server-amd64	Licencia GNU GPL
ASW_04	[prp]	Sistema administrativo financiero	Software libre		

Activos de Información

Código	Tipo	Nombre	Estado	Acceso	Características
AD_01	[files]	Base de datos Administrativo Financiero	Digital	Privado	Uso dentro de la organización
AD_02	[backup]	Backups	Digital	Privado	Uso dentro de la organización
AD_03	[conf]	Diagrama de red	Digital	Privado	Uso dentro de la organización
AD_04	[source]	Código fuente	Digital	Privado	Uso dentro de la organización

Activos de Personal

Código	Tipo	Área	Nro. Personal
AP_01	[des]	Desarrollo de software	5
AP_02	[ui]	Administrativa	4

Activos de soportes de información

Código	Tipo	Características			
		Equipo	**Marca**	**Modelo**	**Capacidad**
AMEDIA_01	[disk]	Discos	ADATA	HD710 Pro	1TB
AMEDIA_02	[usb]	Memorias USB	Kingston	DT50	32 Gb

Activos de equipos Auxiliares

Código	Tipo	Características			
		Equipo	**Marca**	**Modelo**	**Descripción**
AAUX_01	[power]	Regulador de voltaje	Forza	Fvr-2201	Regulador Voltaje 2200va 1100w 8 Tomas.
AAUX_02	[ac]	Cooler	Argon		Base Enfriadora Reclinable Laptop Notebook, 2-USB, Alturas ajustables de 5 niveles.

Anexo IV

Valoración de activos

Activos de Hardware

Activo	Ubicación	Valoración			Promedio
		[C]	[I]	[D]	
AHW_01	Área de desarrollo	5	8	9	7,33
AHW_02	En la nube	6	8	9	7,67
AHW_02	Área de desarrollo	2	2	5	3,00

Activos de Software

Activo	Ubicación	Valoración			Promedio
		[C]	[I]	[D]	
ASW_01	Área de desarrollo	5	8	9	7,33
ASW_02	Área de desarrollo	8	8	9	8,33
ASW_03	En la nube	6	8	9	7,67
ASW_04	Área de desarrollo	9	8	8	8,33

Activos de Información

Activo	Ubicación	Valoración			Promedio
		[C]	[I]	[D]	
AD_01	Área de desarrollo	9	9	9	9,00
AD_02	Área de desarrollo	9	9	9	9,00
AD_03	Área de desarrollo	5	5	6	5,33
AD_04	Área de desarrollo	9	9	9	9,00

Activos de Personal

Activo	Ubicación	Valoración			Promedio
		[C]	[I]	[D]	
AP_01	Área de desarrollo	5	2	0	2,33
AP_02	Área administrativa	5	2	0	2,33

Activos de soportes de información

Activo	Ubicación	Valoración			Promedio
		[C]	[I]	[D]	
AMEDIA_01	Área de desarrollo	8	9	9	8,67
AMEDIA_02	Área de desarrollo	8	9	9	8,67

Activos de equipos Auxiliares

Activo	Ubicación	Valoración			Promedio
		[C]	[I]	[D]	
AAUX_01	Área de desarrollo	0	0	0	0,00
AAUX_02	Área de desarrollo	0	0	0	0,00

Anexo V

Identificación de vulnerabilidades y amenazas

Activos de Hardware

Activo	Tipo	Vulnerabilidades	Amenazas	Dimensiones
Hardware [AHW]	[pc]	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	Disponibilidad
		Fugas en las cañerías de agua.	[N.2] Daños por agua	Disponibilidad
		Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	Disponibilidad
		Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	Disponibilidad
		Mala manipulación, transporte, etc., de los equipos	[E.1] Errores de los usuarios	Integridad Confidencialidad Disponibilidad
		Mala manipulación, transporte, configuración, etc., de los equipos	[E.2] Errores del administrador	Integridad Disponibilidad Confidencialidad

		Mala manipulación, transporte, configuración, etc., de los equipos	[E.23] Errores de mantenimiento/ actualización de equipos (hardware)	Disponibilidad
		No contar con un inventario de activos y de custodios actualizado	[E.25] Perdida de equipos	Disponibilidad Confidencialidad
		Utilizar los activos asignados para realizar otras tareas.	[A.7] Uso no previsto	Disponibilidad Confidencialidad Integridad
		Ingresar a los equipos de la organización sin previo aviso o autorización.	[A.11] Acceso no autorizado	Confidencialidad Integridad
		Cambio de partes o piezas sin previo aviso o autorización.	[A.23] Manipulación de los equipos	Confidencialidad Disponibilidad
		Robo de los equipos de desarrollo.	[A.25] Robo	Disponibilidad Confidencialidad
		Fallo en el servicio de Internet	[I.8] Fallo de servicios de telecomunicaciones	Disponibilidad
		Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	Disponibilidad
	[modem]	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	Disponibilidad

		Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	Disponibilidad
		Mala manipulación, transporte, etc., de los equipos	[E.1] Errores de los usuarios	Integridad Confidencialidad Disponibilidad
		No contar con un inventario de activos y de custodios actualizado	[E.25] Perdida de equipos	Disponibilidad Confidencialidad
		Procesos que ocupan grandes recursos de procesamiento en procesador, memoria y disco.	[E.24] Caída del sistema por agotamiento de recursos	Disponibilidad
	[vhost]	Ingresar a los equipos de la organización sin previo aviso o autorización.	[A.11] Acceso no autorizado	Confidencialidad Integridad
		Fallo en el servicio de Internet	[I.8] Fallo de servicios de telecomunicaciones	Disponibilidad

Activos de Software

Activo	Tipo	Vulnerabilidades	Amenazas	Dimensiones
Software [ASW]	[os]	Errores de fábrica de los componentes electrónicos.	[I.5] Avería de origen físico o lógico	Disponibilidad
		Ingreso erróneo de información, claves de acceso a la vista.	[E.1] Errores de los usuarios	Integridad Confidencialidad Disponibilidad
		Claves de acceso comprometidas, configuración de puertos de acceso por defecto.	[E.2] Errores del administrador	Disponibilidad Integridad Confidencialidad
		No existe una política de cual es procedimiento para seguir.	[E.20] Errores de mantenimiento/ actualización de programas (software)	Integridad Disponibilidad Confidencialidad
		Compartición de archivos infectos.	[E.8] Difusión de software dañino	Integridad Disponibilidad Confidencialidad
	[prp]	Actualización del código fuente en el SVN.	[E.15] Alteración accidental de la información	Integridad
		Copias no autorizadas del código fuente.	[E.19] Fugas de información	Confidencialidad

		A presar de que existe un framework de trabajo se aplican malas prácticas de desarrollo.	[E.20] Vulnerabilidades de los programas (software)	Integridad Disponibilidad Confidencialidad
		Errores en la configuración de seguridad, contraseñas por defecto y no encriptadas.	[A.5] Suplantación de identidad	Confidencialidad Autenticidad Integridad
		Ingreso de código malicioso para fines lucrativos o poco éticos.	[A.7] Uso no previsto	Disponibilidad Confidencialidad Integridad
		Errores en la configuración de seguridad, contraseñas por defecto y no encriptadas.	[A.15] Modificación deliberada de la información	Integridad
		Ingreso de código malicioso para borrar trazabilidad de acciones en los sistemas.	[A.18] Destrucción de la información	Disponibilidad
		Falta de controles de acceso, perfiles y grupos de usuarios.	[A.19] Divulgación de la información	Confidencialidad
		Robo de información como claves de acceso, cuentas bancarias, etc.	[A.22] Manipulación de programas	Confidencialidad Integridad Disponibilidad

Activos de Información

Activo	Tipo	Vulnerabilidades	Amenazas	Dimensiones
Datos/Información [AD]	[files]	Falla en los procesos de copia de la información, errores.	[I.5] Avería de origen físico o lógico	Disponibilidad

		Falla en los componentes electrónicos de las unidades de almacenamiento.	[I.5] Avería de origen físico o lógico	Disponibilidad
		Procesos ad hoc	[E.1] Errores de los usuarios	Integridad Confidencialidad Disponibilidad
		No existe una política clara de cual es procedimiento para seguir.	[E.2] Errores del administrador	Disponibilidad Integridad Confidencialidad
		Gestión deficiente al momento de almacenar los logs de los sistemas.	[E.3] Errores de monitorización	Integridad (Trazabilidad)
		No existe un correcto control de personas que tienen acceso a las bases de datos.	[E.15] Alteración accidental de la información	Integridad
		Falta de un control de registro de las transacciones que se dan en las bases de datos.	[E.18] Destrucción de información	Disponibilidad
		Falta de un control de registro de las transacciones que se dan en las bases de datos.	[A.18] Destrucción de la información	Disponibilidad

		Robo de información de clientes y proveedores.	[A.19] Divulgación de la información	Confidencialidad
	[backup]	No existe una política clara de cual es procedimiento para seguir.	[E.2] Errores del administrador	Disponibilidad Integridad Confidencialidad
		No existe un correcto control de personas que tienen acceso a las bases de datos.	[E.15] Alteración accidental de la información	Integridad
		Falta de un control de registro de las transacciones que se dan en las bases de datos.	[A.18] Destrucción de la información	Disponibilidad
		Copias de los backups sin previa autorización.	[A.6] Abuso de privilegios de acceso	Integridad Confidencialidad Disponibilidad
	[conf]	Falta de una política clara sobre el manejo y cambio de contraseñas y puertos de acceso.	[A.5] Suplantación de identidad	Confidencialidad Autenticidad Integridad
	[source]	Falla en los procesos de copia de la información, errores.	[I.5] Avería de origen físico o lógico	Disponibilidad
		Robo de información del código fuente.	[A.19] Divulgación de la información	Confidencialidad

Activos de Personal

Activo	Tipo	Vulnerabilidades	Amenazas	Dimensiones
Personal [AP]	[des]	Roles no definidos dentro de la organización.	[E.7] Deficiencia en la organización	Disponibilidad
		Políticas internas pocos definidas.	[E.19] Fugas de información	Confidencialidad
		Personal poco motivado o con exceso de carga laboral.	[E.28] Indisponibilidad del personal	Disponibilidad
		Amenazas para la entrega de información a terceros.	[A.29] Extorsión	Integridad Confidencialidad Disponibilidad
		Robo de información, claves de acceso.	[A.30] Ingeniería Social	Confidencialidad Integridad Disponibilidad
	[ui]	Roles no definidos dentro de la organización.	[E.7] Deficiencia en la organización	Disponibilidad
		Políticas internas pocos definidas.	[E.19] Fugas de información	Confidencialidad
		Personal poco motivado o con exceso de carga laboral.	[E.28] Indisponibilidad del personal	Disponibilidad

		Amenazas para la entrega de información a terceros.	[A.29] Extorsión	Integridad Confidencialidad Disponibilidad
		Robo de información, claves de acceso.	[A.30] Ingeniería Social	Confidencialidad Integridad Disponibilidad

Activos de soportes de información

Activo	Tipo	Vulnerabilidades	Amenazas	Dimensiones
Soporte de información [AMedia]	[disk]	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	Disponibilidad
		Caídas inintencionales de agua	[N.2] Daños por agua	Disponibilidad
		Fallas en los componentes electrónicos de los equipos.	[I.5] Avería de origen físico o lógico	Disponibilidad
		Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	Disponibilidad

		Fallas en los componentes electrónicos de los equipos.	[I.10] Degradación de los soportes de almacenamiento de la información	Disponibilidad
		Mala manipulación de los equipos.	[E.1] Errores de los usuarios	Integridad Confidencialidad Disponibilidad
		Formateo o pérdida total de la información.	[E.18] Destrucción de información	Disponibilidad
		Política poco clara sobre las unidades de almacenamiento dentro de la organización.	[E.19] Fugas de información	Confidencialidad
		Robo de las unidades de almacenamiento.	[E.25] Perdida de equipos	Disponibilidad Confidencialidad
		Uso de las unidades de almacenamiento para otros fines (música, videos, fotos, etc)	[A.7] Uso no previsto	Disponibilidad Confidencialidad Integridad
		Destrucción de las unidades de almacenamiento.	[A.18] Destrucción de la información	Disponibilidad
		Política poco clara sobre las unidades de almacenamiento dentro de la organización.	[A.19] Divulgación de la información	Confidencialidad
		Robo de las unidades de almacenamiento.	[A.25] Robo	Disponibilidad Confidencialidad

		Destrucción deliberada de las unidades de almacenamiento.	[A.26] Ataque destructivo	Disponibilidad
	[usb]	Fallas en los componentes electrónicos de los equipos.	[I.5] Avería de origen físico o lógico	Disponibilidad
		Mala manipulación de los equipos.	[E.1] Errores de los usuarios	Confidencialidad Disponibilidad Integridad
		Formateo o pérdida total de la información.	[E.18] Destrucción de información	Disponibilidad
		Robo de las unidades de almacenamiento.	[E.25] Perdida de equipos	Disponibilidad Confidencialidad
		Uso de las unidades de almacenamiento para otros fines (música, videos, fotos, etc)	[A.7] Uso no previsto	Disponibilidad
		Destrucción de las unidades de almacenamiento.	[A.18] Destrucción de la información	Disponibilidad
		Política poco clara sobre las unidades de almacenamiento dentro de la organización.	[A.19] Divulgación de la información	Confidencialidad
		Robo de las unidades de almacenamiento.	[A.25] Robo	Disponibilidad Confidencialidad
		Destrucción deliberada de las unidades de almacenamiento.	[A.26] Ataque destructivo	Disponibilidad

Activos de equipos Auxiliares

Activo	Tipo	Vulnerabilidades	Amenazas	Dimensiones
Equipos auxiliares [AAUX]	[power]	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	Disponibilidad
		Fugas en las cañerías de agua	[N.2] Daños por agua	Disponibilidad
		Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	Disponibilidad
		Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	Disponibilidad
		Destrucción de los equipos de forma deliberada.	[A.26] Ataque destructivo	Disponibilidad
	[ac]	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	Disponibilidad
		Destrucción de los equipos de forma deliberada.	[A.26] Ataque destructivo	Disponibilidad

Anexo VI

Valoración de las amenazas

Activos de Hardware

Activo	Vulnerabilidad	Amenaza	Degradación	Probabilidad de ocurrencia	Justificación
AHW_01	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	2	3	Falta de mantenimientos a las instalaciones eléctricas dentro de la organización.
	Fugas en las cañerías de agua.	[N.2] Daños por agua	2	2	Falta de mantenimientos a las cañerías de agua dentro de la organización.
	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	3	5	Fallas en los componentes electrónicos por descargas

					eléctricas. Falla de los componentes internos por obsolescencia. Fallas de origen de fábrica.
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	3	8	Falta de mantenimientos a las instalaciones eléctricas dentro de la organización.
	Mala manipulación, transporte, etc., de los equipos	[E.1] Errores de los usuarios	1	5	No existe una guía del procedimiento a seguir, procedimientos ad hoc, manejo inadecuado de los procesos.
	Mala manipulación, transporte, configuración, etc., de los equipos	[E.2] Errores del administrador	2	3	No existe una guía del procedimiento a seguir, procedimientos ad hoc, manejo inadecuado de los procesos.
	Mala manipulación, transporte, configuración, etc., de los equipos	[E.23] Errores de mantenimiento/ actualización de equipos (hardware)	2	3	No existe una guía del procedimiento a seguir, ni las herramientas necesarias para realizar los mantenimientos, manipulación

					errónea del hardware.
	No contar con un inventario de activos y de custodios actualizado	[E.25] Perdida de equipos	2	5	No existe un inventario actualizado de los equipos con los que cuenta la organización, ni cuales han sido los custodios, hay equipos que no cuentan con un código de barras o se encuentran apilados en la bodega.
	Utilizar los activos asignados para realizar otras tareas.	[A.7] Uso no previsto	5	8	Existe personal que todavía se encuentra en formación académica y los equipos son usados para realizar tareas, enviar archivos, etc.
	Ingresar a los equipos de la organización sin previo aviso o autorización.	[A.11] Acceso no autorizado	2	8	Al ser una empresa familiar, entran y salen familiares de los dueños en diferentes horarios del día y en algún momento pueden ingresar a los

					equipos sin que se tenga previo conocimiento.
	Cambio de partes o piezas sin previo aviso o autorización.	[A.23] Manipulación de los equipos	2	2	El personal previo la autorización de los directivos de la empresa pueden llevarse los equipos de desarrollo a la casa, pero al momento de regresar a la empresa se desconoce si los equipos fueron o no cambiada alguna pieza o parte.
	Robo de los equipos de desarrollo.	[A.25] Robo	9	2	El personal previo la autorización de los directivos de la empresa pueden llevarse los equipos de desarrollo a la casa y pueden ser víctimas de la delincuencia.
	Fallo en el servicio de Internet	[I.8] Fallo de servicios de telecomunicaciones	5	8	Problemas con el servicio de internet, la conexión se vuelve lenta, no permite conectarse a la red

					Wifi, se llama al proveedor de servicio, entregan una solución momentánea y el servicio vuelve a fallar.
AHW_02	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	2	3	Falta de mantenimientos a las instalaciones eléctricas dentro de la organización.
	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	3	5	Fallas en los componentes electrónicos por descargas eléctricas. Falla de los componentes internos por obsolescencia.
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	3	8	Falta de mantenimientos a las instalaciones eléctricas dentro de la organización.
	Mala manipulación, transporte, etc., de los equipos	[E.1] Errores de los usuarios	1	5	No existe una guía del procedimiento a seguir, procedimientos ad hoc, manejo inadecuado de los procesos.
	No contar con un inventario de	[E.25] Perdida de equipos	2	5	No existe un inventario

	activos y de custodios actualizado				actualizado de los equipos con los que cuenta la organización, ni cuales han sido los custodios, hay equipos que no cuentan con un código de barras o se encuentran apilados en la bodega.
	Procesos que ocupan grandes recursos de procesamiento en procesador, memoria y disco.	[E.24] Caída del sistema por agotamiento de recursos	8	9	Al utilizar diferentes módulos y procesos del ERP tiende a consumir gran cantidad de recursos y el servidor de aplicaciones colapsa.
AHW_03	Ingresar a los equipos de la organización sin previo aviso o autorización.	[A.11] Acceso no autorizado	2	8	Al ser una empresa familiar, entran y salen familiares de los dueños en diferentes horarios del día y en algún momento pueden ingresar a los equipos sin que se tenga previo conocimiento.

	Fallo en el servicio de Internet	[I.8] Fallo de servicios de telecomunicaciones	5	8	Problemas con el servicio de internet, la conexión se vuelve lenta, no permite conectarse a la red Wifi, se llama al proveedor de servicio, entregan una solución momentánea y el servicio vuelve a fallar.

Activos de Software

Activo	Vulnerabilidad	Amenaza	Degradación	Probabilidad de ocurrencia	Justificación
ASW_01	Errores de fábrica de los componentes electrónicos.	[I.5] Avería de origen físico o lógico	3	5	Fallas en los componentes electrónicos por descargas eléctricas. Falla de los componentes internos por obsolescencia.
ASW_02	Ingreso erróneo de información, claves de acceso a la vista.	[E.1] Errores de los usuarios	1	5	Claves de acceso a la vista, contraseñas sencillas, equipos sin contraseña

ASW_03	Claves de acceso comprometidas, configuración de puertos de acceso por defecto.	[E.2] Errores del administrador	2	5	Mala manipulación de los equipos.
	No existe una política de cual es procedimiento para seguir.	[E.20] Errores de mantenimiento/ actualización de programas (software)	5	5	Personal poco capacitado.
	Compartición de archivos infectos.	[E.8] Difusión de software dañino	8	9	Falta de contratar el servicio de antivirus. Falta de configuración de acceso a páginas y sitios web dentro de la organización.
ASW_04	Actualización del código fuente en el SVN.	[E.15] Alteración accidental de la información	9	8	No trabajar con los últimos fuentes que se encuentran en el SVN.
	Copias no autorizadas del código fuente.	[E.19] Fugas de información	9	2	Personal poco capacitado. Falta de políticas internas sobre cual es tratamiento y confidencialidad de la información.
	A presar de que existe un framework de trabajo se aplican malas prácticas de desarrollo.	[E.20] Vulnerabilidades de los programas (software)	8	8	Personal poco capacitado. Malas prácticas de programación. La no aplicación de

					una metodología de desarrollo.
	Errores en la configuración de seguridad, contraseñas por defecto y no encriptadas.	[A.5] Suplantación de identidad	9	5	Falta de políticas de acceso y configuración a los servidores.
	Ingreso de código malicioso para fines lucrativos o poco éticos.	[A.7] Uso no previsto	2	2	Personal poco capacitado. Ocultamiento de código fuente. Falta de principios éticos por parte de empleados de la organización.
	Errores en la configuración de seguridad, contraseñas por defecto y no encriptadas.	[A.15] Modificación deliberada de la información	9	2	Falta de políticas de seguridad de control y acceso a los equipos dentro de la organización.
	Ingreso de código malicioso para borrar trazabilidad de acciones en los sistemas.	[A.18] Destrucción de la información	10	2	Falta de capacitación al personal sobre las consecuencias que conlleva el borrar información.
	Falta de controles de acceso, perfiles y grupos de usuarios.	[A.19] Divulgación de la información	10	2	Personal poco capacitado. Procesos poco normados.

	Robo de información como claves de acceso, cuentas bancarias, etc.	[A.22] Manipulación de programas	10	2	Al trabajar con un ERP, se cuenta con información de empleados, clientes, proveedores que si no existe un control de las personas que acceden a la información de la base de datos.

Activos de Información

Activo	Vulnerabilidad	Amenaza	Degradación	Probabilidad de ocurrencia	Justificación
AD_01	Falla en los procesos de copia de la información, errores.	[I.5] Avería de origen físico o lógico	3	5	Fallas en los componentes electrónicos por descargas eléctricas. Falla de los componentes

					internos por obsolescencia.
	Falla en los componentes electrónicos de las unidades de almacenamiento.	[I.5] Avería de origen físico o lógico	3	5	Fallas en los componentes electrónicos por descargas eléctricas. Falla de los componentes internos por obsolescencia.
	Procesos ad hoc	[E.1] Errores de los usuarios	1	5	No existe una guía del procedimiento a seguir normados dentro de la organización.
	No existe una política clara de cual es procedimiento para seguir.	[E.2] Errores del administrador	2	5	Mala manipulación de los equipos.
	Gestión deficiente al momento de almacenar los logs de los sistemas.	[E.3] Errores de monitorización	9	5	Falta de una política de cuál va a ser el tratamiento de los logs en los diferentes servidores.
	No existe un correcto control de personas que tienen acceso a las bases de datos.	[E.15] Alteración accidental de la información	9	2	Política no existente sobre las personas que tienes acceso a las bases de datos de pruebas y producción.
	Falta de un control de registro de las transacciones que	[E.18] Destrucción de información	9	5	Personal poco capacitado. Falta de control del

	se dan en las bases de datos.				personal que acceden a las bases de datos de pruebas o producción.
	Falta de un control de registro de las transacciones que se dan en las bases de datos.	[A.18] Destrucción de la información	10	5	Falta de control de acceso de las personas que ingresan scripts en las bases de datos.
	Robo de información de clientes y proveedores.	[A.19] Divulgación de la información	10	5	Falta de control interno del personal que tiene acceso a las bases de datos e información relevante de clientes y/o proveedores.
AD_02	No existe una política clara de cual es procedimiento para seguir.	[E.2] Errores del administrador	2	5	Mala manipulación de los equipos.
	No existe un correcto control de personas que tienen acceso a las bases de datos.	[E.15] Alteración accidental de la información	9	2	Política no existente sobre las personas que tienes acceso a las bases de datos de pruebas y producción.
	Falta de un control de registro de las transacciones que se dan en las bases de datos.	[A.18] Destrucción de la información	10	5	Falta de control de acceso de las personas que ingresan scripts en las bases de datos.
	Copias de los backups sin previa autorización.	[A.6] Abuso de privilegios de acceso	8	2	La no existencia de políticas almacenamiento,

					responsabilidades y bitácora de copia de backups dentro de la organización.
AD_03	Falta de una política clara sobre el manejo y cambio de contraseñas y puertos de acceso.	[A.5] Suplantación de identidad	9	5	Falta de políticas de acceso y configuración a los servidores.
AD_04	Falla en los procesos de copia de la información, errores.	[I.5] Avería de origen físico o lógico	3	5	Fallas en los componentes electrónicos por descargas eléctricas. Falla de los componentes internos por obsolescencia.
	Robo de información del código fuente.	[A.19] Divulgación de la información	10	5	Contraseñas de acceso a la vista, uso de unidades de almacenamiento externo, copias no autorizadas.

Activos de Personal

Activo	**Vulnerabilidad**	**Amenaza**	**Degradación**	**Probabilidad de ocurrencia**	**Justificación**
AP_01 AP_02	Roles no definidos dentro de la organización.	[E.7] Deficiencia en la organización	2	2	Falta de personal en diferentes áreas dentro de la organización.
	Políticas internas pocos definidas.	[E.19] Fugas de información	9	2	Personal poco capacitado.

					Falta de políticas internas sobre cual es tratamiento y confidencialidad de la información.
	Personal poco motivado o con exceso de carga laboral.	[E.28] Indisponibilidad del personal	9	5	Personal con exceso de carga laboral. Atrasos en los pagos mes a mes. Personal que ocupa otra área ajena a su formación.
	Amenazas para la entrega de información a terceros.	[A.29] Extorsión	9	2	Amenazas hacia los empleados de la organización para la entrega de documentación sensible almacenada en las bases de datos.
	Robo de información, claves de acceso.	[A.30] Ingeniería Social	9	2	Divulgación de información delicada o de suma importancia en conversaciones fuera de la organización.

Activos de soportes de información

Activo	Vulnerabilidad	Amenaza	Degradación	Probabilidad de ocurrencia	Justificación
AMEDIA_01 **AMEDIA_02**	Falta de mantenimiento en	[N.1] Fuego	2	3	Falta de mantenimientos a las instalaciones

	las instalaciones eléctricas.				eléctricas dentro de la organización.
	Caídas inintencionales de agua	[N.2] Daños por agua	2	2	Falta de mantenimientos a las cañerías de agua dentro de la organización.
	Fallas en los componentes electrónicos de los equipos.	[I.5] Avería de origen físico o lógico	3	5	Fallas en los componentes electrónicos por descargas eléctricas. Falla de los componentes internos por obsolescencia.
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	3	8	Cortes de energía eléctrica por eventos ajenos a la organización (Accidentes, mantenimientos programados, etc.)
	Fallas en los componentes electrónicos de los equipos.	[I.10] Degradación de los soportes de almacenamiento de la información	8	5	Falla en los componentes electrónicos internos de los equipos.
	Mala manipulación de los equipos.	[E.1] Errores de los usuarios	1	5	Personal poco capacitado. Errores involuntarios.

	Formateo o pérdida total de la información.	[E.18] Destrucción de información	9	5	Personal poco capacitado. Errores involuntarios.
	Política poco clara sobre las unidades de almacenamiento dentro de la organización.	[E.19] Fugas de información	9	2	Falta de control de las unidades de almacenamiento externo del personal dentro de la organización.
	Robo de las unidades de almacenamiento.	[E.25] Perdida de equipos	2	5	No existe un inventario actualizado de los equipos con los que cuenta la organización, ni cuales han sido los custodios, hay equipos que no cuentan con un código de barras o se encuentran apilados en la bodega.
	Uso de las unidades de almacenamiento para otros fines (música, videos, fotos, etc.)	[A.7] Uso no previsto	5	9	No se controla el uso de unidades de almacenamiento dentro de la organización y acceso a la red.
	Destrucción de las unidades de almacenamiento.	[A.18] Destrucción de la información	10	2	Unidades de almacenamiento defectuosas.

	Política poco clara sobre las unidades de almacenamiento dentro de la organización.	[A.19] Divulgación de la información	10	8	Falta de políticas internas sobre el manejo de unidades de almacenamiento externas dentro de la organización.
	Robo de las unidades de almacenamiento.	[A.25] Robo	9	2	No se controla las personas que se llevan o no las unidades de almacenamiento.
	Destrucción deliberada de las unidades de almacenamiento.	[A.26] Ataque destructivo	9	2	Mala manipulación de los equipos.

Activos de equipos Auxiliares

Activo	Vulnerabilidad	Amenaza	Degradación	Probabilidad de ocurrencia	Justificación
AAUX_01	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	2	3	Falta de mantenimientos a las instalaciones eléctricas dentro de la organización.
	Fugas en las cañerías de agua	[N.2] Daños por agua	2	2	Falta de mantenimientos a las cañerías de agua dentro de la organización.
	Fallas en los componentes	[I.5] Avería de origen físico o lógico	3	5	Fallas en los componentes electrónicos por

	electrónicos internos.				descargas eléctricas. Falla de los componentes internos por obsolescencia.
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	3	8	Cortes de energía eléctrica por eventos ajenos a la organización (Accidentes, mantenimientos programados, etc.)
	Destrucción de los equipos de forma deliberada.	[A.26] Ataque destructivo	9	2	Mala manipulación de los equipos.
AAUX_02	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	3	5	Fallas en los componentes electrónicos por descargas eléctricas. Falla de los componentes internos por obsolescencia.
	Destrucción de los equipos de forma deliberada.	[A.26] Ataque destructivo	9	2	Mala manipulación de los equipos.

Anexo VII

Valoración del impacto

Activos de Hardware

Activo	Vulnerabilidad	Amenaza	Valoración impacto				Magnitud del impacto			
			[C]	[I]	[D]	Prom	[C]	[I]	[D]	Prom
AHW_01	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	2	5	5	4,00	[B]	[M]	[M]	[M]
	Fugas en las cañerías de agua.	[N.2] Daños por agua	2	5	5	4,00	[B]	[M]	[M]	[M]
	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	8	8	8	8,00	[A]	[A]	[A]	[A]
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	3	2	5	3,33	[M]	[B]	[M]	[M]
	Mala manipulación, transporte, etc., de los equipos	[E.1] Errores de los usuarios	5	8	5	6,00	[M]	[A]	[M]	[A]
	Mala manipulación, transporte, configuración, etc., de los equipos	[E.2] Errores del administrador	5	5	2	4,00	[M]	[M]	[B]	[M]
	Mala manipulación, transporte, configuración, etc., de los equipos	[E.23] Errores de mantenimiento/	6	8	8	7,33	[A]	[A]	[A]	[A]

		actualización de equipos (hardware)								
	No contar con un inventario de activos y de custodios actualizado	[E.25] Perdida de equipos	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Utilizar los activos asignados para realizar otras tareas.	[A.7] Uso no previsto	5	5	5	5,00	[M]	[M]	[M]	[M]
	Ingresar a los equipos de la organización sin previo aviso o autorización.	[A.11] Acceso no autorizado	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Cambio de partes o piezas sin previo aviso o autorización.	[A.23] Manipulación de los equipos	5	6	8	6,33	[M]	[A]	[A]	[A]
	Robo de los equipos de desarrollo.	[A.25] Robo	3	2	2	2,33	[M]	[B]	[B]	[B]
	Fallo en el servicio de Internet	[I.8] Fallo de servicios de telecomunicaciones	0	0	5	1,67	[D]	[D]	[M]	[B]
AHW_02	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	2	5	5	4,00	[B]	[M]	[M]	[M]
	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	8	8	8	8,00	[A]	[A]	[A]	[A]
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	3	2	5	3,33	[M]	[B]	[M]	[M]

	Mala manipulación, transporte, etc., de los equipos	[E.1] Errores de los usuarios	5	8	5	6,00	[M]	[A]	[M]	[A]
	No contar con un inventario de activos y de custodios actualizado	[E.25] Perdida de equipos	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Procesos que ocupan grandes recursos de procesamiento en procesador, memoria y disco.	[E.24] Caída del sistema por agotamiento de recursos	8	10	10	9,33	[A]	[E]	[E]	[MA]
AHW_03	Ingresar a los equipos de la organización sin previo aviso o autorización.	[A.11] Acceso no autorizado	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Fallo en el servicio de Internet	[I.8] Fallo de servicios de telecomunicaciones	0	0	5	1,67	[D]	[D]	[M]	[B]

Activos de Software

Activo	**Vulnerabilidad**	**Amenaza**	**Valoración impacto**				**Magnitud del impacto**			
			[C]	**[I]**	**[D]**	**Prom**	**[C]**	**[I]**	**[D]**	**Prom**
ASW_01	Errores de fábrica de los	[I.5] Avería de origen físico o lógico	8	8	8	8,00	[A]	[A]	[A]	[A]

	componentes electrónicos.									
ASW_02	Ingreso erróneo de información, claves de acceso a la vista.	[E.1] Errores de los usuarios	5	8	5	6,00	[M]	[A]	[M]	[A]
ASW_03	Claves de acceso comprometidas, configuración de puertos de acceso por defecto.	[E.2] Errores del administrador	5	5	2	4,00	[M]	[M]	[B]	[M]
	No existe una política de cuales es procedimiento para seguir.	[E.20] Errores de mantenimiento/ actualización de programas (software)	5	8	8	7,00	[M]	[A]	[A]	[A]
	Compartición de archivos infectos.	[E.8] Difusión de software dañino	8	8	10	8,67	[A]	[A]	[E]	[MA]
ASW_04	Actualización del código fuente en el SVN.	[E.15] Alteración accidental de la información	5	9	9	7,67	[M]	[MA]	[MA]	[A]
	Copias no autorizadas del código fuente.	[E.19] Fugas de información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	A presar de que existe un framework de	[E.20] Vulnerabilidades de los	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]

	trabajo se aplican malas prácticas de desarrollo.	programas (software)								
	Errores en la configuración de seguridad, contraseñas por defecto y no encriptadas.	[A.5] Suplantación de identidad	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Ingreso de código malicioso para fines lucrativos o poco éticos.	[A.7] Uso no previsto	5	5	5	5,00	[M]	[M]	[M]	[M]
	Errores en la configuración de seguridad, contraseñas por defecto y no encriptadas.	[A.15] Modificación deliberada de la información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Ingreso de código malicioso para borrar trazabilidad de acciones en los sistemas.	[A.18] Destrucción de la información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Falta de controles de acceso, perfiles y grupos de usuarios.	[A.19] Divulgación de la información	9	9	5	7,67	[MA]	[MA]	[M]	[A]

	Robo de información como claves de acceso, cuentas bancarias, etc.	[A.22] Manipulación de programas	9	8	3	6,67	[MA]	[A]	[M]	[A]

Activos de Información

Activo	Vulnerabilidad	Amenaza	Valoración impacto				Magnitud del impacto			
			[C]	**[I]**	**[D]**	**Prom**	**[C]**	**[I]**	**[D]**	**Prom**
AD_01	Falla en los procesos de copia de la información, errores.	[I.5] Avería de origen físico o lógico	8	8	8	8,00	[A]	[A]	[A]	[A]
	Falla en los componentes electrónicos de las unidades de almacenamiento.	[I.5] Avería de origen físico o lógico	8	8	8	8,00	[A]	[A]	[A]	[A]
	Procesos ad hoc	[E.1] Errores de los usuarios	8	8	8	8,00	[A]	[A]	[A]	[A]
	No existe una política clara de cual es procedimiento para seguir.	[E.2] Errores del administrador	5	5	2	4,00	[M]	[M]	[B]	[M]

	Gestión deficiente al momento de almacenar los logs de los sistemas.	[E.3] Errores de monitorización	5	9	9	7,67	[M]	[MA]	[MA]	[A]
	No existe un correcto control de personas que tienen acceso a las bases de datos.	[E.15] Alteración accidental de la información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Falta de un control de registro de las transacciones que se dan en las bases de datos.	[E.18] Destrucción de información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Falta de un control de registro de las transacciones que se dan en las bases de datos.	[A.18] Destrucción de la información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Robo de información de clientes y proveedores.	[A.19] Divulgación de la información	9	9	5	7,67	[MA]	[MA]	[M]	[A]
AD_02	No existe una política clara de cual es procedimiento para seguir.	[E.2] Errores del administrador	5	5	2	4,00	[M]	[M]	[B]	[M]
	No existe un correcto control	[E.15] Alteración	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]

	de personas que tienen acceso a las bases de datos.	accidental de la información								
	Falta de un control de registro de las transacciones que se dan en las bases de datos.	[A.18] Destrucción de la información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Copias de los backups sin previa autorización.	[A.6] Abuso de privilegios de acceso	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
AD_03	Falta de una política clara sobre el manejo y cambio de contraseñas y puertos de acceso.	[A.5] Suplantación de identidad	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
AD_04	Falla en los procesos de copia de la información, errores.	[I.5] Avería de origen físico o lógico	8	8	8	8,00	[A]	[A]	[A]	[A]
	Robo de información del código fuente.	[A.19] Divulgación de la información	9	9	5	7,67	[MA]	[MA]	[M]	[A]

Activos de Personal

Activo	Vulnerabilidad	Amenaza	Valoración impacto				Magnitud del impacto			
			[C]	[I]	[D]	Prom	[C]	[I]	[D]	Prom
AP_01 AP_02	Roles no definidos dentro de la organización.	[E.7] Deficiencia en la organización	8	5	5	6,00	[A]	[M]	[M]	[A]
	Políticas internas pocos definidas.	[E.19] Fugas de información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Personal poco motivado o con exceso de carga laboral.	[E.28] Indisponibilidad del personal	8	9	9	8,67	[A]	[MA]	[MA]	[MA]
	Amenazas para la entrega de información a terceros.	[A.29] Extorsión	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Robo de información, claves de acceso.	[A.30] Ingeniería Social	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]

Activos de soportes de información

Activo	Vulnerabilidad	Amenaza	Valoración impacto				Magnitud del impacto			
			[C]	[I]	[D]	Prom	[C]	[I]	[D]	Prom
AMEDIA_01 AMEDIA_02	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	2	5	5	4,00	[B]	[M]	[M]	[M]
	Caídas inintencionales de agua	[N.2] Daños por agua	2	5	5	4,00	[B]	[M]	[M]	[M]
	Fallas en los componentes electrónicos de los equipos.	[I.5] Avería de origen físico o lógico	8	8	8	8,00	[A]	[A]	[A]	[A]
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	3	2	5	3,33	[M]	[B]	[M]	[M]
	Fallas en los componentes electrónicos de los equipos.	[I.10] Degradación de los soportes de almacenamiento de la información	8	8	8	8,00	[A]	[A]	[A]	[A]
	Mala manipulación de los equipos.	[E.1] Errores de los usuarios	5	3	6	4,67	[M]	[M]	[A]	[M]
	Formateo o pérdida total de la información.	[E.18] Destrucción de información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]

	Política poco clara sobre las unidades de almacenamiento dentro de la organización.	[E.19] Fugas de información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Robo de las unidades de almacenamiento.	[E.25] Perdida de equipos	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Uso de las unidades de almacenamiento para otros fines (música, videos, fotos, etc.)	[A.7] Uso no previsto	5	5	5	5,00	[M]	[M]	[M]	[M]
	Destrucción de las unidades de almacenamiento.	[A.18] Destrucción de la información	9	9	9	9,00	[MA]	[MA]	[MA]	[MA]
	Política poco clara sobre las unidades de almacenamiento dentro de la organización.	[A.19] Divulgación de la información	9	9	5	7,67	[MA]	[MA]	[M]	[A]
	Robo de las unidades de almacenamiento.	[A.25] Robo	3	2	2	2,33	[M]	[B]	[B]	[B]
	Destrucción deliberada de las unidades	[A.26] Ataque destructivo	9	9	5	7,67	[MA]	[MA]	[M]	[A]

	de almacenamiento.									

Activos de equipos Auxiliares

Activo	Vulnerabilidad	Amenaza	Valoración impacto				Magnitud del impacto			
			[C]	[I]	[D]	Prom	[C]	[I]	[D]	Prom
AAUX_01	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	2	5	5	4,00	[B]	[M]	[M]	[M]
	Fugas en las cañerías de agua	[N.2] Daños por agua	2	5	5	4,00	[B]	[M]	[M]	[M]
	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	8	8	8	8,00	[A]	[A]	[A]	[A]
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	3	2	5	3,33	[M]	[B]	[M]	[M]
	Destrucción de los equipos de forma deliberada.	[A.26] Ataque destructivo	9	9	5	7,67	[MA]	[MA]	[M]	[A]

AAUX_02	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	8	8	8	8,00	[A]	[A]	[A]	[A]
	Destrucción de los equipos de forma deliberada.	[A.26] Ataque destructivo	9	9	5	7,67	[MA]	[MA]	[M]	[A]

Anexo VIII

Valoración del riesgo por degradación y probabilidad de ocurrencia

Activos de Hardware

Activo	Vulnerabilidad	Amenaza	Valoración				Magnitud		
			Degradación	Probabilidad	Total	Probabilidad de ocurrencia	Degradación	Probabilidad	Probabilidad de ocurrencia
AHW_01	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	3	2	5	2	[M]	[B]	[B]
	Fugas en las cañerías de agua.	[N.2] Daños por agua	2	2	4	2	[B]	[B]	[B]
	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	8	5	13	5	[A]	[M]	[M]
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	8	8	16	8	[A]	[A]	[A]
	Mala manipulación, transporte, etc., de los equipos	[E.1] Errores de los usuarios	5	8	13	8	[M]	[A]	[A]
	Mala manipulación, transporte, configuración, etc., de los equipos	[E.2] Errores del administrador	5	8	13	8	[M]	[A]	[A]
	Mala manipulación, transporte, configuración, etc., de los equipos	[E.23] Errores de mantenimiento/ actualización de	8	8	16	8	[A]	[A]	[A]

		equipos (hardware)							
	No contar con un inventario de activos y de custodios actualizado	[E.25] Perdida de equipos	8	2	10	2	[A]	[B]	[B]
	Utilizar los activos asignados para realizar otras tareas.	[A.7] Uso no previsto	8	8	16	8	[A]	[A]	[A]
	Ingresar a los equipos de la organización sin previo aviso o autorización.	[A.11] Acceso no autorizado	2	5	7	5	[B]	[M]	[M]
	Cambio de partes o piezas sin previo aviso o autorización.	[A.23] Manipulación de los equipos	8	2	10	2	[A]	[B]	[B]
	Robo de los equipos de desarrollo.	[A.25] Robo	8	2	10	2	[A]	[B]	[B]
	Fallo en el servicio de Internet	[I.8] Fallo de servicios de telecomunicaciones	9	9	18	9	[MA]	[MA]	[MA]
AHW_02	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	3	2	5	2	[M]	[B]	[B]
	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	8	5	13	5	[A]	[M]	[M]
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	8	8	16	8	[A]	[A]	[A]
	Mala manipulación, transporte, etc., de los equipos	[E.1] Errores de los usuarios	5	8	13	8	[M]	[A]	[A]

	No contar con un inventario de activos y de custodios actualizado	[E.25] Perdida de equipos	8	2	10	2	[A]	[B]	[B]
	Procesos que ocupan grandes recursos de procesamiento en procesador, memoria y disco.	[E.24] Caída del sistema por agotamiento de recursos	10	8	18	8	[E]	[A]	[A]
AHW_03	Ingresar a los equipos de la organización sin previo aviso o autorización.	[A.11] Acceso no autorizado	2	5	7	5	[B]	[M]	[M]
	Fallo en el servicio de Internet	[I.8] Fallo de servicios de telecomunicaciones	9	9	18	9	[MA]	[MA]	[MA]

Activos de Software

Activo	**Vulnerabilidad**	**Amenaza**	**Valoración**				**Magnitud**		
			Degradación	**Probabilidad**	**Total**	**Probabilidad de ocurrencia**	**Degradación**	**Probabilidad**	**Probabilidad de ocurrencia**
ASW_01	Errores de fábrica de los componentes electrónicos.	[I.5] Avería de origen físico o lógico	8	5	13	5	[A]	[M]	[M]
ASW_02	Ingreso erróneo de información, claves de acceso a la vista.	[E.1] Errores de los usuarios	5	8	13	8	[M]	[A]	[A]

ASW_03	Claves de acceso comprometidas, configuración de puertos de acceso por defecto.	[E.2] Errores del administrador	5	8	13	8	[M]	[A]	[A]
	No existe una política de cual es procedimiento para seguir.	[E.20] Errores de mantenimiento / actualización de programas (software)	5	5	10	5	[M]	[M]	[M]
	Compartición de archivos infectos.	[E.8] Difusión de software dañino	0	2	2	2	[D]	[B]	[B]
ASW_04	Actualización del código fuente en el SVN.	[E.15] Alteración accidental de la información	5	8	13	8	[M]	[A]	[A]
	Copias no autorizadas del código fuente.	[E.19] Fugas de información	8	2	10	2	[A]	[B]	[B]
	A presar de que existe un framework de trabajo se aplican malas prácticas de desarrollo.	[E.20] Vulnerabilidades de los programas (software)	8	8	16	8	[A]	[A]	[A]
	Errores en la configuración de seguridad,	[A.5] Suplantación de identidad	5	2	7	2	[M]	[B]	[B]

	contraseñas por defecto y no encriptadas.								
	Ingreso de código malicioso para fines lucrativos o poco éticos.	[A.7] Uso no previsto	8	2	10	2	[A]	[B]	[B]
	Errores en la configuración de seguridad, contraseñas por defecto y no encriptadas.	[A.15] Modificación deliberada de la información	8	5	13	5	[A]	[M]	[M]
	Ingreso de código malicioso para borrar trazabilidad de acciones en los sistemas.	[A.18] Destrucción de la información	8	5	13	5	[A]	[M]	[M]
	Falta de controles de acceso, perfiles y grupos de usuarios.	[A.19] Divulgación de la información	9	8	17	8	[MA]	[A]	[A]
	Robo de información como claves de acceso,	[A.22] Manipulación de programas	8	2	10	2	[A]	[B]	[B]

	cuentas bancarias, etc.								

Activos de Información

Activo	Vulnerabilidad	Amenaza	Valoración				Magnitud		
			Degradación	Probabilidad	Total	Probabilidad de ocurrencia	Degradación	Probabilidad	Probabilidad de ocurrencia
AD_01	Falla en los procesos de copia de la información, errores.	[I.5] Avería de origen físico o lógico	8	5	13	5	[A]	[M]	[M]
	Falla en los componentes electrónicos de las unidades de almacenamiento.	[I.5] Avería de origen físico o lógico	8	5	13	5	[A]	[M]	[M]
	Procesos ad hoc	[E.1] Errores de los usuarios	5	8	13	8	[M]	[A]	[A]
	No existe una política clara de cual es procedimiento para seguir.	[E.2] Errores del administrador	5	8	13	8	[M]	[A]	[A]
	Gestión deficiente al momento de almacenar los	[E.3] Errores de monitorización	8	5	13	5	[A]	[M]	[M]

	logs de los sistemas.								
	No existe un correcto control de personas que tienen acceso a las bases de datos.	[E.15] Alteración accidental de la información	5	2	7	2	[M]	[B]	[B]
	Falta de un control de registro de las transacciones que se dan en las bases de datos.	[E.18] Destrucción de información	8	2	10	2	[A]	[B]	[B]
	Falta de un control de registro de las transacciones que se dan en las bases de datos.	[A.18] Destrucción de la información	8	5	13	5	[A]	[M]	[M]
	Robo de información de clientes y proveedores.	[A.19] Divulgación de la información	9	8	17	8	[MA]	[A]	[A]
AD_02	No existe una política clara de cual es procedimiento para seguir.	[E.2] Errores del administrador	5	8	13	8	[M]	[A]	[A]
	No existe un correcto control de personas que tienen acceso a	[E.15] Alteración accidental de	5	2	7	2	[M]	[B]	[B]

	las bases de datos.	la información							
	Falta de un control de registro de las transacciones que se dan en las bases de datos.	[A.18] Destrucción de la información	8	5	13	5	[A]	[M]	[M]
	Copias de los backups sin previa autorización.	[A.6] Abuso de privilegios de acceso	5	2	7	2	[M]	[B]	[B]
AD_03	Falta de una política clara sobre el manejo y cambio de contraseñas y puertos de acceso.	[A.5] Suplantación de identidad	5	2	7	2	[M]	[B]	[B]
AD_04	Falla en los procesos de copia de la información, errores.	[I.5] Avería de origen físico o lógico	8	5	13	5	[A]	[M]	[M]
	Robo de información del código fuente.	[A.19] Divulgación de la información	9	8	17	8	[MA]	[A]	[A]

Activos de Personal

		Amenaza	**Valoración**	**Magnitud**

Activo	Vulnerabilidad		Degradación	Probabilidad	Total	Probabilidad de ocurrencia	Degradación	Probabilidad	Probabilidad de ocurrencia
AP_01 AP_02	Roles no definidos dentro de la organización.	[E.7] Deficiencia en la organización	8	8	16	8	[A]	[A]	[A]
	Políticas internas pocos definidas.	[E.19] Fugas de información	8	5	13	5	[A]	[M]	[M]
	Personal poco motivado o con exceso de carga laboral.	[E.28] Indisponibilidad del personal	8	8	16	8	[A]	[A]	[A]
	Amenazas para la entrega de información a terceros.	[A.29] Extorsión	0	1	1	1	[D]	[B]	[B]
	Robo de información, claves de acceso.	[A.30] Ingeniería Social	0	2	2	2	[D]	[B]	[B]

Activos de soportes de información

Activo	Vulnerabilidad	Amenaza	Valoración				Magnitud		
			Degradación	Probabilidad	Total	Probabilidad de ocurrencia	Degradación	Probabilidad	Probabilidad de ocurrencia

	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	3	2	5	2	[M]	[B]	[B]
	Caídas inintencionales de agua	[N.2] Daños por agua	2	2	4	2	[B]	[B]	[B]
	Fallas en los componentes electrónicos de los equipos.	[I.5] Avería de origen físico o lógico	8	5	13	5	[A]	[M]	[M]
AMEDIA_01 AMEDIA_02	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	8	8	16	8	[A]	[A]	[A]
	Fallas en los componentes electrónicos de los equipos.	[I.10] Degradación de los soportes de almacenamiento de la información	5	5	10	5	[M]	[M]	[M]
	Mala manipulación de los equipos.	[E.1] Errores de los usuarios	5	8	13	8	[M]	[A]	[A]
	Formateo o pérdida total de la información.	[E.18] Destrucción de información	8	2	10	2	[A]	[B]	[B]

	Política poco clara sobre las unidades de almacenamiento dentro de la organización.	[E.19] Fugas de información	8	8	16	8	[A]	[A]	[A]
	Robo de las unidades de almacenamiento.	[E.25] Perdida de equipos	8	2	10	2	[A]	[B]	[B]
	Uso de las unidades de almacenamiento para otros fines (música, videos, fotos, etc.)	[A.7] Uso no previsto	8	8	16	8	[A]	[A]	[A]
	Destrucción de las unidades de almacenamiento.	[A.18] Destrucción de la información	8	5	13	5	[A]	[M]	[M]
	Política poco clara sobre las unidades de almacenamiento dentro de la organización.	[A.19] Divulgación de la información	9	8	17	8	[MA]	[A]	[A]
	Robo de las unidades de almacenamiento.	[A.25] Robo	8	2	10	2	[A]	[B]	[B]
	Destrucción deliberada de las unidades	[A.26] Ataque destructivo	5	2	7	2	[M]	[B]	[B]

	de almacenamiento.								

Activos de equipos Auxiliares

Activo	Vulnerabilidad	Amenaza	Valoración				Magnitud		
			Degradación	Probabilidad	Total	Probabilidad de ocurrencia	Degradación	Probabilidad	Probabilidad de ocurrencia
AAUX_01	Falta de mantenimiento en las instalaciones eléctricas.	[N.1] Fuego	3	2	5	2	[M]	[B]	[B]
	Fugas en las cañerías de agua	[N.2] Daños por agua	2	2	4	2	[B]	[B]	[B]
	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	8	5	13	5	[A]	[M]	[M]
	Fallo en el abastecimiento del suministro eléctrico.	[I.6] Corte de suministro eléctrico	8	8	16	8	[A]	[A]	[A]
	Destrucción de los equipos de forma deliberada.	[A.26] Ataque destructivo	5	2	7	2	[M]	[B]	[B]

AAUX_02	Fallas en los componentes electrónicos internos.	[I.5] Avería de origen físico o lógico	8	5	13	5	[A]	[M]	[M]
	Destrucción de los equipos de forma deliberada.	[A.26] Ataque destructivo	5	2	7	2	[M]	[B]	[B]

CAPÍTULO VI

PROPUESTA

6. Datos informativos

6.1. Título

AUTOMATIZACIÓN DEL DESPLIEGUE DE APLICACIONES WEB JAVA EE EN SERVIDORES LINUX DE x64, BASADO EN LA NORMA ISO/IEC 27001:2018, UTILIZANDO CONTENEDORES DE SOFTWARE.

6.1.1. Institución

Empresas consultoras en el área de desarrollo de software de aplicaciones Java EE. Y servidore de aplicaciones Wildfly.

6.1.2. Beneficiarios

- Uno de los principales beneficiarios son los técnicos en el área de infraestructura ya que se reduce los tiempos de implementación y despliegue de aplicaciones.
- Además, se beneficia la organización ya que se aplica dentro del proceso la Norma ISO/IEC 27001 con sus diferentes controles y metodologías.

6.1.3. Ubicación

- **Provincia:** Pichincha
- **Cantón:** Quito

6.1.4. Técnico responsable

- **Investigador:** Ing. Fernando Alexander Moya Chiluiza

- **Coordinador:** Ing. Oscar Fernando Ibarra Torres Mg
- Personal técnico de las empresas consultoras.

6.2. Antecedentes de la propuesta

En la actualidad uno de los activos más importantes para todo tipo de empresa u organización es la información, lo cual la convierte en un insumo de gran utilidad para bien y para mal lo que obliga a optar por protegerla de cualquier ataque aplicando normas, protocolos, mejorando la infraestructura de red y servidores tanto físicos como en la nube, garantizando aspectos tan importantes como lo es la confidencialidad, integridad y disponibilidad.

Al no trabajar con normas o estándares dentro de una organización genera una brecha que no permite estar a la vanguardia frente a otras organizaciones, lo que conlleva no solo a perder clientes, prestigio, contratos, etc., y ante una eventualidad no existen los procedimientos necesarios para poder afrontarlos lo que se traduce en tiempo, dinero, recursos y ante todo ello es necesario trabajar crear un esquema en el cual la norma o parte de ella se encuentre estipulada con la finalidad de generar buenas prácticas a fin de generar confianza con las clientes y usuarios.

La metodología de trabajo comprende el desarrollo de aplicaciones web Java EE, un servidor de aplicaciones y un motor de bases de datos PostgreSQL en ambientes locales de desarrollo lo cual implica un ambiente ideal de pruebas, por cuestiones de interoperabilidad interna se optó por un SVN (Apache Subversion) a fin de integrar todos los desarrollos en un solo lugar, un servidor que permitan realizar pruebas pertinentes de los sistemas independientemente del equipo donde fue desarrollado.

En el servidor de pruebas coexisten VM (Máquinas virtuales) cada una configurada con diferentes recursos de memoria, disco, red y cuya principal limitación radica en que las pruebas a realizar no consuman más allá de los recursos asignados en cada VM, para reducir o amentar recursos entre VM se debe detener todos los procesos que se encuentren ejecutando lo que conlleva tiempos de espera hasta volver a tener arriba los servicios y la contratación de un nuevo servidor incurre en gastos adicionales que la organización estará o no dispuesta a invertir, además de posibles vulnerabilidades inherentes propias de la configuración inicial lo que implica aplicar normas y estándares vigentes.

Por los expuesto, surge la necesidad de aplicar la norma ISO/IEC 27001:2018 - Gestión de la seguridad de la información y nuevas tecnologías como lo son los contenedores de software que permiten realizar pruebas de implementación rápidas y continuas que en

conjunto presentarán una alternativa de solución en el trabajo del día a día optimizando tiempo, recursos y costos con la finalidad que muestre un constante crecimiento, actualización en uso de las TIC y una ventaja frente a otros competidores.

6.3. Justificación

En base al análisis inicial realizado y en conjunto con la recopilación de información permitió conocer de primera mano cual era la necesidad existente que la momento de configurar servidores de pruebas que trabajen con aplicaciones Java EE, los tiempos de implementación y despliegue tomaban una gran cantidad de tiempo en donde en un inicio se debía recopilar todos y cada uno de los instaladores y verificar que no se encuentren dañados, llevarlos en una unidad USB o acceder por medio de FTP (File Transfer Protocol) lo que conllevaba a muchos problemas de seguridad.

Otras de las dificultades encontradas es que si bien es cierto existen activos tanto físicos como de información dentro de la organización no existe un correcto manejo y control de estos, muchos de controles aplicados son de manera empírica sin una guía técnica y frente a una eventualidad el personal se encuentra poco capacitado de cuál es el procedimiento para seguir y como se debe actuar.

Entregar una solución que permita simplificar el tiempo que lleva una implementación y despliegue permitirá optimizar de mejor manera tiempo, recursos y costos, en conjunto con una serie de controles de seguridad de la información por medio de la ISO/IEC 27001 y nuevas tecnologías como lo son los contenedores de software que permiten realizar pruebas de implementación rápidas y continuas con la finalidad que muestre un constante crecimiento.

6.4. Objetivos

6.4.1. General

Optimizar el uso de recursos informáticos en un entorno de pruebas para aplicaciones Java EE usando contenedores de software aplicando controles de seguridad de la información, basado en la norma ISO/IEC 27001:2018.

6.4.2. Específicos

- Analizar la norma ISO/IEC 27001:2018 y relacionarla con el fundamento teórico para el desarrollo del proyecto.
- Investigar los diferentes ambientes de contenedores de software que trabajan en servidores Linux x64.
- Definir un ambiente de pruebas para aplicaciones Java EE basado en contenedores de software.
- Evaluar el nivel de aceptación y confianza de la propuesta de solución para caso de estudio práctico basado en la norma ISO/IEC 27001:2018.

6.5. Análisis de factibilidad

6.5.1 Factibilidad técnica:

Se cuenta con los recursos tecnológicos requeridos como lo es la infraestructura, herramientas tecnológicas, software, datos e información, además de contar con la norma que determina como gestionar la seguridad de la información.

6.5.2 Factibilidad Operativa:

Se dispone con los conocimientos del investigador, más el apoyo y apertura de la empresa consultora y el personal técnico los cuales se encuentra interesados en aplicar la solución a futuro en diferentes entornos tanto en pruebas como en producción de diferentes aplicativos Java EE.

6.5.3 Factibilidad Económica:

Este proyecto es factible económicamente ya que los costos que implican, la búsqueda, análisis, desarrollo y tiempo empleado son asumidos por parte del investigador y la empresa consultora presta los equipos tecnológicos para en análisis y pruebas.

6.6. Fundamentación

En su libro (Valencia, 2021) describe a la norma ISO/IEC 27001:2013 como un documento de 34 páginas, los requisitos se encuentran concentrados en cerca de 12 de estas páginas y el resto del documento se concentra en el Anexo A relacionado con los objetivos de control y los controles de referencia.

En el trabajo de titulación publicado por (Quiñonez Quintero, 2022), muestra que la norma ISO/IEC 27001 "a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.", para (Camacho, 2021) la Norma ISO/IEC 27001 especifica los requisitos para el diseño e implementación de un SGSI, basado en las necesidades y requerimientos de la organización.

Para (Villegas, 2019) "la norma ISO/IEC 27001 proporciona los requisitos para establecer, implementar, mantener y mejorar un SGSI basado en la integridad, disponibilidad y confidencialidad de la información en una organización".

Para (Tusa, 2021) "el poseer un inventario de activos actualizado, facilita su clasificación según el nivel de riesgo, lo que conlleva a tener mayor protección de los mismos".

Para el autor (Lucano, 2019) recomienda "mantener un apolítica de la seguridad de la información actualizada, cambiando dentro del ciclo PDCA en función a las mejoras tecnológicas, los cambios normativos de las entidades de regulación o el uso injustificado de controles en relación con el valor del activo que resguarda".

Según (Hinojosa, 2021), en su tesis de "Modelado Funcional de Contenedores Virtuales Docker", muestra que los contenedores virtuales han demostrado que son una gran opción frente al problema de la portabilidad, facilitando un desarrollo rápido y ágil de aplicaciones de software de manera fácil y uniforme independiente del entorno ya sea este un centro de datos, nube pública o privada o incluso una laptop.

Según la investigación de (Hinojosa, 2021; Javed & Toor, 2021) para el año 2020 existe un crecimiento del 40% en la adopción de uso de contenedores con una tendencia que va en aumento por la facilidad de despliegue y un desarrollo fácil y ágil. En base al número de descargas en la plataforma Docker Hub existe un crecimiento del 145% año

tras año y de un 45% en la creación de nuevas cuentas de usuario, un 40% en la creación de nuevas imágenes y un 38% en instalaciones de Docker Desktop.

Como lo mencionan (Rosero, 2019; Vergara, 2019), una aplicación web es un sistema informático con interfaces similares a las aplicaciones de escritorio al cual se puede acceder por medio de internet o una intranet gracias a su accesibilidad por medio de un navegador web, la gran facilidad de actualización y mantenimiento sin la instalación software en miles de clientes, a diferencia de un sitio web las aplicaciones web se crean en respuestas a varias necesidades y procesos de la organización.