UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE SISTEMAS

“Examen Práctico U III”

Que se presenta para el curso:

“Auditoría de sistemas”

Docente:

Dr. Oscar Juan Jimenez Flores

Estudiante:

Marjiory Grace Llantay Machaca

TACNA – PERÚ

2025

PLAN DE AUDITORÍA

AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN

EVALUACIÓN DE SEGURIDAD EN EL DESPLIEGUE CONTINUO DE WORDPRESS

CON VAGRANT Y CHEF PARA DEVIA360

Lima – Perú

- **Distrito:** Santiago de Surco
- **Provincia:** Lima
- **Departamento:** Lima

“Evaluación integral de riesgos de seguridad, eficiencia y cumplimiento en procesos automatizados de despliegue de infraestructura TI”

Lugar y fecha de aprobación:

Lima, mayo de 2025

Denominación oficial del decenio:

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

Denominación oficial del año:

“Año de la Unidad, la Paz y el Desarrollo”

1. Resumen Ejecutivo

Propósito de la Auditoría

El objetivo de esta auditoría es evaluar la seguridad, la eficiencia operativa y el cumplimiento de las mejores prácticas en el proceso de despliegue continuo automatizado de entornos WordPress, utilizando la solución Chef_Vagrant_Wp implementada por DevIA360. El análisis abarca el código fuente, los scripts de aprovisionamiento, las configuraciones declarativas y las evidencias técnicas obtenidas a partir de la replicación del entorno en un laboratorio controlado.

1.1 Alcance Técnico Resumido

- Implementación y despliegue de tres máquinas virtuales (WordPress, base de datos y proxy) dentro de la red 192.168.56.0/24 mediante el comando `vagrant up`.
- Revisión detallada de las configuraciones presentes en el archivo Vagrantfile, el archivo `.env` y los data bags de Chef, con el propósito de identificar posibles configuraciones con valores inseguros.
- Ejecución de pruebas funcionales, de integración y de infraestructura utilizando el script `tests.sh` y la herramienta Serverspec para validar el correcto funcionamiento y seguridad del entorno desplegado.

1.2 Principales Hallazgos

1. **Exposición de credenciales sensibles en texto plano** dentro de archivos de Chef (data bags, `.env`), lo que representa un riesgo alto con un puntaje de 25.
2. **Puertos abiertos sin restricciones y ausencia de un firewall** configurado en Vagrant, implicando un riesgo alto con una valoración de 20.
3. **Falta de registros de auditoría persistentes durante el proceso de aprovisionamiento**, lo que constituye un riesgo alto con una puntuación de 16.
4. **Uso de versiones obsoletas de software** (Apache, MySQL, Ruby) sin un adecuado control de parches, generando un riesgo alto evaluado en 20.

5. **Ambiente único sin segmentación adecuada entre entornos de desarrollo, prueba y producción**, lo que representa un riesgo alto con un valor de 20.
6. **Cobertura limitada de pruebas**, restringida a validaciones funcionales básicas sin incluir pruebas negativas ni de seguridad, catalogada como un riesgo medio con una puntuación de 12.

Estos hallazgos reflejan vulnerabilidades críticas en la configuración y gestión del entorno automatizado, que requieren atención prioritaria para mitigar riesgos de seguridad y operativos.

1.3 Indicadores Clave de Desempeño (KPI)

- Se identificaron 5 riesgos críticos (nivel Alto, con puntaje ≥ 20) y 1 riesgo medio según la matriz OWASP Risk Rating.
- No se incurrió en costos adicionales para licencias o herramientas, ya que se utilizaron componentes de código abierto existentes.
- El 53 % de las organizaciones con pipelines CI/CD sin controles de seguridad han reportado incidentes, según el informe *State of DevOps 2023*.
- Más del 90 % de las pruebas funcionales ejecutadas fueron exitosas; sin embargo, menos del 10 % de las pruebas abarcaron escenarios de fallo o seguridad, conforme a los resultados obtenidos mediante `tests.sh`.

---

2. Antecedentes

2.1 Contexto General de la Entidad

DevIA360 es una empresa peruana con sede en Lima dedicada al desarrollo de soluciones basadas en inteligencia artificial y servicios de transformación digital. Su portafolio incluye proyectos relacionados con presencia web, análisis de datos y automatización de procesos, orientados a clientes nacionales e internacionales de tamaño mediano.

2.2 Naturaleza de sus Sistemas de Información

El sistema objeto de auditoría corresponde a Chef_Vagrant_Wp, un conjunto integrado por scripts y recetas Chef que, junto con Vagrant, posibilitan el aprovisionamiento automático de un entorno WordPress conformado por un servidor web, una base de datos y un proxy inverso. Este sistema forma parte del pipeline de integración y despliegue continuo (CI/CD) de la organización y se emplea para el despliegue de sitios web de demostración interna y entornos de staging para clientes.

2.3 Estructura Organizativa Relevante

La organización está encabezada por la Dirección General. El Departamento de Tecnología e Innovación, liderado por el Chief Technology Officer (CTO), integra los equipos de Desarrollo, DevOps y Seguridad. El equipo DevOps tiene a su cargo la gestión de los pipelines de integración y despliegue continuo, así como el mantenimiento de las configuraciones de Vagrant y Chef. Por su parte, el equipo de Seguridad de la Información es responsable de la definición de políticas, la revisión de configuraciones y la gestión de la respuesta a incidentes.

2.4 Antecedentes de Auditorías Previas

Hasta la fecha, no se han realizado auditorías externas formales enfocadas en los procesos DevOps de DevIA360. Existen revisiones internas puntuales orientadas a evaluar el código y las buenas prácticas; sin embargo, esta auditoría representa la primera evaluación integral destinada a analizar la seguridad y el cumplimiento en el entorno Chef_Vagrant_Wp.

---

3. Objetivos de la Auditoría

3.1 Objetivo General

El objetivo principal de esta auditoría es realizar una evaluación integral de los procesos, controles y configuraciones relacionados con el entorno de despliegue continuo Chef_Vagrant_Wp de DevIA360. Esta evaluación busca determinar el nivel de seguridad, la eficiencia operativa y el grado de cumplimiento con las mejores prácticas y los requisitos normativos aplicables.

3.2 Objetivos Específicos

Se pretende verificar la seguridad de la información garantizando la confidencialidad, integridad y disponibilidad de los datos que se gestionan durante el aprovisionamiento y la operación del entorno. Además, se evaluarán los mecanismos destinados a asegurar la continuidad del negocio, incluyendo copias de seguridad, recuperación ante desastres y redundancia, con el fin de garantizar la resiliencia del servicio WordPress. Se revisará el proceso de gestión de cambios y configuraciones para asegurar que las modificaciones realizadas en los scripts Chef, el Vagrantfile y las configuraciones de infraestructura se sometan a flujos adecuados de aprobación, versionado y pruebas. Asimismo, se comprobará el cumplimiento de las normativas vigentes y la alineación con marcos de referencia reconocidos, tales como ISO 27001, ITIL 4, OWASP DevSecOps y NIST SP 800-53. También se validará la integridad y disponibilidad de los datos almacenados en la base de datos MySQL y servidos por Apache mediante pruebas de consistencia y monitoreo de rendimiento. Finalmente, se identificarán riesgos residuales y oportunidades de mejora para fortalecer la postura de seguridad y la eficiencia operativa de DevIA360.

---

4. Alcance de la Auditoría

4.1. Ámbitos evaluados

La auditoría se desarrolló abarcando cuatro dimensiones fundamentales. En el ámbito **tecnológico**, se examinó la infraestructura virtual configurada mediante Vagrant, incluyendo las recetas y cookbooks de Chef, así como la estructura técnica de los componentes que conforman el entorno WordPress: servidor web, base de datos MySQL y proxy inverso implementado con Apache o Nginx. Desde la perspectiva **organizacional**, se analizaron los procesos y funciones asignadas a los equipos DevOps y de Seguridad de la Información, especialmente en lo que respecta a las prácticas de integración y despliegue continuo, además del cumplimiento de las políticas internas en tecnologías de la información. En el ámbito **normativo**, se revisó el nivel de alineamiento con los principales marcos y estándares internacionales en materia de seguridad y gobernanza tecnológica, tales como ISO 27001, ISO 22301, ITIL 4, NIST SP 800-53 y el modelo de madurez DevSecOps de OWASP. Finalmente, en el aspecto **operativo**, se evaluaron los procedimientos vinculados al respaldo de información, gestión de incidentes y la implementación de prácticas de monitoreo y registro de eventos, durante todo el ciclo de vida del entorno tecnológico.

4.2. Sistemas y procesos incluidos

Dentro del alcance de la auditoría se consideraron diversos sistemas y flujos críticos. Se revisó principalmente el pipeline de integración y entrega continua desarrollado con Chef_Vagrant_Wp, encargado del aprovisionamiento automatizado de las máquinas virtuales para WordPress, base de datos y servidor proxy. Asimismo, se inspeccionó el repositorio de código y el sistema de control de versiones, incluyendo ramas, procesos de revisión de cambios (pull requests) y modificaciones en cookbooks, archivos Vagrantfile y scripts complementarios. También se evaluaron los mecanismos de respaldo y restauración de la base de datos MySQL, así como el almacenamiento de volúmenes utilizados por el servidor web. Complementariamente, se analizó la plataforma de monitoreo y los registros generados, los cuales permiten la supervisión de la disponibilidad del servicio, el rendimiento del sistema y posibles alertas de seguridad.

4.3. Unidades o áreas auditadas

La auditoría contempló a tres áreas estratégicas dentro de la organización. El **Equipo DevOps** fue evaluado como responsable directo del mantenimiento del pipeline de despliegue y la infraestructura como código. El **Equipo de Seguridad de la Información** fue revisado por su función en la implementación de políticas, la revisión de configuraciones y la atención de incidentes de seguridad. Finalmente, el **Departamento de Tecnología e Innovación** fue considerado por su papel en la planificación estratégica, supervisión y coordinación general de los recursos tecnológicos de la organización.

4.4. Periodo auditado

El intervalo temporal comprendido en esta auditoría abarca desde el 1 de marzo hasta el 27 de junio de 2025. Durante este periodo, se analizaron las actividades desarrolladas, las configuraciones aplicadas y las evidencias generadas mediante la implementación de la versión activa del entorno Chef_Vagrant_Wp, incluyendo todas las acciones relacionadas con los procesos de despliegue.

---

5. Normativa y Criterios de Evaluación

5.1. Normas y marcos internacionales

La evaluación se sustentó en el uso de marcos normativos internacionales ampliamente reconocidos en la gestión de tecnologías de la información. Se adoptó **COBIT 2019** como referencia para la gobernanza y la generación de valor en TI. Asimismo, se aplicaron los requerimientos de la norma **ISO/IEC 27001:2022**, orientada a la implementación y mejora continua de un sistema de gestión de seguridad de la información, complementada por **ISO/IEC 27002:2022**, que brinda recomendaciones sobre controles de seguridad. Para los aspectos vinculados a la continuidad operativa, se consideró **ISO 22301:2019**, mientras que los controles técnicos de seguridad fueron evaluados con base en la guía **NIST SP 800-53 Rev. 5**, de aplicación internacional. Además, se recurrió a las buenas prácticas de gestión de servicios establecidas en **ITIL 4**, y al **OWASP DevSecOps Maturity Model**, utilizado como marco de referencia específico para entornos de integración y despliegue continuo (CI/CD).

5.2. Normativa nacional

En el contexto normativo peruano, se consideraron dos instrumentos legales fundamentales. En primer lugar, la **Ley N.º 29733** sobre Protección de Datos Personales, junto con su reglamento aprobado por el Decreto Supremo N.º 003-2013-JUS, que regula el tratamiento adecuado y seguro de la información personal. En segundo lugar, se tomó en cuenta la **Ley N.º 30424**, que establece la responsabilidad administrativa de las

personas jurídicas, con énfasis en la adopción de programas de cumplimiento que garanticen el respeto de las normativas vigentes en materia de seguridad y gobernanza.

5.3. Políticas y procedimientos internos de DevIA360

La auditoría también valoró el grado de cumplimiento de las políticas internas de la organización. Se revisaron tres documentos institucionales: la **Política de Seguridad de la Información (versión 2025-01)**, el **Procedimiento de Gestión de Cambios TI (versión 2025-02)** y el **Estándar de Desarrollo Seguro y DevOps (versión 2025-01)**. Estos documentos fueron fundamentales para contrastar los hallazgos con los lineamientos internos establecidos por la empresa auditada.

5.4. Criterios de evaluación

Para determinar la criticidad de los hallazgos y establecer prioridades de mejora, se aplicó la metodología de clasificación de riesgos desarrollada por **OWASP Risk Rating**, que permite asignar niveles de riesgo a partir del impacto y la probabilidad de ocurrencia. Asimismo, se respetaron los niveles de tolerancia al riesgo definidos por el Comité de Seguridad de DevIA360. Finalmente, se incorporaron como guía técnica las mejores prácticas de **Infraestructura como Código (IaC)**, promovidas por organizaciones como **HashiCorp** y **Chef Software**, las cuales permiten establecer entornos estandarizados, seguros y reproducibles en los procesos de aprovisionamiento y despliegue de infraestructura.

---

6. Metodología y Enfoque

6.1. Enfoque adoptado

La auditoría siguió un enfoque mixto, combinando dos perspectivas complementarias: la basada en riesgos y la orientada al cumplimiento. En primer lugar, desde el enfoque **basado en riesgos**, se identificaron, analizaron y priorizaron las amenazas potenciales que pudieran comprometer la confidencialidad, integridad y disponibilidad del entorno Chef_Vagrant_Wp. En segundo lugar, bajo el enfoque **basado en cumplimiento**, se verificó la alineación del entorno auditado con los marcos normativos y estándares aplicables, como COBIT 2019, ISO/IEC 27001:2022 y la Ley N.º 29733, entre otros.

6.2. Etapas de la auditoría

La auditoría fue desarrollada en cinco etapas secuenciales:

1. **Planificación**: Se definieron el alcance, los objetivos, los recursos y el cronograma de trabajo, cubriendo el periodo del 1 de marzo al 27 de junio de 2025.
2. **Levantamiento de información**: Se recopilaron evidencias mediante entrevistas con responsables de áreas clave, revisión de documentación técnica y acceso controlado a los sistemas.
3. **Ejecución de pruebas técnicas**: Se llevaron a cabo análisis de vulnerabilidades, inspecciones de configuraciones y evaluación de controles implementados.
4. **Evaluación y correlación**: Se contrastaron los hallazgos con los marcos normativos establecidos, considerando además el apetito de riesgo definido por la organización.
5. **Informe**: Se elaboró la documentación final con resultados, conclusiones y recomendaciones, presentada en el presente informe.

6.3. Métodos aplicados

Durante la auditoría se aplicaron diversos métodos de análisis:

- **Entrevistas estructuradas** con los responsables de las áreas de TI, DevOps y Seguridad de la Información, con el fin de comprender los procesos, controles y prácticas vigentes.
- **Pruebas técnicas específicas**, incluyendo:
  - Análisis de registros (logs) y correlación de eventos.
  - Escaneo de vulnerabilidades mediante herramientas como InSpec, OpenVAS y nmap.
  - Revisión de código y controles con Serverspec e integración continua.
- **Evaluación de configuraciones**, mediante la comparación de parámetros críticos con guías de endurecimiento reconocidas, como CIS Benchmarks y OWASP DevSecOps.
- **Listas de verificación estructuradas**, empleadas para mapear controles definidos por ISO 27001, COBIT 2019 y NIST SP 800-53, permitiendo evaluar el nivel de madurez y cumplimiento del entorno tecnológico auditado.

---

7. Hallazgos y Observaciones

7.1. Seguridad de la Información

1. Exposición de credenciales sensibles
Se detectó la presencia de variables sensibles como `DB_PASSWORD` y `WP_ADMIN_PASS` almacenadas en texto plano dentro de los data bags de Chef y en el archivo `.env`.

- **Evidencia**: Captura del data_bag_item `mysql/root.json` y commit #3c1f2a7 del repositorio.
- **Criticidad**: Alto (25)
- **Normas vulneradas**: ISO/IEC 27001:2022 (Control 8.12), NIST SP 800-53 (AC-6), política interna art. 4.3
- **Causa**: Ausencia de cifrado (Chef Vault o HashiCorp Vault).
- **Efecto**: Posible acceso no autorizado al sistema y a la base de datos.

2. Puertos abiertos sin restricciones y falta de firewall
Las máquinas virtuales fueron aprovisionadas sin restricciones de acceso a nivel de red, permitiendo la exposición de puertos críticos.

- **Evidencia**: Resultado de `nmap 192.168.56.0/24` indicando puertos 22, 80, 443 y 3306 abiertos.
- **Criticidad**: Alto (20)
- **Normas vulneradas**: ISO/IEC 27002:2022 (Control 8.20), CIS Benchmark Ubuntu 22.04
- **Causa**: Configuración predeterminada no endurecida.
- **Efecto**: Ampliación de la superficie de ataque.

3. Falta de registros de auditoría persistentes
Se identificó la ausencia de un sistema de registro duradero durante el aprovisionamiento.

- **Evidencia**: Cookbooks sin directiva `log_location`, `rsyslog` no habilitado.
- **Criticidad**: Alto (16)
- **Normas vulneradas**: ISO 22301 (Cláusula 8.4), NIST SP 800-53 (AU-6)
- **Causa**: Prioridad operativa frente a trazabilidad.
- **Efecto**: Dificultad en la reconstrucción de eventos ante incidentes.

4. Uso de versiones de software obsoletas
Se emplearon versiones desactualizadas de Apache (2.4.54), MySQL (5.7) y Ruby (2.6), sin aplicación de

parches recientes.

- **Evidencia**: Resultados de `apachectl -v` y `mysql --version`; presencia de CVE sin mitigar.
- **Criticidad**: Alto (20)
- **Normas vulneradas**: OWASP A06:2021, Política de Gestión de Parches TI
- **Causa**: Falta de automatización en la gestión de actualizaciones.
- **Efecto**: Exposición a vulnerabilidades conocidas.

7.2. Gestión de Cambios y Configuración

1. Ambiente único sin segmentación (dev/test/prod)
Se observó el uso de un único archivo `Vagrantfile` para todos los entornos, sin perfiles diferenciados.

- **Evidencia**: Solo rama `main` en el repositorio; ausencia de variables `VAGRANT_ENV`.
- **Criticidad**: Alto (20)
- **Normas vulneradas**: COBIT 2019 (BAI03.03), ITIL 4 (Change Enablement)
- **Causa**: Simplificación operativa.
- **Efecto**: Riesgo de que configuraciones inestables lleguen a producción.

2. Cobertura limitada de pruebas
Las pruebas ejecutadas (`tests.sh`) solo validan servicios básicos, sin contemplar escenarios de fallo o pruebas de seguridad.

- **Evidencia**: Resultado de 10/10 pruebas “OK”; solo 8 de 50 controles Serverspec aplicados.
- **Criticidad**: Medio (12)
- **Normas vulneradas**: OWASP DevSecOps MM Nivel 2, Política QA art. 3.1
- **Causa**: Ausencia de casos de prueba negativos.
- **Efecto**: Vulnerabilidades podrían pasar desapercibidas.

7.3. Continuidad del Negocio

1. Respaldos manuales y no verificados
El proceso de respaldo de base de datos se realiza manualmente con `mysqldump` y no se han ejecutado pruebas de restauración.

- **Evidencia**: Cron job deshabilitado en `db_backup.sh`, sin logs de restauración.
- **Criticidad**: Medio (15)
- **Normas vulneradas**: ISO 22301 (Cláusula 8.7), NIST SP 800-53 (CP-9)
- **Causa**: Recursos limitados en planes de recuperación.
- **Efecto**: Alta exposición ante pérdida de datos o fallos.

---

8. Análisis de Riesgos

8.1. Metodología de valoración

La evaluación de los riesgos se llevó a cabo utilizando la metodología **OWASP Risk Rating**, la cual permite categorizar los hallazgos según su impacto (alto, medio o bajo) y su probabilidad de ocurrencia (porcentual). Esta clasificación facilita priorizar las acciones correctivas en función del nivel de criticidad identificado. Los niveles de riesgo se interpretan de la siguiente manera:

- **Crítico/Alto**: ≥ 20
- **Medio**: 10–19
- **Bajo**: ≤ 9

8.2. Matriz de Riesgos Identificados

Nº	Riesgo identificado	Causa técnica	Impacto	Probabilidad	Nivel de riesgo	Vínculo a evidencia
1	Exposición de credenciales en texto plano	`.env`, data bags sin cifrado	Alto	100%	Crítico (25)	Anexo D
2	Puertos abiertos y sin firewall	Configuración Vagrant por defecto	Alto	100%	Alto (20)	Anexo C
3	Falta de registros de auditoría persistentes	Sin `rsyslog`, sin logs duraderos	Medio	80%	Alto (16)	Anexo F
4	Software desactualizado (Apache, MySQL, Ruby)	Falta de gestión de parches	Alto	80%	Alto (20)	Anexo E
5	Ausencia de entornos segmentados (dev/test/prod)	Vagrantfile único sin perfiles	Alto	80%	Alto (20)	Anexo G
6	Pruebas insuficientes de seguridad	tests.sh con cobertura limitada	Medio	60%	Medio (12)	Evidencia tests.sh
7	Respaldos no automatizados ni verificados	mysqldump manual y sin restauraciones	Medio	75%	Medio (15)	Anexo backup logs

8.3. Análisis consolidado

El análisis integral evidencia que **cinco de los siete riesgos identificados** se ubican en el rango **alto o crítico**, lo cual implica una amenaza considerable para la seguridad y continuidad del entorno auditado. Esta situación demanda acciones correctivas inmediatas, orientadas a mitigar el riesgo residual y reforzar los controles existentes. Se recomienda priorizar las medidas propuestas en función de los niveles de criticidad y en alineamiento con las políticas internas de DevIA360 y los marcos normativos establecidos.

---

9. Conclusiones

El proceso de auditoría realizado sobre el entorno de despliegue automatizado **Chef_Vagrant_Wp** ha permitido identificar vulnerabilidades significativas que afectan tanto la seguridad como la eficiencia operativa del sistema. Si bien la solución auditada proporciona una base funcional adecuada para el aprovisionamiento rápido de entornos WordPress, presenta deficiencias críticas en aspectos clave como la gestión de secretos, la segmentación de entornos, la implementación de controles de red y la trazabilidad operativa.

Se constató que **la ausencia de mecanismos de cifrado para credenciales sensibles**, junto con **la exposición de puertos sin restricciones de acceso**, incrementa el riesgo de accesos no autorizados y compromete la integridad de los servicios desplegados. Asimismo, **la falta de registros de auditoría persistentes** y el uso de **software desactualizado** sin gestión automatizada de parches representan puntos críticos que vulneran los principios de seguridad de la información establecidos por estándares como ISO/IEC 27001 y NIST SP 800-53.

En el ámbito de la gestión del cambio, se evidenció que el entorno carece de una adecuada **segmentación entre ambientes de desarrollo, pruebas y producción**, lo que puede derivar en la promoción inadvertida de código no validado a entornos sensibles. Esta situación se agrava por **la cobertura limitada de pruebas**, que se restringe a validaciones funcionales básicas y no incluye escenarios de fallo o pruebas de seguridad estructuradas.

Finalmente, desde la perspectiva de continuidad del negocio, **el enfoque manual y no verificado de los respaldos** expone a la organización a una potencial pérdida de datos o interrupciones del servicio ante fallos del sistema.

Pese a estos hallazgos, se destaca positivamente que DevIA360 dispone de un equipo técnico competente y de una cultura tecnológica abierta, basada en herramientas de código abierto. Esto constituye una ventaja estratégica para ejecutar de manera eficiente las medidas correctivas propuestas, sin incurrir en costos elevados por licenciamiento.

Se concluye que, una vez implementadas las recomendaciones priorizadas, la organización podrá lograr una **reducción del riesgo global superior al 80 %**, así como una mejora sustancial en su madurez operativa y su nivel de cumplimiento con buenas prácticas internacionales en gobernanza, seguridad y automatización de infraestructura TI.