BD14711_**Logotipo

El contenido generado por IA puede ser incorrecto.Imagen que contiene Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.Logotipo, nombre de la empresa

El contenido generado por IA puede ser incorrecto.**

**Culiacán, SINALOA, A 1 de junio de 2025.**

**EMPRESA:**

Coppel

**NO. CONTROL. NOMBRE CARRERA**

**20170704 Inzunza Jiménez Bryan Jovanny Sistemas**

**EXTERNO:**

**INTERNO:**

LIC. José Arturo Solís Ramírez

LIC. Jaime Arturo Félix Medina

**ASESORES:**

Remediación de Vulnerabilidades en Aplicación Botonera Intranet

**DEPARTAMENTO DE SISTEMAS Y COMPUTACION**

**REPORTE DE**

**RESIDENCIA PROFESIONAL**

Tecnológico Nacional de México Campus Culiacán

1. Agradecimientos

Agradezco a Coppel, la empresa en la que tuve la oportunidad de realizar mis residencias profesionales, por brindarme un espacio de aprendizaje y crecimiento. En especial, mi gratitud hacia el gerente José Arturo Solís Ramírez, quien me apoyó con el seguimiento de mis residencias, facilitando los medios para que pudiera desarrollar mi proyecto de manera eficiente. Asimismo, agradezco a Luis Antonio Bayliss Ayala, mi líder de proyectos, por su guía constante, sus enseñanzas y su disposición para orientarme en cada etapa del proceso.

Extiendo mi agradecimiento al Instituto Tecnológico de Culiacán donde adquirí los conocimientos fundamentales que me permitieron desarrollar mis habilidades profesionales. Gracias a esta institución y a su equipo docente, pude prepararme para afrontar los retos del mundo laboral con confianza y determinación.

A mis amigos Maximiliano Rendón y Sebastián Arellanes, quienes han sido un pilar fundamental en mi camino. Maximiliano, por estar siempre a mi lado con su apoyo incondicional en los momentos difíciles, y Sebastián, por ayudarme desde el inicio de la carrera, brindándome su conocimiento y motivación para seguir adelante.

A mis padres, por ser mi mayor inspiración y mi fortaleza inquebrantable. Su amor, paciencia y sacrificio han sido la base sobre la que he construido mis logros. Gracias por confiar en mí y por impulsarme a alcanzar mis metas con esfuerzo y dedicación.

Finalmente, quiero expresar mi reconocimiento al maestro Jaime Arturo Félix Medina, quien me impartió Lenguaje Ensamblador y Matemáticas Discretas. Su enseñanza y pasión por la materia fueron clave en mi formación académica, transmitiendo conocimientos valiosos que han enriquecido mi desarrollo profesional.

1. Resumen

El presente proyecto aborda la actualización de la aplicación Botonera Intranet de Coppel, la cual presentaba problemas de seguridad y rendimiento debido a su desarrollo en una versión obsoleta de PHP. Esta situación limitaba la implementación de nuevas funcionalidades y exponía la aplicación a vulnerabilidades que podían comprometer la seguridad de la información. Además, la ausencia de un proceso sistemático de sanitización de código y la falta de gestión de parches de seguridad en el servidor aumentaban los riesgos de ataques cibernéticos y accesos no autorizados.

El propósito del proyecto fue consolidar la seguridad y optimizar el rendimiento de la aplicación mediante la actualización a PHP 8.3, la mitigación de vulnerabilidades en el código, la aplicación de parches de seguridad y la realización de pruebas integrales en un entorno controlado. Para lograr estos objetivos, se adoptó un enfoque estructurado basado en el análisis estático del código, la refactorización de componentes obsoletos, la implementación de controles de acceso y la verificación de la correcta aplicación de parches en el servidor.

Durante el desarrollo, se realizaron pruebas periódicas para validar el correcto funcionamiento de la aplicación y se documentaron los avances en cada fase. Los resultados obtenidos reflejan una mejora significativa en la seguridad y estabilidad de la aplicación, reduciendo el riesgo de explotación de vulnerabilidades y garantizando su alineación con los estándares actuales.

1. Índice de tablas, gráficas y figuras.

Figura 1: Nombre de la figura …………………………………………………Pagina

Figura 2: Nombre de la figura …………………………………………………Pagina

Figura 3: Nombre de la figura …………………………………………………Pagina

Figura 4: Nombre de la figura …………………………………………………Pagina

Figura 5: Nombre de la figura …………………………………………………Pagina

Figura N: Nombre de la figura …………………………………………………Pagina

Tabla 1: Nombre de la Tabla …………………………………………………Pagina

Tabla 2: Nombre de la Tabla …………………………………………………Pagina

Tabla 3: Nombre de la Tabla …………………………………………………Pagina

Tabla N: Nombre de la Tabla …………………………………………………Pagina

Gráfica 1: Nombre de la Gráfica …….………………………………………Pagina

Gráfica 2: Nombre de la Gráfica …….………………………………………Pagina

Gráfica 3: Nombre de la Gráfica …….………………………………………Pagina

Gráfica N: Nombre de la Gráfica …….………………………………………Pagina

[I. Agradecimientos iii](#_Toc199539538)

[II. Resumen iii](#_Toc199539539)

[III. Índice de tablas, gráficas y figuras. iv](#_Toc199539540)

[Índice v](#_Toc199539541)

[Capítulo: Generalidades del proyecto 1](#_Toc199539542)

[1.- Introducción 1](#_Toc199539543)

[2.- Descripción de la empresa u organización y del puesto o área del trabajo del estudiante. 1](#_Toc199539544)

[3.-Problema a resolver, priorizándolo. 2](#_Toc199539545)

[4.- Objetivos 4](#_Toc199539546)

[4.1. Objetivo General 4](#_Toc199539547)

[4.2. Objetivos Específicos 4](#_Toc199539548)

[5.- Justificación 5](#_Toc199539549)

[Capítulo: Marco Teórico 6](#_Toc199539550)

[6. Fundamentos Teóricos 6](#_Toc199539551)

[6.1 Marco Referencial 6](#_Toc199539552)

[6.2 Marco Contextual 6](#_Toc199539553)

[6.3 Marco Teórico 7](#_Toc199539554)

[6.4 Marco Conceptual 7](#_Toc199539555)

[Capítulo: Desarrollo 8](#_Toc199539556)

[7.- Procedimiento y Descripción de las actividades desarrolladas. 8](#_Toc199539557)

[7.1.- Determinación de tiempos de las actividades. 8](#_Toc199539558)

[7.2.- Descripción de las Actividades realizadas. 8](#_Toc199539559)

[7.2.1.- Inventario de aplicaciones (2 semanas) 8](#_Toc199539560)

[7.2.2.- Inventario de activos (2 semanas) 9](#_Toc199539561)

[7.2.3.- Análisis de las aplicaciones (4 semanas) 10](#_Toc199539562)

[7.2.4.- Diseño del entorno de pruebas (3 semanas) 11](#_Toc199539563)

[7.2.5.- Ejecución de pruebas de seguridad (4 semanas) 12](#_Toc199539564)

[7.2.6.- Detección de dependencias (2 semanas) 12](#_Toc199539565)

[7.2.7.- Implementación de las correcciones (4 semanas) 12](#_Toc199539566)

[7.2.8.- Actualización de la documentación (4 semanas) 13](#_Toc199539567)

[Capítulo: Resultados 14](#_Toc199539568)

[8.1.- Resultados 14](#_Toc199539569)

[Capítulo: Conclusiones 16](#_Toc199539570)

[9.1. Conclusiones del proyecto. 16](#_Toc199539571)

[9.2. Recomendaciones 16](#_Toc199539572)

[9.3. Experiencia personal profesional adquirida. 17](#_Toc199539573)

[Capítulo: Competencias desarrolladas 19](#_Toc199539574)

[10. Competencias desarrolladas y/o aplicadas. 19](#_Toc199539575)

[Capítulo: Fuentes de Información 21](#_Toc199539576)

[11. Referencias bibliográficas y virtuales 21](#_Toc199539577)

[Anexos: 21](#_Toc199539578)

Índice

Capítulo: Generalidades del proyecto

# 1.- Introducción

En el ámbito de las tecnologías empresariales, la seguridad y el rendimiento de las aplicaciones son factores clave para garantizar la continuidad operativa y la protección de los datos. En este contexto, el presente reporte de residencia detalla el proceso de consolidación de la seguridad y optimización del rendimiento de la infraestructura tecnológica de Coppel, específicamente en la aplicación Botonera Intranet. Se abordó la necesidad de actualizar la plataforma a la versión 8.3 de PHP para mitigar vulnerabilidades en el código y mejorar su desempeño.

Este trabajo surgió de la importancia de mantener la infraestructura tecnológica de Coppel actualizada y segura, asegurando la continuidad de los servicios internos. La actualización a PHP 8.3 y la remediación de vulnerabilidades fueron esenciales para cumplir con los estándares de la industria y los requerimientos del área de seguridad de la aplicación.

El proyecto se estructuró en torno a la actualización de la aplicación, la mitigación de vulnerabilidades de código estático, la aplicación de parches de seguridad, la realización de pruebas y la liberación de la nueva versión a producción.

Se empleó una metodología sistemática que incluyó la revisión del código, la implementación de medidas de seguridad, la realización de pruebas en un entorno controlado y la documentación de los resultados.

Entre las limitaciones del trabajo, se encontró la dependencia de otros equipos para la aplicación de parches y la realización de pruebas en producción. Asimismo, la complejidad del código heredado requirió un análisis detallado y una planificación cuidadosa para garantizar una actualización exitosa.

# 2.- Descripción de la empresa u organización y del puesto o área del trabajo del estudiante.

**Nombre de la empresa**:

Coppel S.A de C.V

* **Razón Social:** Coppel S.A. de C.V.
* **Domicilio:** Calle República 2855 Poniente, Culiacán, Sinaloa.
* **Giro:** Tienda departamental y servicios financieros.

Coppel fue fundada en 1941 y se ha consolidado como una de las empresas mexicanas más importantes en la venta de productos y servicios financieros. Su propósito es mejorar la calidad de vida de sus clientes, ofreciendo opciones accesibles y flexibles de compra a través de sus más de 1,600 tiendas en México y Argentina. A lo largo de su historia, ha evolucionado para integrar nuevas tecnologías en sus servicios y expandir su modelo de negocio.

**Misión:**

Facilitar el acceso a bienes y servicios financieros a millones de clientes mediante soluciones innovadoras y accesibles.

**Visión:**

Ser la tienda omnicanal favorita del mercado masivo, destacando en sostenibilidad y criterios ASG (ambientales, sociales y de gobernanza).

**Objetivos:**

* Ofrecer productos y servicios financieros accesibles.
* Expandir su presencia nacional e internacional.
* Integrar soluciones tecnológicas para mejorar la experiencia del cliente y la seguridad de sus sistemas.

**Área de Trabajo:**

Remediación de Vulnerabilidades (RV)

El área de Remediación de Vulnerabilidades (RV) es responsable de garantizar la seguridad de los sistemas tecnológicos de Coppel, protegiendo la infraestructura ante posibles amenazas y fallas de seguridad. Esta área forma parte del equipo de seguridad informática y trabaja en colaboración con distintos departamentos de TI para mantener la integridad de la información y la infraestructura digital.

**Funciones principales del área:**

* **Sanitización de código:** Identificación y corrección de vulnerabilidades en el código fuente para prevenir ataques.
* **Migración de sistemas:** Actualización y optimización de tecnologías para mejorar su seguridad y rendimiento.
* **Remediación de fallas:** Aplicación de medidas correctivas ante incidentes de seguridad detectados en la infraestructura tecnológica.

**Participación del estudiante:**  
Durante la residencia, el estudiante colaboró en el fortalecimiento de la seguridad tecnológica de Coppel mediante la actualización de sistemas, la identificación y mitigación de vulnerabilidades en código y la aplicación de mejores prácticas de seguridad. Su trabajo incluyó la revisión y optimización de procesos, así como la ejecución de pruebas para validar la efectividad de las soluciones implementadas.

**Organigrama:**

Diagrama

El contenido generado por IA puede ser incorrecto.

# 3.-Problema a resolver, priorizándolo.

**Antecedentes de la situación problemática**

En la empresa Coppel, la aplicación *Botonera Intranet* cumple un papel esencial al facilitar el acceso centralizado a diversas herramientas y servicios internos. Sin embargo, esta aplicación presenta una serie de problemas derivados del uso de versiones obsoletas de PHP, lo que impacta tanto en su rendimiento como en su seguridad. La falta de actualización ha generado riesgos de seguridad significativos debido a vulnerabilidades en el código estático y dinámico, lo que podría comprometer la integridad de los sistemas y la confidencialidad de la información.

Además, la infraestructura subyacente que soporta *Botonera Intranet* no ha recibido actualizaciones críticas de seguridad en el sistema operativo del servidor, lo que aumenta el riesgo de ataques externos. La ausencia de un entorno de pruebas idéntico al de producción también dificulta la detección temprana de errores y vulnerabilidades, lo que podría generar fallas en la aplicación al momento de su implementación.

**Problema a Resolver y Priorización**

A partir de la evaluación de la situación actual, se han identificado los siguientes problemas en orden de prioridad:

1. **Obsolescencia de PHP en la aplicación "Botonera Intranet".**  
   * Actualmente, la aplicación opera con una versión antigua de PHP que contiene múltiples funciones deprecadas, lo que dificulta su mantenimiento y aumenta el riesgo de vulnerabilidades.
   * Se requiere actualizar la aplicación a PHP 8.3, asegurando la compatibilidad del código y mejorando su estabilidad y seguridad.
2. **Vulnerabilidades en el código estático y dinámico.**  
   * La aplicación presenta vulnerabilidades en su código fuente que pueden ser explotadas por atacantes, poniendo en riesgo la seguridad de los datos y la continuidad operativa.
   * Es necesario mitigar estas vulnerabilidades mediante la refactorización y aplicación de prácticas seguras hasta completar su corrección.
3. **Falta de aplicación de parches de seguridad en la infraestructura del servidor.**  
   * El sistema operativo del servidor donde se ejecuta la aplicación no ha recibido actualizaciones críticas de seguridad, lo que lo hace vulnerable a ataques.
   * Es fundamental aplicar los parches de seguridad de alta prioridad para reducir la exposición a amenazas.
4. **Ausencia de un entorno de pruebas idéntico al de producción.**  
   * Actualmente, no se cuenta con un entorno de pruebas que replique las condiciones de producción, lo que dificulta la detección de fallas antes de la liberación de nuevas versiones.
5. **Necesidad de un plan de contingencia para la actualización de la aplicación.**  
   * Dado el impacto que puede tener la actualización de PHP en la operación de la aplicación, es necesario contar con un plan de rollback en caso de fallas críticas.

**Impacto esperado**

La solución de estos problemas permitirá consolidar la seguridad de la *Botonera Intranet*, optimizar su rendimiento y garantizar la continuidad operativa de la aplicación. Además, al mitigar vulnerabilidades y aplicar buenas prácticas de seguridad, se reducirá el riesgo de incidentes que puedan afectar la infraestructura tecnológica de Coppel.

# 4.- Objetivos

## 4.1. Objetivo General

Consolidar la seguridad y optimizar el rendimiento de la infraestructura tecnológica de Coppel mediante la actualización de la aplicación *Botonera Intranet* a la última versión estable de PHP, la implementación de medidas de seguridad para mitigar vulnerabilidades en código estático y dinámico, y la aplicación de parches críticos al sistema operativo. Esto garantizará la estabilidad, continuidad y protección de los servicios internos de la empresa, alineándose con los estándares de la industria y los requerimientos del área de seguridad.

## 4.2. Objetivos Específicos

* Actualizar la aplicación Botonera Intranet a PHP 8.3 para mejorar la seguridad y el rendimiento del sistema, reemplazando al menos el 80% de las sentencias obsoletas por equivalentes modernos antes del 31 de julio.
* Mitigar el 100% de las vulnerabilidades detectadas en el código estático de la aplicación en bloques de 500 líneas por semana, iniciando el 1 de febrero y finalizando el 15 de julio.
* Aplicar todos los parches de seguridad críticos y de alta prioridad en el sistema operativo del servidor aplicativo antes del 15 de abril, verificando su correcta instalación y funcionamiento.
* Realizar pruebas integrales en un entorno de pruebas idéntico al de producción en ciclos de dos semanas, comenzando el 15 de abril, y documentar al menos el 98% de los casos de prueba ejecutados y sus resultados.
* Liberar la nueva versión de la aplicación Botonera Intranet a producción el 31 de julio, asegurando un rollback planificado en caso de incidentes críticos, y elaborar un plan de contingencia detallado para el 15 de mayo.

5.- Justificación

La aplicación *Botonera Intranet* es una herramienta esencial dentro de la infraestructura tecnológica de Coppel, ya que centraliza y gestiona el acceso a múltiples sistemas internos. Sin embargo, actualmente enfrenta diversas limitaciones que comprometen su seguridad, rendimiento y escalabilidad.

Uno de los principales problemas es la obsolescencia de la versión de PHP en la que está desarrollada, lo que restringe la adopción de nuevas funcionalidades, impide la implementación de estándares modernos de seguridad y aumenta el riesgo de vulnerabilidades explotables. Además, la aplicación carece de un proceso sistemático de sanitización de código, lo que la hace susceptible a ataques de inyección y otras amenazas cibernéticas.

Este proyecto tiene como propósito mitigar estos riesgos mediante:

* **La actualización de la aplicación a PHP 8.3**, lo que garantizará compatibilidad con las versiones más recientes de librerías y frameworks, mejorando la eficiencia y seguridad del sistema.
* **La implementación de medidas de seguridad robustas**, como la sanitización del código y la mitigación de vulnerabilidades, alineadas con estándares de la industria.
* **La optimización de la infraestructura tecnológica**, aplicando parches críticos al sistema operativo del servidor y mejorando el proceso de gestión de seguridad.

Los beneficios esperados de este proyecto incluyen:

* **Mayor seguridad:** La actualización de PHP y la aplicación de medidas preventivas reducirán significativamente el riesgo de ataques cibernéticos y protegerán la información confidencial de la empresa.
* **Mejor rendimiento:** La optimización del código y del entorno de ejecución incrementará la eficiencia y estabilidad del sistema.
* **Reducción de costos:** Disminuirá los gastos asociados a incidentes de seguridad y a la resolución de problemas técnicos en la aplicación.
* **Alineación con mejores prácticas:** La implementación de estándares modernos facilitará la mantenibilidad del software y garantizará su cumplimiento con los lineamientos de seguridad de la empresa.

Este proyecto es fundamental para mejorar la seguridad, el rendimiento y la sostenibilidad de la aplicación *Botonera Intranet*. Su implementación contribuirá a la protección de los sistemas internos de Coppel, asegurando la continuidad operativa y fortaleciendo la postura de seguridad de la empresa.

Capítulo: Marco Teórico

6. Fundamentos Teóricos

6.1 Marco Referencial

El desarrollo de sistemas seguros y eficientes ha sido un tema central en la ingeniería de software moderna, especialmente en aplicaciones empresariales críticas como las utilizadas por grandes corporativos. En este contexto, Coppel ha implementado la aplicación Botonera Intranet como herramienta de uso interno para facilitar el acceso a servicios y sistemas internos de la empresa. Sin embargo, con el paso del tiempo y los constantes cambios tecnológicos, se han identificado limitaciones y vulnerabilidades que requieren atención prioritaria, particularmente en lo relacionado con la seguridad, la actualización tecnológica y el mantenimiento de la infraestructura.

Diversos estudios han señalado la importancia de mantener actualizados tanto los entornos de desarrollo como los entornos de producción. Por ejemplo, según Rodríguez y Martínez (2021), las organizaciones que operan con versiones obsoletas de lenguajes de programación como PHP presentan un mayor riesgo ante vulnerabilidades conocidas que ya han sido corregidas en versiones recientes. En este sentido, el caso de Botonera Intranet representa una situación común en muchas empresas, donde la necesidad de mantener la compatibilidad con sistemas legados entra en conflicto con la necesidad de adoptar tecnologías más seguras y eficientes.

Además, conforme a lo señalado por Ramírez (2020), la ausencia de procesos sistemáticos para la gestión de parches de seguridad y la falta de controles de acceso adecuados son factores críticos que incrementan la exposición de los sistemas empresariales ante ataques informáticos. Por ello, se vuelve necesario implementar buenas prácticas de seguridad, tales como el principio de privilegios mínimos, la autenticación robusta y la auditoría constante de accesos.

El presente proyecto se alinea con iniciativas similares enfocadas en la modernización de sistemas internos mediante prácticas de desarrollo seguro, buenas prácticas de programación y estandarización de procesos de mantenimiento. Este marco referencial sienta las bases teóricas y prácticas sobre las que se apoya la optimización de la aplicación Botonera Intranet en Coppel, y destaca la relevancia de su actualización tanto para la continuidad operativa como para la protección de los activos digitales de la organización. Asimismo, se busca cumplir con el estándar empresarial llamado “n-2” que consiste en estar actualizado como mínimo en las últimas dos versiones de la tecnología en uso, es decir que si existe la versión 8.3 de PHP el sistema se debe encontrar desarrollado como mínimo en la versión 8.1 o considerar que la versión actual de sistema tenga como mínimo 2 años de soporte.

6.2 Marco Contextual

La empresa Coppel es una de las cadenas comerciales más grandes de México, con una fuerte presencia en sectores como venta de artículos, servicios financieros y tecnologías de la información. su infraestructura tecnológica sustenta operaciones críticas a gran escala, por lo que la disponibilidad, seguridad y eficiencia de sus sistemas internos es una prioridad estratégica. dentro de este contexto, la aplicación botonera intranet desempeña un rol clave al centralizar accesos a sistemas y servicios utilizados por los colaboradores para desempeñar sus funciones diarias.

Esta aplicación fue desarrollada hace varios años bajo una versión antigua del lenguaje PHP, lo que ha generado una serie de limitaciones tanto a nivel de rendimiento como de seguridad. Además, la ausencia de procesos de actualización periódica, mecanismos de autenticación avanzados y prácticas modernas de mantenimiento ha derivado en una creciente vulnerabilidad ante amenazas cibernéticas, como ataques de inyección, escalamiento de privilegios y exposición de información sensible.

El entorno organizacional de Coppel está en constante transformación, impulsado por la necesidad de adoptar nuevas tecnologías, cumplir con normativas internas de seguridad informática y mejorar la experiencia del usuario interno. En este marco, el presente proyecto de residencia se desarrolla en el área de sistemas, específicamente en un equipo encargado de la modernización de aplicaciones internas con el nombre de Remediación de Vulnerabilidades (RV). Este entorno proporciona acceso a herramientas especializadas, lineamientos corporativos y colaboración con profesionales del área, lo que permite aplicar metodologías reales de la industria para el desarrollo e implementación de soluciones seguras.

Este marco contextual resalta la importancia de modernizar la aplicación Botonera Intranet no solo desde una perspectiva técnica, sino también estratégica, ya que su mejora impacta directamente en la productividad de los colaboradores, la protección de datos sensibles y el cumplimiento de estándares empresariales que buscan mantener la competitividad tecnológica de la organización y la seguridad tecnológica.

6.3 Marco Teórico

6.4 Marco Conceptual

Capítulo: Desarrollo

# 7.- Procedimiento y Descripción de las actividades desarrolladas.

## 7.1.- Determinación de tiempos de las actividades.

Gráfico, Tabla

El contenido generado por IA puede ser incorrecto.

## 7.2.- Descripción de las Actividades realizadas.

7.2.1.- Inventario de aplicaciones (2 semanas)

Se elaboró un inventario detallado de las aplicaciones internas utilizadas por el área, con especial atención en aquellas que operaban sobre tecnologías obsoletas o carecían de mantenimiento. Esta actividad implicó reuniones con los responsables de cada sistema, revisión de los accesos y rutas dentro del portal de intranet y verificación de forma manual de los activos disponibles. Se tuvo un acercamiento con líderes de otras áreas, reuniones con gerentes de proyectos y videoconferencias en el que se compartía una parte del sistema y un poco de su funcionalidad. Se trabajó guardando registros dentro de hojas de cálculo en la nube conforme se llevaban a cabo las revisiones de las aplicaciones.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

Figura 1.1: Resumen de especificaciones del servidor

Se realizó un recorrido por la botonera para identificar accesos y rutas a cada sistema. También se llevaron a cabo sesiones remotas mediante videollamadas, donde líderes técnicos y gerentes compartieron pantallas y funcionalidades clave de las herramientas en uso. Todo lo recabado fue registrado y organizado en hojas de cálculo alojadas en la nube para su constante actualización y revisión por parte del equipo de desarrollo.

7.2.2.- Inventario de activos (2 semanas)

Se identificaron y clasificaron los activos tecnológicos asociados a las aplicaciones detectadas, incluyendo servidores, bases de datos, frameworks, versiones de lenguaje de programación y la infraestructura de red utilizada. Se realizó un listado de todos los activos que se incluyen dentro de botonera, registrando el numero de archivos, realizando un conteo agrupando por tipo de archivo y el URL con el que esta declarado dentro de la botonera que sirve para el redireccionamiento.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Figura 1.2: Hoja de cálculo de inventario de aplicaciones

Esta actividad fue realizada junto con apoyo del área de Linux ya que el equipo de desarrollo tiene permisos limitados dentro de los servidores empresariales, esto incluyó levantamiento de tickets en el que se autorizaron a través del dueño del servidor.  
Se llevó un control dentro de hojas de cálculo y reportes que fueron entregados y revisados por el líder de proyectos.

Interfaz de usuario gráfica, Aplicación, Teams

El contenido generado por IA puede ser incorrecto.

Figura 1.3: Ticket de solicitud de permisos

7.2.3.- Análisis de las aplicaciones (4 semanas)

Durante esta fase se evaluó el estado técnico y funcional de las aplicaciones priorizadas. El objetivo fue identificar dependencias tecnológicas, niveles de acoplamiento, problemas de seguridad, y calidad del código.

Se realizó una revisión manual del código fuente y los archivos de configuración mediante editores como Visual Studio Code. Además, se utilizó la herramienta Checkmarx, que permitió escanear los proyectos completos y generar informes detallados de vulnerabilidades y prácticas inseguras.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Figura 1.4: Código de aplicaciones en la botonera intranet

Se analizaron estructuras de carpetas, rutas internas, controladores, variables de entorno y puntos críticos en la comunicación con otros servicios, además de revisión exhaustiva de código y revisión de falsos positivos por la herramienta.

Texto

El contenido generado por IA puede ser incorrecto.

Figura 1.5 Estructura de carpeta de botonera intranet

Se hizo uso de inteligencia artificial con un proyecto de otra área en el que se procesaron archivos del proyecto botonera intranet para encontrar vulnerabilidades y mitigar, para esto se tuvo que actualizar la base de datos con un listado de sentencias deprecadas de PHP, se navego entre la documentación oficial para recopilar de forma completa las sentencias deprecadas hasta la versión 8.3 de PHP

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Figura 1.6: Hoja de calculo de sentencias deprecadas PHP

7.2.4.- Diseño del entorno de pruebas (3 semanas)

Se diseñó un entorno de pruebas aislado del entorno productivo, replicando las condiciones técnicas necesarias para garantizar una correcta validación de las actualizaciones. Para ello se configuraron contenedores usando la herramienta de Docker y posteriormente se migró a Podman, se emplearon versiones equivalentes de los servidores web y bases de datos en uso. También se realizaron pruebas de conexión con servicios internos para validar su integración. Fue necesaria la creación de los archivos y las configuraciones necesarias para los contenedores en conjunto con el equipo de desarrollo.

Diagrama

El contenido generado por IA puede ser incorrecto.

Figura 1.7: Arquitectura del servidor aplicativo y base de datos de botonera intranet

7.2.5.- Ejecución de pruebas de seguridad (4 semanas)

Se llevaron a cabo pruebas de seguridad sobre las aplicaciones previamente desplegadas en el entorno de pruebas. Estas pruebas incluyeron análisis estático, escaneos de vulnerabilidades en bibliotecas, y validaciones de configuraciones insegura

7.2.6.- Detección de dependencias (2 semanas)

Durante esta fase se identificaron las bibliotecas, paquetes, frameworks y APIs de terceros utilizados por las aplicaciones. Esto incluyó dependencias explícitas dentro de archivos de configuración, fueron verificadas la vigencia de las versiones, soporte oficial y la correcta implementación de estas.

7.2.7.- Implementación de las correcciones (4 semanas)

Con base en los escaneos anteriores, se procedió a implementar correcciones en el código de las aplicaciones. Esto incluyó la actualización de dependencias, saneamiento de entradas, cambios en la lógica insegura, implementación de validaciones, y refactorización de fragmentos críticos.

Se hicieron a base de comentarios debajo del código de manera que fueran revisados en equipo y determinar si el programador había llegado a la correcta solución, además de hacer un segundo escaneo al terminar la mitigación de vulnerabilidades y comprobar la funcionalidad.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Figura 1.8: Vulnerabilidad encontrada por checkmarx en archivo proc\_validarhuella.php

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

Figura 1.9: Corrección de la vulnerabilidad archivo proc\_validarhuella.php

La mayor parte de mi trabajo y la manera de trabajar fue dejando la solución de modo de comentario para que fuera revisado por el programador sr y aplicar el cambio de ser correcto, además de dejar recomendaciones al código que me tocaba revisar.

Texto

El contenido generado por IA puede ser incorrecto.

Figura 1.10: Comentario resaltando vulnerabilidades de archivo de en botonera intranet

7.2.8.- Actualización de la documentación (4 semanas)

El proyecto fue acortado, la única documentación que fue realizada fueron los diagramas de las actividades, el plan de trabajo y la documentación de los activos dentro de las hojas de cálculo, esto por cuestiones de tiempo y de urgencia de otros proyectos, lamentablemente esto ocurre seguido, por órdenes superiores la documentación se deja de lado o se hace a la par de nuevos proyectos. En este proyecto no fue la excepción, llegaron proyecto al área y se comenzaron a trabajar por la urgencia.

Capítulo: Resultados

8.1.- Resultados

Durante la realización del proyecto de mejora en el sistema de botonera de intranet, se lograron avances importantes en cuanto a la organización, análisis y seguridad de las aplicaciones internas. Estas mejoras estuvieron enfocadas en la creación de un inventario robusto, la identificación de activos, el análisis de vulnerabilidades y la estandarización de entornos de pruebas, lo cual permitió sentar las bases para una gestión más segura y eficiente de los sistemas internos.

**1. Organización y Control del Inventario de Aplicaciones**

Uno de los principales logros fue la creación de un inventario completo de las aplicaciones disponibles en la botonera. Este inventario contempló tanto las rutas internas de acceso como el propósito, tecnología y estado de mantenimiento de cada aplicación. A través de reuniones con líderes de área, revisión manual de accesos y análisis funcional de los sistemas, se obtuvo un panorama claro de la infraestructura interna.

El resultado fue una hoja de cálculo organizada y compartida en la nube, que sirve como fuente única de consulta y actualización para el equipo de desarrollo y áreas involucradas. Esto ha permitido priorizar las aplicaciones que requieren atención urgente por obsolescencia o falta de soporte.

**2. Identificación de Activos Tecnológicos y Dependencias**

Se realizó un inventario detallado de activos relacionados con las aplicaciones: desde servidores, archivos y rutas, hasta frameworks y versiones de lenguaje. Este proceso fue respaldado por el área de Linux, debido a las restricciones de acceso sobre los servidores empresariales. La información recabada permitió conocer la infraestructura exacta donde operan las aplicaciones de botonera, y se documentó con URLs internas, cantidad y tipo de archivos por sistema.

También se generó un mapa completo de dependencias tecnológicas, lo cual permitió identificar librerías en desuso, frameworks sin soporte y riesgos potenciales asociados a versiones obsoletas.

**3. Detección y Análisis de Vulnerabilidades**

Otro resultado clave fue la revisión profunda del código fuente de las aplicaciones más críticas. Se utilizaron editores como Visual Studio Code y herramientas automáticas como CheckMarx para detectar vulnerabilidades, malas prácticas y estructuras inseguras.

Además, se elaboró una guía con sentencias deprecadas en PHP hasta la versión 8.3, lo cual se integró en el proceso de análisis con apoyo de inteligencia artificial. Esto facilitó el reconocimiento automático de funciones inseguras y permitió acelerar la detección de puntos de riesgo en el código.

**4. Creación de un Entorno de Pruebas Aislado y Seguro**

Como parte de las acciones preventivas, se configuró un entorno de pruebas usando contenedores. Inicialmente se utilizó Docker, y posteriormente se migró a Podman, replicando las condiciones técnicas del entorno productivo sin poner en riesgo los sistemas reales.

Este entorno permitió validar configuraciones, probar cambios de código, y realizar escaneos de seguridad en un ambiente controlado, lo cual mejoró significativamente la calidad del proceso de pruebas y redujo el margen de error.

**5. Implementación Guiada de Correcciones y Buenas Prácticas**

Una parte importante del trabajo consistió en proponer correcciones sobre el código detectado como vulnerable. Las recomendaciones se realizaron directamente en los archivos como comentarios, de forma que pudieran ser revisadas y validadas por desarrolladores sénior.

Esta dinámica fomentó la colaboración y el aprendizaje dentro del equipo de desarrollo. Además, permitió aplicar buenas prácticas como sanitización de entradas, validación de datos y refactorización de lógica crítica, lo cual mejoró la seguridad general del sistema.

7. Impacto en la Gestión y Seguridad de Sistemas Internos

Gracias a estos resultados, la botonera de intranet ahora cuenta con un mayor control, una visión clara del ecosistema de aplicaciones y herramientas para detectar y corregir vulnerabilidades de forma anticipada. Esto reduce el riesgo de fallas críticas, facilita el mantenimiento preventivo, y permite escalar mejoras en futuras iteraciones.

El proyecto también dejó como legado una guía técnica que estandariza el proceso de análisis y mitigación, útil para otros equipos dentro de la organización.

Capítulo: Conclusiones

9.1. Conclusiones del proyecto.

El proyecto de fortalecimiento en seguridad para la aplicación Botonera Intranet representó una oportunidad valiosa para aplicar mis conocimientos en un entorno real y de alto impacto dentro de la empresa Coppel. El problema principal detectado al inicio fue la falta de validaciones, controles y prácticas seguras dentro de la aplicación, lo cual representaba un riesgo tanto para los usuarios como para la integridad del sistema.

Desde el planteamiento del objetivo —realizar actividades que aumentaran la seguridad de la aplicación y de sus entornos relacionados— se trazó una ruta de trabajo clara que permitió realizar un análisis detallado del código fuente, configurar entornos de prueba y aplicar escaneos de vulnerabilidad con herramientas especializadas. A partir de los hallazgos se realizaron correcciones puntuales en los repositorios, mejoras en la documentación y se propusieron lineamientos que permitirán mantener un estándar de seguridad más robusto a largo plazo.

Uno de los mayores aprendizajes fue comprender cómo los procesos internos de Coppel están orientados a mantener altos estándares de calidad, aunque también identifiqué áreas que pueden fortalecerse, especialmente en el manejo y la actualización de documentación técnica, así como en el seguimiento continuo de vulnerabilidades. También fue necesario adaptarme al trabajo con tecnologías heredadas y procesos ya establecidos, lo cual representó un reto al principio, pero que logré superar con dedicación y apoyo del equipo.

En síntesis, el proyecto cumplió su objetivo principal: aportar a la mejora de la seguridad de la aplicación Botonera. También me permitió crecer profesionalmente, comprender cómo se estructuran los procesos de seguridad en una empresa de gran escala y confirmar que las buenas prácticas, la colaboración y la documentación continua son claves para garantizar la calidad del software.

9.2. Recomendaciones

Con base en la experiencia adquirida durante la residencia profesional, propongo las siguientes recomendaciones para la mejora continua del sistema y del área de seguridad en relación con la aplicación Botonera:

* Documentación técnica continua: Es recomendable mantener actualizada la documentación de código, configuraciones y pruebas realizadas. Esto facilitará futuras intervenciones en la aplicación y reducirá el tiempo de análisis para nuevos desarrolladores o equipos de seguridad.
* Automatización de pruebas de seguridad: Implementar escaneos automáticos y programados mediante herramientas como GitLab CI/CD que alerten sobre vulnerabilidades comunes antes de cada despliegue.
* Capacitación del equipo técnico: Invertir en sesiones regulares de capacitación en temas de seguridad para desarrolladores y responsables del sistema, buenas prácticas de desarrollo seguro y respuesta a incidentes.
* Validaciones en capas: Fortalecer el sistema incluyendo validaciones tanto en el backend como en el frontend para evitar manipulaciones indebidas, accesos no autorizados y entradas maliciosas.
* Revisión de accesos y privilegios: Auditar regularmente los roles y permisos asignados a los usuarios del sistema, garantizando que cada perfil tenga únicamente los accesos necesarios.
* Establecer un ciclo de revisión periódica: Definir un cronograma de mantenimiento y revisión de la seguridad de la aplicación, incluyendo pruebas de penetración internas o revisiones de terceros especializados.

Estas recomendaciones permitirán que la aplicación Botonera mantenga una evolución constante en términos de seguridad, confiabilidad y eficiencia, alineándose con los objetivos estratégicos de Coppel y las mejores prácticas de la industria del software.

9.3. Experiencia personal profesional adquirida.

Durante mi residencia profesional, desarrollé habilidades técnicas más sólidas y adquirí nuevos conocimientos relacionados con la seguridad de aplicaciones, análisis de vulnerabilidades, pruebas en entornos controlados y mantenimiento de documentación técnica. Al inicio, mis conocimientos en ciberseguridad y configuración de entornos de pruebas eran limitados, pero con el acompañamiento del equipo y la práctica constante logré avanzar notablemente en estas áreas. También mejoré mi capacidad para trabajar con herramientas específicas como Docker, Podman, Git, GitHub, Jira.

Además de los conocimientos técnicos, fortalecí competencias importantes como la organización personal, la responsabilidad, el análisis crítico, y la resolución de problemas reales. Aprendí a gestionar mejor mis tiempos y tareas, y a adaptar soluciones a sistemas existentes con restricciones de tecnología heredada, sin comprometer la funcionalidad ni la seguridad.

Una de las dificultades que enfrenté fue la falta de documentación en algunas partes del sistema, lo que complicaba el análisis inicial de la aplicación. También hubo ocasiones en las que la carga de trabajo se acumuló por imprevistos o prioridades cambiantes. Sin embargo, estas experiencias me enseñaron la importancia de mantener la calma, pedir apoyo y adaptarme a los cambios con una actitud positiva.

En cuanto a la relación con mis compañeros y superiores, fue muy buena. Siempre recibí su apoyo y apertura para plantear dudas o proponer soluciones. Aprendí mucho de la convivencia con perfiles técnicos experimentados, y desarrollé habilidades de comunicación efectiva, respeto, formalidad y colaboración dentro del equipo.

Mi jefe inmediato mostró un perfil de líder responsable, accesible y con enfoque en el desarrollo profesional del equipo. Su guía fue clave para mi integración y crecimiento dentro del entorno laboral. La relación que sostuve con él fue de cordialidad y respeto mutuo, lo que permitió que pudiera expresar mis avances y también pedir retroalimentación cuando fue necesario.

Algunos procesos internos de la empresa varían dependiendo del área correspondiente, afortunadamente el área en la que colaboré contaba con estándares definidos para la revisión del código, control de versiones, administración del tiempo y de proyectos, lo que facilitó trabajas en equipo de forma ordenada.

En general, mi residencia profesional fue una experiencia altamente productiva y formativa, que me permitió poner en práctica mis conocimientos universitarios, adquirir nuevas habilidades, y prepararme de forma más sólida para integrarme al mundo laboral como ingeniero en sistemas.

Capítulo: Competencias desarrolladas

10. Competencias desarrolladas y/o aplicadas.

Durante mi desempeño en el proyecto de fortalecimiento de seguridad y modernización de la aplicación Botonera Intranet en Coppel, logré aplicar y desarrollar competencias clave que forman parte del perfil de egreso de la carrera de Ingeniería en Sistemas Computacionales. Estas competencias se dividen en dos categorías principales: específicas y genéricas.

**Competencias específicas**

Las competencias específicas están directamente relacionadas con los conocimientos técnicos adquiridos durante la carrera. A continuación, explico cómo cada una contribuyó a mi desempeño en el proyecto:

1. **Fundamentos de Programación, Programación Web, Temas Selectos de Programación, Desarrollo de Aplicaciones Seguras**

Estas materias me proporcionaron la base técnica para identificar y resolver vulnerabilidades dentro del sistema, así como mejorar su funcionamiento. Estas competencias me permitieron:

* Analizar el código fuente de la aplicación Botonera Intranet para identificar malas prácticas de seguridad y técnicas obsoletas.
* Implementar mejoras en el backend desarrollado en PHP, asegurando la compatibilidad con versiones más modernas del lenguaje.
* Aplicar principios de desarrollo seguro, como validación de entradas, manejo adecuado de sesiones y protección contra ataques comunes.

1. **Fundamentos de Ingeniería de Software, Métodos de Desarrollo, Ingeniería de Requisitos**

Gracias a estas materias pude estructurar el proyecto de manera ordenada, siguiendo prácticas recomendadas en la industria. Algunas de las aplicaciones específicas fueron:

* Elaboración de inventarios de aplicaciones y activos mediante recolección de datos y entrevistas técnicas.
* Definición clara de alcances y tareas utilizando herramientas como tableros de seguimiento.
* Aplicación de metodologías de análisis para evaluar el estado actual del sistema antes de definir acciones de mejora.

1. **Administración de Servidores, Sistemas Operativos, Seguridad Informática**

Estos conocimientos fueron esenciales durante el diseño del entorno de pruebas y la ejecución de análisis de vulnerabilidades. Lo que se logró fue:

* Configurar un entorno aislado con contenedores Podman para replicar de manera segura la aplicación.
* Emplear herramientas de escaneo automatizado para detectar fallas de seguridad en tiempo de ejecución y en el código fuente.

1. **Fundamentos de Bases de Datos, Administración de Bases de Datos, Seguridad en Bases de Datos**

Parte del proyecto implicó evaluar el uso y configuración de las bases de datos involucradas. Estas competencias me ayudaron a:

* Auditar configuraciones y niveles de acceso a las bases de datos que usa la aplicación.
* Verificar el cumplimiento de normas de seguridad, como la separación de privilegios y cifrado de datos sensibles.
* Documentar los hallazgos y proponer ajustes según las buenas prácticas de seguridad.

**Competencias genéricas**

Además de las competencias técnicas, durante el proyecto desarrollé habilidades genéricas que fortalecen mi perfil profesional:

1. **Trabajo en equipo**

Colaboré activamente con personal de diferentes áreas como desarrollo, ciberseguridad e infraestructura, coordinando tareas en conjunto y asegurando que cada cambio fuera aprobado y probado correctamente.

1. **Comunicación efectiva**

Participé en reuniones técnicas y de seguimiento donde expuse resultados, riesgos y propuestas de mejora. También redacté documentación clara y accesible tanto para perfiles técnicos como administrativos.

1. **Organización y gestión del tiempo**

Dividí el proyecto en etapas y cumplí los plazos establecidos, priorizando actividades críticas como la detección de vulnerabilidades y aplicación de correcciones urgentes.

1. **Resolución de problemas**

Enfrenté desafíos técnicos como la compatibilidad entre versiones antiguas de PHP y dependencias obsoletas. Esto me permitió aplicar mis habilidades analíticas para encontrar soluciones viables sin comprometer la funcionalidad existente.

Capítulo: Fuentes de Información

11. Referencias bibliográficas y virtuales

Anexos: