**Biblioteca INFOTEC**

Ciudad de México, a 2 de abril de 2025

# VISTO BUENO DE TRABAJO TERMINAL

**Técnico Superior Universitario en Ciberseguridad**

**UNIDAD DE POSGRADOS**
**PRESENTE**

Por medio de la presente se hace constar que el **Reporte final** desarrollado por el alumno: **Roberto Carlos González Bernal** cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que el alumno no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Dr. Juan Antonio Vega Garfias
Subgerente de Innovación Gubernamental

JAVG/jah

C.c.p. Mtra. Analy Mendoza Rosales. – Encargada de la Gerencia de Capital Humano. - Para su conocimiento.
Roberto Carlos González Bernal. – Alumno Técnico Superior Universitario en Ciberseguridad.- Para su conocimiento.

Jah

2025 Año de La Mujer Indígena

# Reporte final

# Roberto Carlos González Bernal

Datos eliminados: matrícula, correo, celular; con fundamento en lo establecido en los artículos 65, fracción II, 98, fracción III, 113, fracción I y último párrafo de la Ley Federal de Transparencia y Acceso a la Información Pública, 44, fracción II, 106, fracción III y 116 de la Ley General de Transparencia y Acceso a la Información Pública, así como a lo establecido en los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas, por tratarse de datos personales concernientes a una persona física identificada, en la modalidad de confidencial. Área Dirección Adjunta de Innovación y Conocimiento. Periodo indefinido, toda vez que no está sujeta a temporalidad alguna y solo podrán tener acceso a ella los titulares de la misma. Aprobada en la Primera Sesión Extraordinaria del Comité de Transparencia de INFOTEC ejercicio 2025.

# Índice


**Índice** ..... 2

**1. Introducción** ..... 3

1.1. Actividades Previas ..... 3

1.2. Vulnerabilidades Detectadas ..... 3

1.3. Aplicaciones Afectadas ..... 3

1.4. Recomendaciones y Links de Referencia ..... 3

1.5. Evidencias ..... 3

**2. Práctica profesional** ..... 5

**3. Estructura organizacional: INFOTEC** ..... 6

3.1. Sector de actividad ..... 6

3.2. Presentación de la empresa e historia de la empresa ..... 6

3.3. Características Clave de la Identidad de INFOTEC ..... 7

3.4. Organización de la empresa. ..... 7

3.5. Comité Técnico ..... 8

3.6. Estructura Orgánica ..... 8

3.7. Política de la Organización ..... 9

3.8. Organigrama ..... 9

**4. Informe de la práctica profesional** ..... 11

4.1. Descripción de las funciones ..... 11

4.2. Desglose de actividades ..... 11

4.3. Bitácora de prácticas ..... 13

**5. Conclusiones** ..... 14

5.1. Cuadro CQA de mi estancia en la organización ..... 15

**6. Evaluación de desempeño** ..... 16

6.1. Evaluación del Desempeño ..... 16

6.2. Apoyo del Conocimiento Previo ..... 16

6.3. Conclusión ..... 16

**7. Referencias** ..... 17

# 1. Introducción

Este informe presenta el análisis de seguridad realizado a diversas aplicaciones web de INFOTEC, con el objetivo de identificar vulnerabilidades potenciales y evaluar la posibilidad de su explotación por parte de atacantes. El propósito es determinar el nivel de intrusión que podría alcanzarse, proporcionando una visión integral de las principales debilidades detectadas, así como recomendaciones para su mitigación.

A continuación, se describe de manera general el contenido y estructura de cada informe técnico desarrollado:

## 1.1. Actividades Previas

Se detallan los pasos iniciales del análisis, incluyendo escaneos de puertos *TCP* y *UDP*, reconocimiento de versiones de software y recopilación de datos básicos de configuración.

## 1.2. Vulnerabilidades Detectadas

Cada vulnerabilidad identificada es descrita con un enfoque técnico, incluyendo su criticidad, impacto y evidencia recopilada. Entre las vulnerabilidades más recurrentes se incluyen:

- Exposición de encabezados *HTTP* y versiones de software.
- Falta de configuraciones avanzadas en certificados *SSL*.
- Ausencia de encabezados de seguridad como *X-Content-Type-Options* y *X-Frame-Options*.
- Métodos HTTP inseguros o mal configurados.
- Uso de configuraciones estándar en servicios SSH y STUN.

## 1.3. Aplicaciones Afectadas

Se enumeran las aplicaciones web analizadas, como bitwarden-gep.infotec.mx, repositorio-contrataciones.infotec.mx, servicedesk.infotec.mx, entre otras, indicando las tecnologías y configuraciones específicas evaluadas.

## 1.4. Recomendaciones y Links de Referencia

Se presentan propuestas de mitigación basadas en las mejores prácticas y estándares de seguridad, con enlaces a documentación técnica relevante.

## 1.5. Evidencias

Capturas y logs que respaldan los hallazgos, facilitando su comprensión y validación.

Este análisis proporciona una base sólida para mejorar la postura de seguridad de las aplicaciones evaluadas, reduciendo riesgos y fortaleciendo la protección frente a posibles amenazas.

---

***NOTA:*** *No se presenta ni adjunta la bitácora de actividades* ***por ser de carácter confidencial****, si se requiere la misma, se debe solicitar autorización a mi asesor, si se autoriza la entrega de esta, se puede proporcionar para su revisión en un anexo.*

---

***Agradezco públicamente a mi asesor Ing. Ulises López, quien mostró un interés permanente y se mostró receptivo a todo requerimiento y solicitud de mi parte. Así mismo el invaluable apoyo de Luz Estefani quien siempre ha estado al tanto para que todo se realice en tiempo y forma y sobre facilitando todos los procesos académicos, administrativos y de vinculación de las prácticas profesionales.***

---

## 2. Práctica profesional

| Datos personales del estudiante | | | |
|---|---|---|---|
| Nombre completo: | Roberto Carlos González Bernal | | |
| Matrícula: | Eliminado | Teléfono: | Eliminado |
| Correo: | Eliminado | | |
| Especialidad de TSU: | Ciberseguridad | | |
| Año: | 2024 | Celular: | Eliminado |
| Número de horas de práctica profesional: | | 280 | |

| Datos de la institución | |
|---|---|
| Nombre de la institución: | INFOTEC |
| Departamento en el que realizarás tus prácticas: | Infraestructura Tecnológica |
| Nombre de la persona responsable del departamento: | Ulises López |

# 3. Estructura organizacional: INFOTEC

Para elaborar esta sección me he apoyado en la información establecida por INFOTEC en su Normateca (2024), la cual se documenta en las referencias al final del documento[1].

## 3.1. Sector de actividad

INFOTEC es una institución pública dedicada a la investigación y el desarrollo tecnológico. Es un órgano desconcentrado del CONAHCYT y forma parte del sector público.

## 3.2. Presentación de la empresa e historia de la empresa

INFOTEC, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, es un Centro Público de Investigación del Gobierno Federal mexicano, adscrito al Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONHACYT). Su misión es contribuir a la transformación digital de México mediante la investigación, innovación, formación académica y desarrollo de productos y servicios en el ámbito de las Tecnologías de la Información y Comunicación (TIC).

Fundado en 1974 como un fideicomiso público del CONHACYT, INFOTEC inició brindando servicios de información, documentación y biblioteca, enfocándose en la modernización industrial a través de la difusión de novedades técnicas, incluyendo patentes, diseños y prototipos.

A lo largo de más de cuatro décadas, INFOTEC ha evolucionado significativamente, destacando los siguientes hitos:

- **1980**: Participación en el desarrollo de la Red ARPANET, precursora de Internet, lo que sentó la base tecnológica del desarrollo de Internet en México.
- **1999**: Transformación en un centro de servicios de tecnologías de Internet y desarrollo de COMPRANET, el primer sistema latinoamericano de adquisiciones gubernamentales, reconocido con el premio Reto Estocolmo.
- **2009**: Creación de Semantic Web Builder (SWB), una solución semántica para mejorar el desempeño en la red, ofrecida de forma gratuita para el desarrollo y administración de portales de Internet con tecnología semántica.
- **2013**: Inauguración de un centro de datos certificado en el nivel TIER III por el Uptime Institute y un edificio de investigación en Aguascalientes, consolidando su infraestructura tecnológica.

[1] *Telecomunicaciones*. (s. f.). Gob.mx. Recuperado 7 de abril de 2025, de https://www.proyectosmexico.gob.mx/como-invertir-en-infraestructura-en-mexico/ciclo-inversion/ciclos-telecomunicaciones/#tab-id-5

Actualmente, INFOTEC cuenta con sedes en la Ciudad de México y Aguascalientes, ofreciendo servicios que abarcan desarrollo de software, Internet de las Cosas (IoT), infraestructura tecnológica, investigación y docencia. Su oferta académica incluye programas de maestría y doctorado en áreas como dirección estratégica, gestión de innovación, derecho de las TIC, ciencia de datos y sistemas embebidos.

Como parte de la red de Centros Públicos de Investigación del CONHACYT, INFOTEC se alinea con la Estrategia Digital Nacional, posicionándose como un proveedor clave de servicios TIC para dependencias y entidades del Gobierno de México, contribuyendo al avance tecnológico y digital del país.

### 3.3. Características Clave de la Identidad de INFOTEC

1. **Enfoque en Innovación y Desarrollo**: INFOTEC impulsa proyectos tecnológicos que abordan problemáticas nacionales y generan impacto social, colaborando con instituciones gubernamentales, académicas y empresas para fortalecer el ecosistema digital mexicano.
2. **Compromiso con la Educación y la Capacitación**: La entidad también se enfoca en la formación de talento especializado mediante programas de capacitación y desarrollo profesional en áreas como ciberseguridad, inteligencia artificial, big data y blockchain.
3. **Responsabilidad en Seguridad de la Información**: INFOTEC se especializa en ofrecer soluciones seguras, destacándose en el desarrollo de tecnologías robustas para la protección de datos, consultoría en seguridad de la información y cumplimiento regulatorio, un enfoque esencial en un entorno cada vez más digital y regulado.
4. **Investigación en Tecnologías Emergentes**: INFOTEC lidera proyectos de investigación en TIC avanzadas, incluyendo inteligencia artificial, sistemas de monitoreo, gestión de datos y aplicaciones en el ámbito educativo y gubernamental, fomentando el avance de tecnologías emergentes en México.

INFOTEC refleja una identidad enfocada en el crecimiento y fortalecimiento del sector TIC en México, combinando innovación, seguridad y educación como pilares fundamentales para contribuir al desarrollo tecnológico del país.

### 3.4. Organización de la empresa.

INFOTEC, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, es una entidad paraestatal del Gobierno Federal mexicano, adscrita al Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONHACYT). Su estructura

organizacional está diseñada para cumplir con su misión de mejorar la competitividad, transparencia y eficiencia de diversas organizaciones a través de actividades de investigación, innovación, desarrollo y consultoría en el ámbito de las TIC.

### 3.5. Comité Técnico

Como órgano supremo de decisión, el Comité Técnico de INFOTEC aprueba políticas, estrategias y programas que guían las acciones de la institución. Este comité toma decisiones sobre el uso y destino de los recursos autogenerados y se reúne al menos dos veces al año.

### 3.6. Estructura Orgánica

La estructura organizacional de INFOTEC se detalla en su Manual de Organización, el cual proporciona una visión integral de las funciones y responsabilidades de cada área.

Este documento está disponible en la Normateca de INFOTEC, que ofrece acceso a reglamentos, manuales y políticas que regulan la operación de la institución.

**Figura 1**

*Estructura orgánica de la Dirección Adjunta de Administración de INFOTEC*


Tomado de **Manual de organización de la Dirección Adjunta de Administración**, por Fondo de Información y Documentación para la Industria INFOTEC, (s. f.), https://www.infotec.mx/work/models/Infotec/normateca/admin/manual_de_organizacion_de_la_direccion_adjunta_de_administracion.pdf

## 3.7. Política de la Organización

INFOTEC se compromete a ofrecer productos y servicios tecnológicos de calidad, protegiendo la confidencialidad, integridad y disponibilidad de la información, estableciendo mecanismos para la continuidad del negocio y cumpliendo con los requisitos legales y contractuales aplicables.

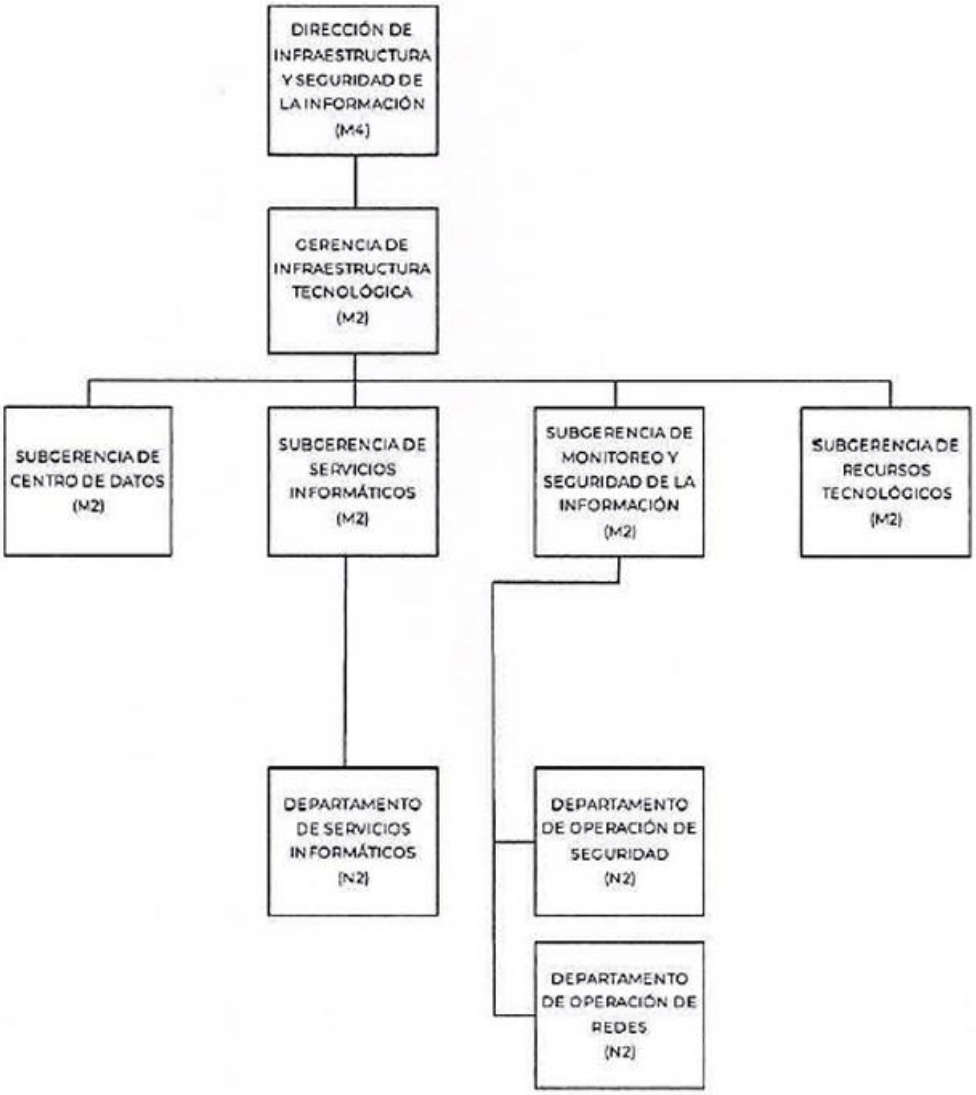
Esta estructura organizacional permite a INFOTEC cumplir eficazmente con su propósito de impulsar la transformación digital en México, alineándose con las directrices del CONHACYT y las necesidades del sector público, académico, social y privado.

## 3.8. Organigrama

El organigrama específico del área en que realicé mis prácticas se presenta a continuación.

**Figura 2**

*Organigrama de la Dirección de Infraestructura y Seguridad de la Información*




Tomado de **Fondo de Información y Documentación para la Industria INFOTEC.** (2024). *Manual de organización*. https://www.infotec.mx/es_mx/Infotec/Normateca

# 4. Informe de la práctica profesional

## 4.1. Descripción de las funciones

El análisis de seguridad realizado a las aplicaciones web de INFOTEC tiene como objetivo identificar y mitigar vulnerabilidades que puedan comprometer la integridad, disponibilidad y confidencialidad de los sistemas. Las funciones desarrolladas se centran en la ejecución de auditorías técnicas de seguridad, documentación de hallazgos, y propuestas de mejora. Estas incluyen:

1. Escaneo de Puertos y Análisis de Redes.
2. Uso de herramientas como *Nmap* para identificar puertos abiertos, servicios en ejecución y configuraciones relacionadas.
3. Detección de Vulnerabilidades en Aplicaciones Web.
4. Evaluación de encabezados *HTTP*, certificados *SSL*, configuraciones de seguridad, y métodos *HTTP* permitidos.
5. Documentación y Clasificación de Vulnerabilidades.
6. Clasificación de hallazgos por criticidad e impacto utilizando estándares como OWASP, que identifica las principales vulnerabilidades en aplicaciones web, y CWE, que proporciona una taxonomía detallada de debilidades de seguridad en el software.
7. Elaboración de Reportes Técnicos detallados que incluyen evidencia recopilada, recomendaciones y referencias técnicas.

## 4.2. Desglose de actividades

Mi rol consistió en las actividades que se resumen a continuación:

1. **Recopilación de Información Previa**
    a. Realización de escaneos iniciales de puertos *TCP* y *UDP* utilizando herramientas como *Nmap* y *Nessus*.
    b. Identificación de las versiones de software en los servicios expuestos.
    c. Registro de rutas de acceso a recursos y configuraciones detectadas, como robots.txt y encabezados *HTTP*.
2. **Identificación y documentación de vulnerabilidades**
    a. Análisis de configuraciones de certificados *SSL* y seguridad de los encabezados *HTTP*.

   b. Análisis de encabezados clave, como *X-Frame-Options* y *X-Content-Type-Options*.

3. **Identificación de configuraciones inseguras en servicios como SSH y STUN.**
4. **Generación de Evidencias.**
5. **Captura de pantallas, registros (logs) y resultados de pruebas realizadas.**
6. **Organización y presentación de la evidencia recopilada de forma clara en los informes técnicos.**
7. **Presentación de propuestas de mitigación.**
8. **Redacción de recomendaciones técnicas breves para mitigar las vulnerabilidades detectadas.**
9. **Elaboración de Informes Técnicos** con la información recolectada, incluyendo contenido técnico y referencias.
10. **Verificación que los informes cumplieran con los lineamientos de confidencialidad y estándares de calidad establecidos por INFOTEC.**

## 4.3. Bitácora de prácticas

| Semanas | Actividades realizadas |
|---|---|
| 1 a 2 | • **Reuniones iniciales para explicar el alcance de las actividades a realizar**<br>• **Asignación de actividades por parte de nuestro asesor**<br>• **Ronda de dudas y preguntas** |
| 3 a 4 | • **Análisis y gestión de actividades para el objetivo:**<br>  ○ ***bitwarden-gep.infotec.mx***<br>• **Escaneos y análisis del objetivo.**<br>• **Recopilación de datos**<br>• **Elaboración del informe de resultados.** |
| 5 a 6 | • **Análisis y gestión de actividades para el objetivo:**<br>  ○ ***repositorio-contrataciones.infotec.mx***<br>  ○ ***zabbix-finabien.infotec.mx***<br>• **Escaneos y análisis del objetivo.**<br>• **Recopilación de datos**<br>• **Elaboración del informe de resultados.** |
| 7 a 8 | • **Análisis y gestión de actividades para el objetivo:**<br>  ○ ***servicedesk.infotec.mx***<br>• **Escaneos y análisis del objetivo.**<br>• **Recopilación de datos**<br>• **Elaboración del informe de resultados.** |
| 9 a 10 | • **Análisis y gestión de actividades para el objetivo:**<br>  ○ ***av.infotec.mx***<br>• **Escaneos y análisis del objetivo.**<br>• **Recopilación de datos**<br>• **Elaboración del informe de resultados.** |
| 11 a 12 | • **Análisis y gestión de actividades para el objetivo:**<br>  ○ ***tsu.infotec.edu.mx***<br>• **Escaneos y análisis del objetivo.**<br>• **Recopilación de datos**<br>• **Elaboración del informe de resultados.** |

## 5. Conclusiones

Mi estancia profesional representó una experiencia enriquecedora tanto a nivel personal como profesional. A través de las actividades realizadas, pude consolidar mis conocimientos en análisis de vulnerabilidades y seguridad informática, aplicándolos en un entorno real y bajo estándares técnicos rigurosos.

Durante el desarrollo de los reportes técnicos, logré entender la importancia de la documentación estructurada y detallada para presentar hallazgos y propuestas de mejora de manera efectiva. Cada actividad realizada, desde los escaneos iniciales hasta la elaboración de evidencias y recomendaciones, me permitió aplicar herramientas y metodologías aprendidas durante mi formación académica.

Además, esta experiencia me enseñó la relevancia del trabajo colaborativo, ya que la creación de los reportes requería coordinación con los equipos involucrados y la alineación con las políticas de INFOTEC. Este aprendizaje no solo fortaleció mis habilidades técnicas, sino también mis capacidades de comunicación y organización.

La vinculación entre esta estancia y los reportes subidos al aula virtual radica en que ambos reflejan un proceso de aprendizaje continuo, donde la teoría se aplicó en práctica tangible. Estos documentos son una evidencia concreta del conocimiento adquirido, el cual será un pilar fundamental para mi desarrollo profesional en el ámbito de la ciberseguridad.

En resumen, mi estancia profesional me proporcionó las herramientas y la confianza necesarias para enfrentar futuros desafíos en mi carrera, permitiéndome aportar valor real a los proyectos en los que participe más adelante.

## 5.1. Cuadro CQA de mi estancia en la organización

| C<br>¿Qué **C**onozco? | Q<br>¿**Q**ué aporte? | A<br>¿Qué **A**prendí? |
|---|---|---|
| Conocimientos en análisis de vulnerabilidades y herramientas como *Nmap*, *Nessus*, *Nikto*, *OWASP* y estándares de seguridad | Realicé evaluaciones técnicas detalladas, documentando vulnerabilidades y proponiendo medidas correctivas basadas en estándares reconocidos. | Aprendí a aplicar técnicas avanzadas de escaneo y análisis, y a generar informes técnicos claros y útiles para la toma de decisiones organizacionales. |
| Habilidades en redacción de reportes técnicos y manejo de herramientas de escaneo. | Generé documentos detallados con evidencias de los hallazgos, incluyendo referencias técnicas y recomendaciones específicas para cada vulnerabilidad identificada. | Mejoré mis capacidades de organización, redacción técnica y uso de herramientas para respaldar mis hallazgos con evidencia clara y verificable. |
| Actitud proactiva y disposición para colaborar en equipos multidisciplinarios. | Contribuí con ideas y enfoques para optimizar los procesos de análisis, trabajando de manera colaborativa con los equipos técnicos y de seguridad. | Aprendí a trabajar eficientemente en equipo y a coordinar esfuerzos para cumplir con los objetivos establecidos en tiempo y forma. |
| Conocimientos en normativas y estándares internacionales de seguridad, como *OWASP* y *CVE*. | Proporcioné análisis alineados con estos estándares, asegurando la calidad y precisión en los resultados obtenidos. | Aprendí a interpretar y aplicar normativas de seguridad para garantizar que los sistemas evaluados cumplan con los requisitos de seguridad esperados. |
| Conocimientos sobre técnicas de autoaprendizaje y actualización constante en ciberseguridad. | Busqué nuevas tendencias y mejores prácticas en el ámbito de la ciberseguridad para integrarlas en mis análisis y recomendaciones. | Desarrollé una rutina de aprendizaje continuo, consultando fuentes confiables para mantenerme al día en un campo dinámico y cambiante. |

# 6. Evaluación de desempeño

Durante mi estancia profesional en la organización, considero que mi desempeño fue satisfactorio y alineado con las expectativas del proyecto. Mi capacidad para aplicar el conocimiento adquirido previamente en otros ciclos académicos jugó un papel crucial en la realización de las actividades asignadas.

## 6.1. Evaluación del Desempeño

- **Compromiso y Responsabilidad**: Mantener un enfoque proactivo y organizado me permitió cumplir con los objetivos asignados dentro de los plazos establecidos, asegurando la calidad de cada entrega.
- **Dominio Técnico**: Las herramientas y conceptos aprendidos en ciclos anteriores, como el manejo de *Nmap*, *OWASP* y la redacción técnica, fueron fundamentales para abordar las auditorías de seguridad y generar reportes con hallazgos y recomendaciones claras.
- **Adaptabilidad**: Me adapté rápidamente a las dinámicas y procesos internos de la organización, integrándome con el equipo y aplicando las metodologías requeridas de forma eficiente.

## 6.2. Apoyo del Conocimiento Previo

- **Ciclos Académicos Previos**: Los conocimientos adquiridos en materias como análisis de redes, seguridad informática y programación me permitieron comprender las vulnerabilidades y métodos de ataque evaluados durante los análisis.
- **Proyectos Anteriores**: La experiencia previa en trabajos de investigación y desarrollo técnico me ayudó a estructurar y documentar los resultados obtenidos de forma profesional y alineada con los estándares requeridos por la organización.
- **Habilidades Transversales**: Las habilidades en comunicación, trabajo en equipo y resolución de problemas adquiridas en ciclos previos fueron esenciales para colaborar con colegas y enfrentar desafíos técnicos.

## 6.3. Conclusión

Mi estancia profesional no solo me permitió aplicar los conocimientos adquiridos, sino también fortalecer habilidades clave que serán indispensables en mi desarrollo laboral futuro. Al reflexionar sobre mi desempeño, considero que esta experiencia consolidó mi perfil técnico y profesional, preparándome para asumir retos más complejos en el ámbito de la ciberseguridad.

## 7. Referencias


I. Caulfield, J. (2021, 29 abril). Cómo citar una imagen en formato APA. Scribbr. Recuperado el 6 de abril de 2025, de https://www.scribbr.es/normas-apa/ejemplos/imagen/

II. Dragon. (2015, marzo 26). ¿Cómo se realiza un Pentest? DragonJAR - Servicios de Seguridad Informática. https://www.dragonjar.org/como-realizar-un-pentest.xhtml

III. Fondo de Información y Documentación para la Industria INFOTEC. (2024). Manual de organización. Recuperado el 6 de abril de 2025, de https://www.infotec.mx/es_mx/Infotec/Normateca

IV. Fondo de Información y Documentación para la Industria INFOTEC. (s. f.). Manual de organización de la Dirección Adjunta de Administración. INFOTEC. Recuperado el 6 de abril de 2025, de https://www.infotec.mx/work/models/Infotec/normateca/admin/manual_de_organizacion_de_la_direccion_adjunta_de_administracion.pdf

V. Hamilton, T. (2024, junio 17). Tutorial de pruebas de penetración: ¿Qué es PenTest? Guru99. https://www.guru99.com/es/learn-penetration-testing.html

VI. Hernandez, M. (2022, enero 26). Pentesting con OWASP: fases y metodología. Blog de Hiberus; Hiberus. https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

VII. Jerez, L. V. (s. f.). *Habilidades blandas deseables en profesionales de TI por empleadores de la empresa privada y pública costarricense. Infotec.mx. Recuperado el 29 de octubre de 2024, de https://aulavirtual.infotec.mx/pluginfile.php/113201/mod_page/content/68/3.%20Habilidades%20blandas%20deseables%20en%20profesionales%20de%20TI.pdf

VIII. Las 10 habilidades que necesitarás en tu trabajo en el 2020. (s. f.). Infotec.mx. Recuperado el 29 de octubre de 2024, de https://aulavirtual.infotec.mx/pluginfile.php/113201/mod_page/content/68/2.%20Las%2010%20habilidades%20que%20necesitara%CC%81s%20en%20tu%20trabajo%20en%20el%202020.pdf

IX. Máximo Abel Ramírez Chávez, N. N. M. F. (s. f.). Habilidades blandas y habilidades duras, clave para la formación profesional integral. Infotec.mx. Recuperado el 29 de octubre de 2024, de https://aulavirtual.infotec.mx/pluginfile.php/113201/mod_page/content/68/1.%20Habilidades%2Bblandas%2By%2Bhabilidades%2Bduras.pdf?time=1700777441515

X. Órgano de Gobierno. (s. f.). Edu.mx. Recuperado el 1 de diciembre de 2024, de https://infotec.edu.mx/es_mx/Infotec/Organo-de-Gobierno

XI. Pruebas de penetración para principiantes: 5 herramientas para empezar. (s. f.). Unam.mx. Recuperado el 28 de octubre de 2024, de https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

XII. ¿Qué es INFOTEC? (s. f.). Infotec.mx. Recuperado el 1 de diciembre de 2024, de https://www.infotec.mx/Infotec

XIII. Sánchez, M. (2024, junio 25). Penetration Test (Pentest): ¿En qué consiste? OpenSecurity. https://www.opensecurity.es/penetration-test-pentest-en-que-consiste/

XIV. Secure, N. L. T. (2021, octubre 8). ¿Cómo hacer un pentest? Nltsecure.com. https://www.nltsecure.com/blog/como-hacer-un-pentest-nlt-secure-expertos-en-ciberseguridad

XV. TOTAL: CompTIA PenTest+ (Ethical Hacking) PT0-002 + 2 Tests. (s. f.). Udemy.com. Recuperado el 28 de octubre de 2024, de https://www.udemy.com/course/ethical-hacking-and-comptia-pentest-exam-prep-pt0-001