Biblioteca INFOTEC

Ciudad de México, a 19 de mayo 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 la alumna: **Lourdes Escobar Rodríguez** 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 la alumna 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.
Lourdes Escobar Rodríguez. – Alumna Técnico Superior Universitario en Ciberseguridad.- Para su conocimiento.

Reporte final

Datos eliminados: matrícula, correo, celular, teléfono; 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

Introducción

Este documento tiene como propósito plasmar lo realizado durante las estancias profesionales en el INFOTEC.

Durante las 12 semanas estuve realizando investigaciones sobre las herramientas a utilizar, así como los reportes de las 6 ligas que se me asignaron por parte del profesor Arturo, en la mayoría de las ligas encontré vulnerabilidades de CSP no configurado, Clickjacking, archivo oculto y metadatos.

De acuerdo a la red Developer.mozilla, la Política de Seguridad del Contenido o (CSP) - del inglés Content Security Policy - es una capa de seguridad adicional que ayuda a prevenir y mitigar algunos tipos de ataque, incluyendo Cross Site Scripting (XSS) y ataques de inyección de datos. Los ataques XSS se aprovechan de la confianza del navegador en el contenido que recibe del servidor y el navegador de la víctima ejecutará los scripts maliciosos porque confía en la fuente del contenido, aun cuando dicho contenido no provenga de donde se supone.

Mientras que el Clickjacking de acuerdo con la página de comunidad de OWASP dice que es básicamente como “secuestrar” clics para la página del atacante y enrutarlos a otra página. Dentro de esta página de comunidad nos dan un ejemplo sobre el Clickjacking, como cuando un atacante que construye un sitio web que tiene un botón en él qué dice “haga clic aquí para obtener un iPod” gratis.

En un Post del aplicativo Avast antivirus, dice que los metadatos son los datos ocultos que acompañan a cada imagen, vídeo y archivo que encuentre, sirven para organizar y gestionar conjuntos de datos.

Práctica profesional

Datos personales del estudiante			
Nombre completo:	Lourdes Escobar Rodríguez		
Matrícula:	Eliminado	Teléfono:	N/A
Correo:	Eliminado		
Especialidad de TSU:	Ciberseguridad		
Año:	2024	Celular:	Eliminado
Número de horas de práctica profesional:		240	

Datos de la institución	
Nombre de la institución:	INFOTEC, Centro de Investigación e Innovación en TIC.
Departamento en el que realizarás tus prácticas:	Ciberseguridad
Nombre de la persona responsable del departamento:	Ing. Arturo Montoya

Estructura organizacional

- **El sector de actividad**

Tecnología, Ciberseguridad.

- **Presentación de la empresa e historia de la empresa**

De acuerdo con la página oficial del INFOTEC, es un Centro Público de Investigación del Gobierno Federal que contribuye a la Transformación académica y el desarrollo de productos y servicios TIC.

Así mismo en la página oficial del INFOTEC comentan sobre la trayectoria que ha tenido, desde sus orígenes en el año de 1974, se ha hecho notar en materia de novedades industriales y en estas últimas décadas en la instrumentación de proyectos de tecnologías de información y comunicación (TIC). Actualmente el INFOTEC cuenta con dos sedes, uno en la Ciudad de México y otra en Aguascalientes. Sus principales líneas de negocio son el desarrollo de software, el internet de las cosas (IoT), infraestructura tecnológica, también la investigación y docencia.

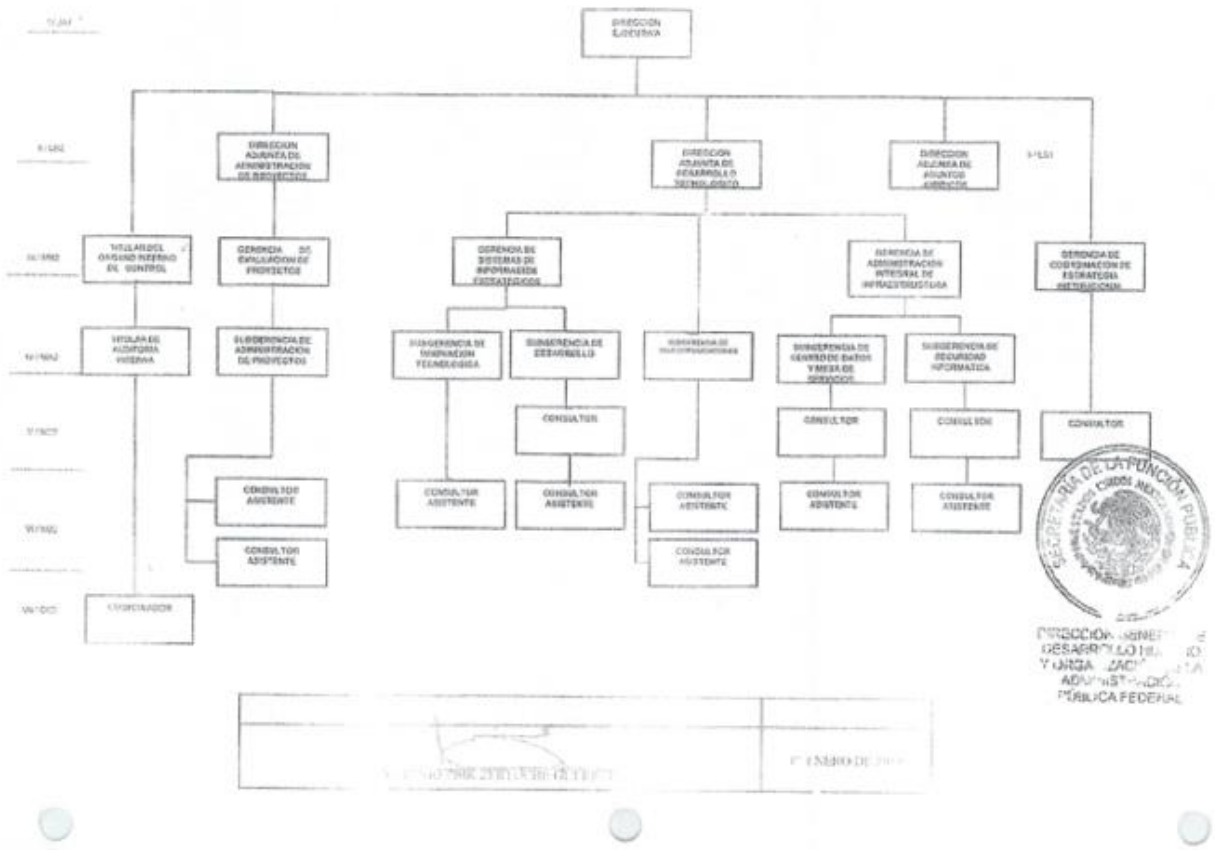
- **La organización de la empresa (incluir organigrama)**

En el manual de organización del INFOTEC dice que se integra por una estructura orgánica, con las siguientes direcciones:

- Dirección Adjunta de Asuntos Jurídicos.
- Gerencia de Coordinación de Estrategia Institucional
- Dirección Adjunta de Administración.
- Dirección Adjunta de Desarrollo Tecnológico.
- Dirección Adjunta de Competitividad.
- Dirección Adjunta de Innovación y Conocimiento.
- Dirección Adjunta de Administración de Proyectos.

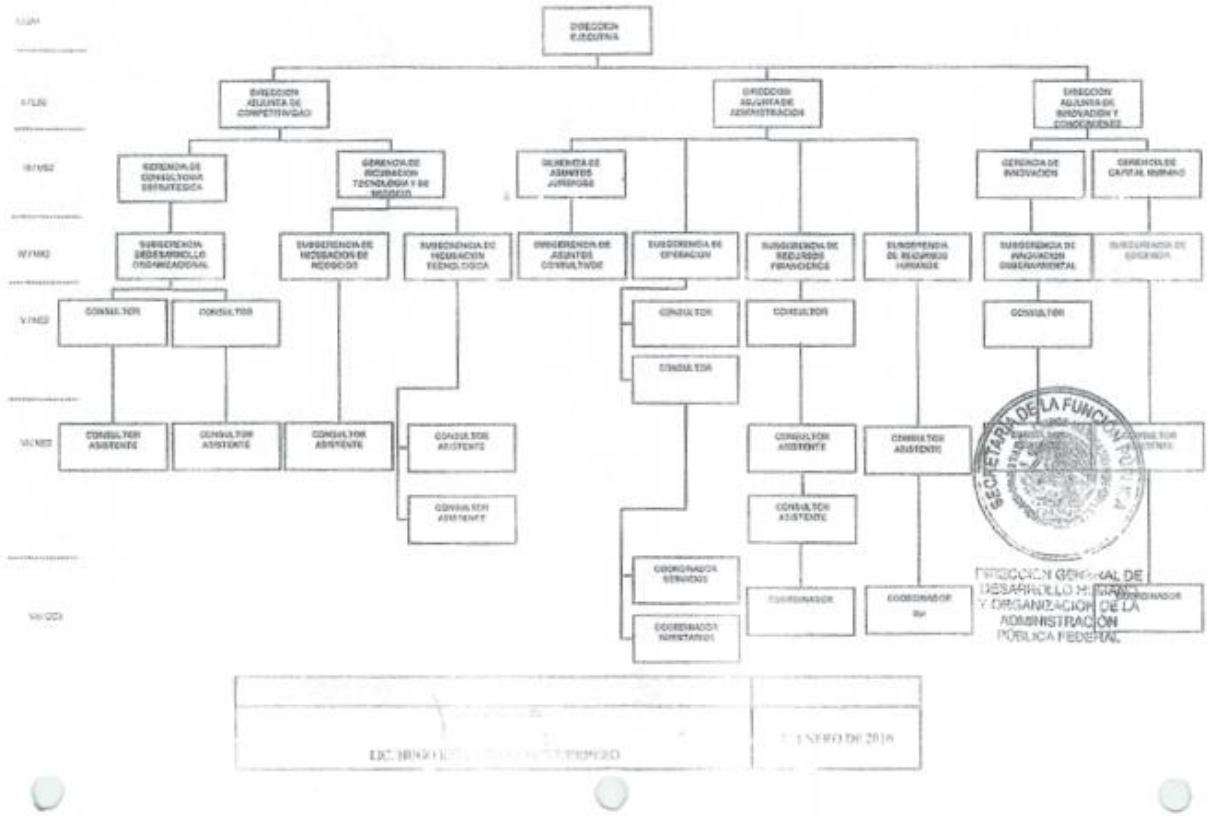
FONDO DE INFORMACION Y DOCUMENTACION PARA LA INDUSTRIA

PRIMERA PARTE



FONDO DE INFORMACION Y DOCUMENTACION PARA LA INDUSTRIA

SEGUNDA PARTE



1 ENERO DE 2018

Informe de la práctica profesional

- **Descripción de las funciones**

En cada una de las ligas que nos compartió el profesor, se debe revisar que hay acceso normal desde cualquier navegador, así como hacer un reconocimiento de vulnerabilidades.

- **Desglose de actividades**

En las 240 horas de prácticas, realicé los análisis de vulnerabilidades y sobre los puertos abiertos en cada una de las ligas, así como la investigación pertinente sobre las herramientas que utilicé, como son:

- Nmap.
- Burpsuite.
- OWASP ZAP.
- Nikto.

- **Bitácora de prácticas**

Semanas	Actividades realizadas	Observaciones
1 a 2	Estuve realizando investigación sobre los análisis de puertos abiertos en la primera liga que nos compartió el Ing. Arturo, sin embargo, me dio retroalimentación de lo que se esperaba en el reporte por lo que lo corregí y lo compartí nuevamente. Encontré vulnerabilidades de CSP.	Se adjuntan por correo los informes generados con las herramientas de NMAP y ZAP.
3 a 4	Continué con la investigación en las herramientas que utilicé para el escaneo de puertos y de vulnerabilidades, utilicé OWASP ZAP para realizar un monitoreo de las amenazas que tenía la segunda liga de las 6 que nos asignó el profesor, así como estuve trabajando con NMAP para conocer los puertos abiertos e investigar un poco más al respecto. Encontré vulnerabilidades como: Clickjacking, archivo oculto metadatos.	Se adjuntan por correo los informes generados con las herramientas de NMAP y ZAP.
5 a 6	Estuve realizando el escaneo de las vulnerabilidades con las herramientas de OWASP y NMAP para conocer las vulnerabilidades, aunque tuve un ligero inconveniente con mi equipo y con la virtualización de kali Linux, al final lo resolvíy pude entregar mi tercer reporte, donde encontré la vulnerabilidad de Slowloris DOS	Se adjuntan por correo los informes generados con las herramientas de NMAP y ZAP.

	attack.	
7 a 8	En estas semanas estuve investigando un poco sobre otra herramienta llamada Metasploit, con la cual realicé un escaneo de vulnerabilidades y entregué mi cuarto reporte, en el cual encontré 3 vulnerabilidades, como el CSP, Clickjacking y el servidor filtra información de versión a través del campo server.	Se adjuntan por correo los informes generados con las herramientas de NMAP, ZAP y Metasploit.
9 a 10	En estas semanas estuve investigando otra herramienta con la cual también realicé escaneos, con Nikto, sin embargo, como no comprendí mucho al respecto continué realizando mis reportes con NMAP y ZAP, por lo que mis reportes contienen en su mayoría dichas herramientas.	Se adjuntan por correo los informes generados con las herramientas de NMAP y ZAP.
11 a 12	En esta última semana realicé un escaneo de las últimas ligas que tenía asignadas, por lo que utilicé NMAP, ZAP y Nikto para hacer un análisis de vulnerabilidades y en la liga no encontré vulnerabilidades, únicamente la de CSP y con un nivel medio.	Se adjuntan por correo los informes generados con las herramientas de NMAP, ZAP y Nikto.

Conclusiones

Estas estancias profesionales me dieron la oportunidad para adquirir experiencia práctica en el uso de herramientas de ciberseguridad, como Nmap, ZAPROXY, Metasploit y Nikto, herramientas que son fundamentales en el ámbito de la seguridad informática y nos permiten a nosotros los estudiantes desarrollar habilidades críticas en el análisis y la mitigación de vulnerabilidades.

Me hubiera gustado un poco más de involucramiento por parte del docente a cargo y del área de ciberseguridad, ya que en algunas ocasiones me llegué a sentir confundida sobre lo que buscaba el profesor ver en los reportes, sin embargo, al acercarme y compartir mis dudas me orientó y me apoyó para la entrega de los reportes.

Con estas estancias me llevo una enriquecedora experiencia, ya que la combinación de teoría y práctica es esencial para formar profesionales competentes que puedan contribuir significativamente a la seguridad informática.

Cuadro CQA de mi estancia en la organización

C ¿Qué **C**onozco?	Q ¿**Q**ué aporte?	A ¿Qué **A**prendí?
Herramientas de análisis de puertos abiertos, vulnerabilidades y la estructura de los informes al documentar las vulnerabilidades y sus posibles soluciones por aplicar y mitigar los riesgos.	Información que puede llegar a considerarse para investigar más sobre las vulnerabilidades que encontré. Mitigar algunas vulnerabilidades.	Aprendí a utilizar herramientas de pentesting, análisis de vulnerabilidades, así como la gestión de reportes y la comunicación para que las vulnerabilidades sean comprendidas y solucionadas.

Evaluación de desempeño

Considero que tuve un desempeño valorado en profesional, ya que concluí en tiempo y forma los reportes, así como el acercamiento con el profesor para compartir dudas me ayudó a encontrar el camino sobre los requerimientos que solicitaba el profesor.

Estoy practicando con herramientas de Nmap, Zaproxy y Nikto para afianzar mi carrera en el área de la ciberseguridad, comenzando a realizar proyectos para agregar a mi portafolio.

Referencias

Content Security Policy (CSP). (s/f). MDN Web Docs. Recuperado el 5 de abril de 2025, de https://developer.mozilla.org/es/docs/Web/HTTP/Guides/CSP

Clickjacking. (s. f.). Owasp.Org. Recuperado 5 de abril de 2025, de https://owasp.org/www-community/attacks/Clickjacking

Farrier, E. (2022, octubre 10). ¿Qué son los metadatos?: definición y significado. ¿Qué son los metadatos?: definición y significado; Avast. Recuperado el 05 de abril de 2025, de https://www.avast.com/es-es/c-what-is-metadata

Filosofía. (s/f). Infotec.mx. Recuperado el 05 de abril de 2025, de https://infotec.mx/es_mx/Infotec/Filosofia

Nuestra historia. (s/f). Infotec.mx. Recuperado el 05 de abril de 2025, de https://www.infotec.mx/nuestra-historia

INFOTEC. (2021). Fondo de Información y Documentación para la Industria. Recuperado el 05 de abril de 2025, de https://www.infotec.mx/work/models/Infotec/TransparenciaInfotec/1535/ORGANIGRAMA.pdf

INFOTEC. (2023). Fondo de Información y Documentación para la Industria INFOTEC; Manual de Organización. Recuperado el 05 de abril de 2025, de https://www.infotec.mx/work/models/Infotec/TransparenciaInfotec/1741/MANUAL_DE_ORGANIZACION_SOLO_FUNCIONES.pdf

¿Qué es INFOTEC? (s/f). Infotec.mx. Recuperado el 5 de abril de 2025, de https://www.infotec.mx/Infotec