Año Académico 2020-2021

I. Información General:

Título del Curso: Practica Externa Profesional (Capstone)

Código: PWHE1030

Horas Crédito: 135

Profesor: Joel Vargas Ramos

Email: jvargas@passwordpr.com

II. Descripción General

Experiencia supervisada y evaluada de 135 horas en el área de seguridad en el manejo de información y tecnología, donde se ponen en práctica las destrezas y conocimientos desarrollados durante el programa de estudios.

III. Objetivos Terminales

AI finalizar el internado los estudiantes estarán capacitados para:

1. Ejecutar las funciones de un profesional del campo de un técnico especialista de seguridad en sistemas de información.
2. Conocer los diferentes tipos de arquitecturas en I.T. y la aplicación de seguridad en las mismas.
3. Ejecutar y reconocer reportes y métricas de diferentes sistemas de monitoreo y desempeño en las redes.
4. Reconocer las políticas, reglas y leyes aplicables a diferentes estructuras y acciones en el ámbito de seguridad en I.T. (Information Technology).
5. Podrá Instalar y configurar “Firewall” básicos, e implementar reglas necesarias para prevenir ataques.
6. Diagnosticar y resolver problemas comunes de seguridad en la red.
7. Demostrará tener la capacidad para trabajar tanto individualmente como en grupo.
8. Conocerá y podrá recomendar ejecuciones de acuerdo a los niveles de vulnerabilidad de la empresa u organización.
9. Conocerá como crear máquinas virtuales y haciendo uso de las mismas estudiará

diferentes niveles de seguridad en una red.

10. Desarrollará un plan de manejo de riesgos y hare recomendaciones

11. Demostrará su conocimiento en seguridad y eficiencia al manejar la data en arquitecturas tecnológicas.

12. Participara de diferentes foros y entidades de seguridad en informática

13. Participara de alguna actividad social donde pueda aportar con su conocimiento hacia el manejo preventivo y seguro de los servicios tecnológicos

IV. Objetivos Capacitantes

AI terminar su práctica profesional los estudiantes podrán:

1. Utilizar y aplicar inteligencia proactiva contra amenazas para apoyar seguridad organizacional y gestión de vulnerabilidades.

2. Trabajar como un técnico de manejo de seguridad en sistemas de información.

3. Supervisar actividades e implementar cambios en la configuración de los controles existentes para mejorar la seguridad

4. Reconocer, Diagnosticar y ejecutar niveles de seguridad óptimos en sistemas y redes personales y profesionales intermedias.

5. Conocer el procedimiento de respuesta a incidentes apropiado, reconocer ataques y alternativas de mitigación, y recomendar técnicas forenses digitales.

6. Comparar y contrastar diferentes tipos de vulnerabilidades de redes.

7.Orientar y demostrar su capacidad profesional para fomentar el uso de actividades tecnológicas de la forma más segura posible.

Portfolio Professional Externship Capstone (200 pts)

Portfolio	Puntos
1. Página de Presentación 2. Tabla de Contenido 3. Introducción del Trabajo	5 pts 5 pts 5pts
4. Autobiografía 5. Resume 6. Cover Letter	5 pts 5 pts 5 pts
Webinars Certification 7. Attack Recognition and Incident Response. 8. Deciphering Dictionary and Brute Force attacks. 9. Security and Web Browsers.	 10 pts 10 pts 10 pts
TED Talk Submissions 10. The 1s and 0s behind cyber warfare. 11. You aren't at the mercy of your emotions. 12. How the IoT is making cybercrime investigation easier. 13. Your human firewall the answer to the cybersecurity problem. 14. Wiretapping the Secret Service can be easy and fun.	 10 pts 10 pts 10 pts 10 pts 10 pts
ICS Cert Training 15. Cybersecurity Risk 16. Cybersecurity Threat 17. Cybersecurity Vulnerabilities 18. Cybersecurity Consequences	 10 pts 10 pts 10 pts 10 pts
Taller Redaccion de Fuentes de Referencia APA 19. Evidencia Certificado APA	 10 pts
20. Cybersecurity and Society (Assessment)	30 pts
21. Conclusión 22. Bibliografía	5pts 5pts
Gran TOTAL	**200 pts**

Laboratorios (100 pts)

Laboratorios	Puntos
1. Installing Virtual Machine	25 pts
2. IOT Devices Attack	25 pts
3. Creating USB with ISO file	50 pts
TOTAL	**100 pts**

Proyectos a Evaluar (300 pts)

Proyectos a Evaluar	Puntos
1. Home Network Hardening	100 pts
2. Create your Own TED	200 pts
TOTAL	**300 pts**

Requisito: Haber terminado las 135 horas de práctica o su equivalente, Para poder terminar su práctica profesional tiene que cumplir con este requisito. Si no termina el internado de 135 horas de práctica los demás criterios de evaluación no aplican.

Escala de Calificaciones:

- 90 a 100 (A)
- 80 a 89 (B)
- 70 a 79 (C)
- 60 a 69 (D)
- 0 a 59 (F)

VI. Notas Especiales

A. La práctica podrá ser realizada en el periodo comprendido del penúltimo o último trimestre. EI internado comprende 135 horas de practica en un centro de práctica aprobado y autorizado por Password Technical College. Debe de terminar el practica en o antes de culminar el trimestre.

B. La asistencia al internado se evidenciará con hojas de asistencia que se complementarán semanalmente hasta complementar las 135 horas requeridas. Las hojas de asistencia deben de estar firmadas por el supervisor del centro de práctica y por el interno.

C. En caso de que la práctica profesional se haga de forma individual no optando por la opción de un centro de practica corporativo o de negocios el inciso b será sustituido por este. El estudiante será responsable de asistir puntualmente a las reuniones con su profesor y proveer toda la documentación requerida con tiempo de anticipación a finalizar el curso para evidenciar la misma y en caso de que algún documento sea rechazado tendrá que realizar los mismos nuevamente.

D. EI supervisor/profesor del centro de practica someterá tres evaluaciones de 100 puntos cada una evidenciando, la labor y progreso del estudiante de internado. La primera evaluación se complementará luego que el estudiante de internado complete el cincuenta por ciento de las
horas de práctica y la segunda evaluación al terminar las otras 65 horas de práctica.

E. Los originales de las hojas de asistencia y hojas de evaluación se entregarán al terminar el trimestre como parte del portafolio del internado. (solo aplica cuando el estudiante opta por la práctica profesional corporativa o en un entorno de negocios)

F. EI portafolio se entregará en o antes de siete días calendarios después de terminada la práctica profesional.

G. EI estudiante será responsable de reponer las horas de practica en caso de ausencia, al igual que será responsable de reponer todo trabajo que no sea aceptado en el caso de la practica individual.

H. EI horario de practica será el acordado por el supervisor, el profesor y el estudiante.

I. EI estudiante deberá de cumplir con las normas y reglamentos del centro de práctica.

J. Deberá asistir a reuniones u otra actividad requerida por el curso

K. En el caso de una práctica corporativa o de negocios, no se podrá cambiar el horario de práctica a menos que lo autorice el coordinador y supervisor del centro de práctica.

Infracción Académica

"Falta de honradez, fraude o plagio y cualquier otro comportamiento inapropiado relacionado con la labor académica o cualquier acción encaminada a tal fin no está permitido por esta institución" Esto implica que, en cualquier trabajo, tarea u otra actividad educativa que tenga que presentar el estudiante tiene que ser de su originalidad. De detectarse que no es original del estudiante, será penalizado no acreditando la nota que recibió por el trabajo 0 cualquier otra sanción que determine la institución.

DERECHOS DE ESTUDIANTES CON IMPEDIMENTOS

En cumplimiento con la Sección 504 de la Ley de Rehabilitación, la Ley ADA (American with Disabilities Act) Password Technical College realizará los esfuerzos que estén a su alcance para proveer los acomodos razonables necesarios para que el estudiante con impedimento pueda participar de la vida académica en igualdad de condiciones con el estudiante sin impedimento. Estudiantes con impedimento: debe informar al profesor de cada curso sobre sus necesidades especiales o acomodo razonable para el curso durante la primera semana de clases y notificar al coordinador en la oficina de registraduría lo antes posible. TODA SOLICITUD SERA DE CARÁCTER CONFIDENCIAL.

VII. Material de Referencia

Libros:

1. Wiley, Cyber Risk handbook
2. CompTIA Security + courseware
3. Mile2 C)PEH courseware

Revistas:

1. Tenable, Gestión de riesgos y entornos de políticas globales
2. Security in Depth, 2019 State of cybersecurity report
3. ErreIus – Cibercriminal y delitos informáticos
4. National Cyber security center, Cyber Crime an online business model
5. Cisco Print, Caza de amenzas ocultas