ASIGNATURA DE HACKING ÉTICO

1. Competencias	Diseñar y optimizar soluciones de redes digitales, a través de la administración y dirección de proyectos tecnológicos, alineados a normas y estándares vigentes, para contribuir a la continuidad del negocio.
2. Cuatrimestre	Noveno
3. Horas Teóricas	29
4. Horas Prácticas	46
5. Horas Totales	75
6. Horas Totales por Semana Cuatrimestre	5
7. Objetivo de aprendizaje	El alumno identificará las vulnerabilidades existentes, métodos y técnicas de aprovechamiento, a fin de establecer procedimientos de mitigación para salvaguardar los activos de la organización.

Unidades de Aprendizaje	**Horas**		
	Teóricas	**Prácticas**	**Totales**
I. Exploración de vulnerabilidades	4	6	10
II. Listado de vulnerabilidades	8	12	20
III. Etapa de obtención de acceso	8	12	20
IV. Métodos de conservación de acceso	5	10	15
V. Herramientas y técnicas de encubrimiento	4	6	10
Totales	**29**	**46**	**75**

HACKING ÉTICO

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**I. Exploración de vulnerabilidades**
2. Horas Teóricas	4
3. Horas Prácticas	6
4. Horas Totales	10
5. Objetivo de la Unidad de Aprendizaje	El alumno identificará las vulnerabilidades existentes para establecer una estrategia de salvaguarda de los activos de la organización.

Temas	Saber	Saber hacer	Ser
Preparación de las herramientas y entorno	Identificar las características de la organización objetivo. Enlistar las herramientas necesarias para la detección de vulnerabilidades.	Seleccionar las herramientas de detección de vulnerabilidades. Implementar las herramientas de detección de vulnerabilidades.	Observador Analítico Hábil para interpretar información Proactivo Lógico Ético Trabajo en equipo Metódico
Identificación de huellas.	Enlistar las herramientas de reconocimiento. Identificar las metodologías utilizadas en ingeniería social.	Seleccionar las herramientas de reconocimiento. Valuar las metodologías existentes para ingeniería social.	Observador Analítico Hábil para interpretar información Proactivo Lógico Ético Trabajo en equipo Metódico

Temas	Saber	Saber hacer	Ser
Técnicas de detección de vulnerabilidades.	Enlistar las técnicas y herramientas para el escaneo de puertos. Enlistar las técnicas y herramientas de detección de vulnerabilidades.	Seleccionar las técnicas y herramientas para el escaneo de puertos. Seleccionar las técnicas y herramientas de detección de vulnerabilidades.	Observador Analítico Hábil para interpretar información Proactivo Lógico Ético Trabajo en equipo Metódico

HACKING ÉTICO

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Desarrolla un reporte técnico para el establecimiento de un vector de ataque que incluya lo siguiente: - Técnicas y herramientas empleadas para la detección de vulnerabilidades - Técnicas y herramientas empleadas para obtención de información pública digital - Metodologías empleadas para ingeniería social - Técnicas y herramientas empleadas para escaneo de puertos - Secuencia del vector a ataque a implementar - Estrategia de salvaguarda de los activos de la organización	1. Explicar el vector de ataque. 2. Identificar vulnerabilidades. 3. Identificar huellas digitales de la organización. 4. Comprender las técnicas de detección de vulnerabilidades.	1. Lista de cotejo 2. Rúbrica

HACKING ÉTICO

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Análisis de Casos. -Aprendizaje Basado en Proyectos. -Equipos Colaborativos.	-Equipo de Cómputo -Software Especializado -Proyector -Internet -Pintarrón

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

HACKING ÉTICO

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**II. Listado de vulnerabilidades**
2. Horas Teóricas	8
3. Horas Prácticas	12
4. Horas Totales	20
5. Objetivo de la Unidad de Aprendizaje	El alumno enumerará las vulnerabilidades existentes para establecer una estrategia de salvaguarda de los activos de la organización.

Temas	Saber	Saber hacer	Ser
Tipos de vulnerabilidades	Enumerar las vulnerabilidades de los protocolos de red. Enumerar las vulnerabilidades de las aplicaciones y sus versiones.	Determinar las técnicas y herramientas para la detección de las vulnerabilidades de los protocolos de red. Determinar las técnicas y herramientas de detección de vulnerabilidades para las aplicaciones.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico
Vulnerabilidades en los sistemas de escritorio	Enumerar las vulnerabilidades de los sistemas operativos y aplicaciones de escritorio.	Determinar las técnicas y herramientas de detección de vulnerabilidades de los sistemas operativos y aplicaciones de escritorio.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico

Temas	Saber	Saber hacer	Ser
Vulnerabilidades en dispositivos móviles	Enumerar las vulnerabilidades de los sistemas operativos y aplicaciones de los dispositivos móviles.	Determinar las técnicas y herramientas de detección de vulnerabilidades de los sistemas operativos y aplicaciones de los dispositivos móviles.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico
Vulnerabilidades en los sistemas del Internet de las Cosas.	Enumerar las vulnerabilidades de los sistemas del Internet de las Cosas.	Determinar las técnicas y herramientas de detección de vulnerabilidades de los sistemas del Internet de las Cosas.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico
Vulnerabilidades en el equipo activo de red	Enumerar las vulnerabilidades en el equipo activo de red.	Determinar las técnicas y herramientas de detección de vulnerabilidades en el equipo activo de red.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico

ASIGNATURA DE HACKING ÉTICO

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Desarrolla un reporte de enumeración de vulnerabilidades de los diferentes sistemas que integran a la organización que incluya lo siguiente: - Descripción del sistema, aplicación, equipo y/o dispositivo analizado. - Enumeración de las vulnerabilidades de los sistemas de escritorio. - Enumeración de las vulnerabilidades de los dispositivos móviles. - Enumeración de las vulnerabilidades de los sistemas del Internet de las Cosas. - Enumeración de las vulnerabilidades de los equipos activos de red. - Matriz de vulnerabilidades clasificada por grado de impacto a la continuidad de negocio. - Estrategia de salvaguarda de los activos de la organización	1. Explicar las vulnerabilidades de los sistemas de escritorio. 2. Explicar las vulnerabilidades de los dispositivos móviles. 3. Explicar las vulnerabilidades de los sistemas del Internet de las Cosas. 4. Explicar las vulnerabilidades de los equipos activos de red.	1. Lista de cotejo 2. Rúbrica

HACKING ÉTICO

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Análisis de Casos. -Aprendizaje Basado en Proyectos. -Equipos Colaborativos.	-Equipo de Cómputo -Equipo de red. -Equipo del Internet de las Cosas -Software Especializado -Proyector -Internet -Pintarrón

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

HACKING ÉTICO

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**III. Etapa de obtención de acceso**
2. Horas Teóricas	8
3. Horas Prácticas	12
4. Horas Totales	20
5. Objetivo de la Unidad de Aprendizaje	El alumno explicará los métodos y técnicas en la obtención de acceso para establecer una estrategia de salvaguarda de los activos de la organización.

Temas	Saber	Saber hacer	Ser
Técnicas para la obtención de acceso en sistemas de escritorio	Identificar los métodos de obtención de acceso en sistemas de escritorio.	Seleccionar las técnicas y herramientas para la obtención de acceso en sistemas de escritorio.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico
Técnicas para obtención de acceso de en dispositivos móviles	Identificar los métodos de obtención de acceso en dispositivos móviles.	Seleccionar las técnicas y herramientas para la obtención de acceso en dispositivos móviles.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico

Temas	Saber	Saber hacer	Ser
Técnicas para obtención de acceso a los sistemas del Internet de las Cosas.	Identificar los métodos de obtención de acceso a los sistemas del Internet de las Cosas.	Seleccionar las técnicas y herramientas para la obtención de acceso a los sistemas del Internet de las Cosas.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico
Técnicas para obtención de acceso al equipo activo de red	Identificar los métodos de obtención de acceso al equipo activo de red.	Seleccionar las técnicas y herramientas para la obtención de acceso al equipo activo de red.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico

HACKING ÉTICO

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Desarrolla un reporte técnico que describa los resultados de los métodos, técnicas y herramientas de obtención de acceso aplicados en los diferentes sistemas de la organización, que incluya lo siguiente: - Descripción del sistema, aplicación, equipo y/o dispositivo analizado. - Métodos, técnicas y herramientas de obtención de acceso de los sistemas de escritorio. - Métodos, técnicas y herramientas de obtención de acceso de los dispositivos móviles. - Métodos, técnicas y herramientas de obtención de acceso de los sistemas del Internet de las Cosas. - Métodos, técnicas y herramientas de obtención de acceso de los equipos activos de red. - Estrategia de salvaguarda de los activos de la organización	1. Analizar los resultados de las técnicas de obtención de acceso a los sistemas de escritorio. 2. Analizar los resultados de las técnicas de obtención de acceso a los dispositivos móviles. 3. Analizar los resultados de los resultados de las técnicas de obtención de acceso a los sistemas del Internet de las Cosas. 4. Analizar los resultados de las técnicas de obtención de acceso a los equipos activos de red.	1. Lista de cotejo 2. Rúbrica

HACKING ÉTICO

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Análisis de Casos. -Aprendizaje Basado en Proyectos. -Equipos Colaborativos.	-Equipo de Cómputo -Equipo de red. -Equipo del Internet de las Cosas -Software Especializado -Proyector -Internet -Pintarrón

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

HACKING ÉTICO

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**IV. Métodos de conservación de acceso**
2. Horas Teóricas	5
3. Horas Prácticas	10
4. Horas Totales	15
5. Objetivo de la Unidad de Aprendizaje	El alumno explicará los métodos y técnicas en la conservación del acceso para establecer una estrategia de salvaguarda de los activos de la organización.

Temas	Saber	Saber hacer	Ser
Métodos de conservación de acceso en sistemas de escritorio	Identificar los métodos de conservación de acceso en sistemas de escritorio.	Seleccionar las técnicas y herramientas para la conservación de acceso en sistemas de escritorio.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico
Métodos de conservación de acceso en dispositivos móviles	Identificar los métodos de conservación de acceso en dispositivos móviles.	Seleccionar las técnicas y herramientas para la conservación de acceso en dispositivos móviles.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico

Temas	Saber	Saber hacer	Ser
Métodos de conservación de acceso a los sistemas del Internet de las Cosas.	Identificar los métodos de conservación a los sistemas del Internet de las Cosas.	Seleccionar las técnicas y herramientas para la conservación de acceso a los sistemas del Internet de las Cosas.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico
Métodos de conservación de acceso al equipo activo de red	Identificar los métodos de conservación al equipo activo de red.	Seleccionar las técnicas y herramientas para la conservación de acceso al equipo activo de red.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico

HACKING ÉTICO

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Desarrolla un reporte técnico que describa los resultados de los métodos, técnicas y herramientas de conservación de acceso aplicados en los diferentes sistemas de la organización, que incluya lo siguiente: - Descripción del sistema, aplicación, equipo y/o dispositivo analizado. - Métodos, técnicas y herramientas de conservación de acceso de los sistemas de escritorio. - Métodos, técnicas y herramientas de conservación de acceso de los dispositivos móviles. - Métodos, técnicas y herramientas de conservación de acceso de los sistemas del Internet de las Cosas. - Métodos, técnicas y herramientas de conservación de acceso de los equipos activos de red. - Estrategia de salvaguarda de los activos de la organización	1. Analizar los resultados de los métodos de conservación de acceso a los sistemas de escritorio. 2. Analizar los resultados de los métodos de conservación de acceso a los dispositivos móviles. 3. Analizar los resultados de los métodos de conservación de acceso a los sistemas del Internet de las Cosas. 4. Analizar los resultados de los métodos de conservación de acceso a los equipos activos de red.	1. Lista de cotejo 2. Rúbrica

HACKING ÉTICO

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Análisis de Casos. -Aprendizaje Basado en Proyectos. -Equipos Colaborativos.	-Equipo de Cómputo -Equipo de red. -Equipo del Internet de las Cosas -Software Especializado -Proyector -Internet -Pintarrón

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

HACKING ÉTICO

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**V. Herramientas y técnicas de encubrimiento**
2. Horas Teóricas	4
3. Horas Prácticas	6
4. Horas Totales	10
5. Objetivo de la Unidad de Aprendizaje	El alumno identificará las herramientas y técnicas de encubrimiento para establecer una estrategia de salvaguarda de los activos de la organización.

Temas	Saber	Saber hacer	Ser
Eliminación de registros	Identificar los métodos de eliminación de registros en sistemas de escritorio, dispositivos móviles, sistemas del Internet de las Cosas y equipo activo de red.	Seleccionar técnicas y herramientas para eliminar registros en sistemas de escritorio, dispositivos móviles, sistemas del Internet de las Cosas y equipo activo de red.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico
Shell HTTP inversa	Identificar los métodos para la creación de shell HTTP inversa en sistemas de escritorio, dispositivos móviles, sistemas del Internet de las Cosas y equipo activo de red.	Seleccionar técnicas y herramientas para la creación de shell HTTP inversa en sistemas de escritorio, dispositivos móviles, sistemas del Internet de las Cosas y equipo activo de red.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico

Temas	Saber	Saber hacer	Ser
Túnel ICMP	Identificar los métodos para la creación de un túnel ICMP en sistemas de escritorio, dispositivos móviles, sistemas del Internet de las Cosas y equipo activo de red.	Seleccionar técnicas y herramientas para la creación de un túnel ICMP en sistemas de escritorio, dispositivos móviles, sistemas del Internet de las Cosas y equipo activo de red.	Analítico. Crítico. Observador. Coherente. Lógico. Proactivo. Observador Hábil para interpretar información Ético Trabajo en equipo Metódico

HACKING ÉTICO

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Desarrolla un reporte técnico que describa los resultados de los métodos, técnicas y herramientas de encubrimiento, que incluya lo siguiente: - Técnicas y herramientas de eliminación de registros a ña seguridad de una organización - Creación de shell HTTP inversa y creación de túnel ICMP en los sistemas, aplicaciones, equipos y dispositivos de la organización - Estrategia de salvaguarda de los activos de la organización	1. Analizar los resultados de los métodos de eliminación de registros, creación de shell HTTP inversa y creación de túnel ICMP en los sistemas de escritorio, dispositivos móviles, sistemas del Internet de las Cosas y los equipos activos de red.	1. Lista de cotejo 2. Rúbrica

HACKING ÉTICO

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Análisis de Casos. -Aprendizaje Basado en Proyectos. -Equipos Colaborativos.	-Equipo de Cómputo -Equipo de red. -Equipo del Internet de las Cosas -Software Especializado -Proyector -Internet -Pintarrón

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
	X	

HACKING ÉTICO

CAPACIDADES DERIVADAS DE LAS COMPETENCIAS PROFESIONALES A LAS QUE CONTRIBUYE LA ASIGNATURA

Capacidad	Criterios de Desempeño
Diagnosticar riesgos y vulnerabilidades en la seguridad de información a partir del análisis del entorno de las organizaciones, para desarrollar estrategias que permitan su mitigación.	Entrega un reporte técnico que incluya lo siguiente: - Análisis del contexto del negocio. - Listado requerimientos funcionales y no funcionales. - Análisis de la situación actual de la seguridad de información de la organización
Establecer políticas de seguridad de información mediante estándares y procedimientos vigentes aplicables al entorno de la organización, para establecer las bases de continuidad de negocio.	Entrega un documento con la política de seguridad de información que considere los siguientes puntos: - Matriz de riesgos y vulnerabilidades. - Procesos de continuidad del negocio. - Políticas de salvaguarda de los activos de la organización. - Identificación y clasificación de los activos de la organización.
Seleccionar herramientas y servicios para la seguridad de información mediante la aplicación de estándares, para dar cumplimiento a las políticas de seguridad de las organizaciones.	Entrega una propuesta de solución que incluye lo siguiente: - Tabla comparativa de la evaluación de alternativas de solución. - Arquitectura de la solución propuesta. - Análisis del retorno de la inversión. - Hoja técnica de la solución propuesta
Planear las estrategias de implementación de políticas, herramientas y servicios de seguridad de información a partir del análisis del entorno, para salvaguardar los activos de las organizaciones.	Entrega un plan de trabajo que incluye lo siguiente: - Actividades a desarrollar. - Responsables. - Tiempos asignados a cada tarea.
Evaluar la implementación de soluciones de seguridad de información mediante la aplicación de auditorías, pruebas e interpretación de métricas, para determinar áreas de oportunidad en los procesos de continuidad de negocio.	Entrega un reporte de auditoria de seguridad que incluye los siguiente: - Resultados de pruebas de penetración. - Análisis de vulnerabilidades. - Propuesta de mejoras a la política de seguridad de la organización.

Capacidad	Criterios de Desempeño
Monitorear la implementación de soluciones y políticas de seguridad de información a través del análisis de los resultados de auditorías, para optimizar los procesos de continuidad del negocio.	Entrega un reporte técnico que incluye lo siguiente: - Bitácora de eventos. - Lista de verificación de las políticas de seguridad de la organización. - Reportes de rendimiento y eficiencia de la solución.

HACKING ÉTICO

FUENTES BIBLIOGRÁFICAS

Autor	Año	Título del Documento	Ciudad	País	Editorial
Messier, Ric	2019	*CEH v10 Certified Ethical Hacker Study Guide*	IN	USA	John Wiley & Sons, Inc. ISBN-13 : 978-1119533191
Peter Kim	2018	*THE HACKER PLAYBOOK 3*		USA	Secure Planet LLC ISBN-13 : 978-1980901754
Ric Messier	2018	*Learning Kali Linux*	CA	USA	O'Reilly ISBN-13 : 978-1492028697
Dr. Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic	2018	*Gray Hat Hacking: The Ethical Hacker's Handbook*		USA	McGraw-Hill Education ISBN-13 : 978-1260108415
Raphaël Hertzog, JimO'Gorman, and Mati Aharoni	2017	*Kali Linux Revealed*	NC	USA	OffsecPress ISBN-13 : 978-0997615609
Alex Matrosov, Eugene Rodionov, Sergey Bratus	2019	*Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats (English Edition)*	CA	USA	No Starch Press ISBN-13 : 978-1593277161