[IA]Guard

Certificación Ciberseguridad

Plan de estudios

Certificación Ciberseguridad

Información general

En un mundo cada vez más interconectado, la ciberseguridad ha dejado de ser una opción para convertirse en una necesidad urgente en todos los sectores. La protección de datos, la seguridad en la infraestructura tecnológica y la prevención de amenazas digitales son pilares fundamentales para garantizar el funcionamiento seguro de empresas, instituciones y usuarios particulares. Ante este panorama, se requiere de profesionales capacitados, éticos y actualizados que puedan enfrentar desafíos complejos con preparación técnica y criterio analítico.

Este programa de formación integral está diseñado para guiar al estudiante desde los fundamentos más básicos hasta conceptos avanzados dentro del campo de la ciberseguridad, utilizando exclusivamente recursos y certificaciones totalmente gratuitas. A través de seis módulos progresivos, se desarrollan habilidades técnicas en sistemas, redes, análisis de vulnerabilidades, pruebas de penetración, seguridad en la nube y defensa de sistemas, todo dentro de entornos controlados que simulan escenarios reales.

Cada módulo incluye prácticas guiadas, ejercicios aplicados, y evaluaciones que permiten consolidar el conocimiento adquirido. Además, al finalizar cada etapa, el estudiante obtendrá un certificado digital oficial que acredita sus competencias y progresos, los cuales podrán ser integrados en su portafolio profesional.

Este plan de estudios está pensado no solo para formar habilidades técnicas, sino también para fomentar una mentalidad analítica, ética y estratégica, preparando al alumno para desempeñarse con excelencia en roles de ciberseguridad a nivel profesional.

Perfiles

Perfil de ingreso
Personas interesadas en el desarrollo web, con conocimientos básicos de programación o lógica computacional. Idealmente con nociones en HTML, CSS o algún lenguaje como Python, JavaScript o C++.

Perfil de egreso
Al finalizar, el egresado podrá diseñar, desarrollar, implementar y mantener aplicaciones web completas, implementar servicios RESTful, bases de datos, aplicar principios de DevOps y desplegar sus aplicaciones en entornos productivos.

General

Conocimientos previos
No se requiere conocimientos previos.

Duración
24 semanas de cursos

Requisitos técnicos
Hardware: Se recomienda contar con al menos 4 GB de RAM y procesador de doble núcleo. Para una experiencia fluida, es ideal tener 8 GB de RAM y procesador de cuatro núcleos.
Software: Sistema operativo Windows 10, macOS Catalina o superior. Es necesario tener instalado Visual Studio Code con las extensiones para desarrollo web y/o backend. También se requiere tener privilegios de administrador para instalar herramientas adicionales.

Metodología

El programa se estructura en seis módulos secuenciales, cada uno enfocado en una dimensión clave de la ciberseguridad. Se utiliza una metodología por competencias, con un equilibrio entre contenido teórico, práctica autónoma y sesiones grupales en vivo.
Cada semana incluye:

- Contenido autoformativo
- Una clase práctica en vivo de 2 horas para resolver dudas, practicar habilidades técnicas y trabajar en equipo
- Actividades aplicadas en laboratorios simulados o entornos controlados

El aprendizaje es flexible pero guiado, con objetivos claros y herramientas prácticas para avanzar de manera estructurada.

Requisitos finales

Para obtener las certificaciones digitales del programa, el estudiante deberá cumplir con:

1. Finalizar el módulo con todos sus contenidos esenciales.
2. Asistir o revisar al menos el 75% de las clases prácticas en vivo.
3. Realizar las actividades clave y entregar el portafolio final en el último módulo.

Cada módulo cuenta con su propia certificación, y al concluir los seis módulos se emite un certificado global que acredita la formación completa.

Módulo 1: Fundamentos de Ciberseguridad

Duración: Semanas 1 a 4 **Nivel: Principiante**

Objetivo general

Se le brindará al estudiante una base sólida sobre los principios esenciales de la ciberseguridad, permitiéndole comprender el propósito y la importancia de esta disciplina en el contexto actual. A lo largo del módulo, el alumno explorará cómo la ciberseguridad se ha convertido en un componente crítico para el funcionamiento seguro de empresas, instituciones gubernamentales y usuarios individuales.

Contenido principal

- Introducción al concepto de ciberseguridad
- Principales amenazas y vulnerabilidades digitales
- Tipos de ataques cibernéticos más comunes
- Fundamentos de seguridad en redes, dispositivos y datos personales
- Principios de ética digital y buenas prácticas en seguridad

Habilidades a Desarrollar

- Identificación de riesgos y amenazas en entornos digitales
- Aplicación de medidas básicas de protección personal y profesional
- Análisis crítico de incidentes de ciberseguridad reales
- Conciencia sobre la importancia de la privacidad y la protección de datos

Actividades Prácticas

- Identificación de riesgos y amenazas en entornos digitales
- Aplicación de medidas básicas de protección personal y profesional
- Análisis crítico de incidentes de ciberseguridad reales
- Conciencia sobre la importancia de la privacidad y la protección de datos

Resultados esperados

Al finalizar este módulo, el estudiante contará con una comprensión clara de los fundamentos de la ciberseguridad y podrá aplicar conocimientos básicos en escenarios reales. Además, obtendrá un certificado digital gratuito que acredita su participación y aprendizaje, constituyendo un primer logro académico dentro del itinerario profesional en ciberseguridad.

Módulo 1
Incluye certificado

Módulo 2: Herramientas y sistemas operativos

Duración: Semanas 5 a 8 **Nivel: Principiante**

Objetivo general

Se proporcionará al estudiante una introducción práctica y conceptual al uso de herramientas esenciales dentro del ámbito de la ciberseguridad, así como al entorno de sistemas operativos basados en Linux, que representan una pieza clave en el trabajo diario de los profesionales de esta área.
Este módulo tiene como propósito familiarizar al alumno con la terminal de comandos, el manejo básico de sistemas de archivos, permisos, usuarios, redes y procesos para administrar entornos seguros, auditar sistemas y ejecutar análisis forenses.
El estudiante conocerá las herramientas más utilizadas para la supervisión del tráfico de red, el escaneo de puertos y servicios, y la exploración de vulnerabilidades en sistemas operativos y redes locales. Esto permitirá que el estudiante comience a interactuar directamente con entornos controlados que simulan situaciones reales de monitoreo y análisis.

Contenido principal

- Introducción al sistema operativo Linux para ciberseguridad
- Uso básico y avanzado de la terminal de comandos (CLI)
- Gestión de archivos, procesos, permisos y usuarios en Linux
- Primeros pasos en redes: direcciones IP, puertos, protocolos y servicios
- Herramientas esenciales: análisis de tráfico de red, escaneo de puertos, captura de paquetes
- Lectura e interpretación de logs del sistema

Habilidades a Desarrollar

- Dominio funcional del sistema operativo Linux orientado a tareas de seguridad
- Navegación eficiente en entornos de línea de comandos
- Configuración y análisis de red en entornos controlados
- Uso inicial de herramientas como escáneres de red y analizadores de tráfico
- Evaluación básica de la seguridad de un sistema local

Actividades Prácticas

- Simulación de ataques y defensas básicas en entornos Linux
- Pruebas de monitoreo de tráfico y análisis de logs
- Ejercicios guiados de administración y configuración de sistemas

Resultados esperados

Al finalizar este módulo, el estudiante será capaz de desenvolverse con fluidez en un entorno Linux, ejecutar comandos de utilidad para la gestión y análisis de sistemas, y utilizar herramientas fundamentales de inspección y monitoreo de red.

Módulo 2
Incluye certificado

Módulo 3: Análisis de vulnerabilidades

Duración: Semanas 9 a 12 **Nivel: Intermedio**

Objetivo general

Este módulo tiene como finalidad introducir al estudiante en los fundamentos del análisis de vulnerabilidades, una competencia clave dentro del ciclo de defensa en ciberseguridad. Se busca desarrollar la capacidad para identificar, comprender y evaluar debilidades en sistemas informáticos, aplicaciones web y redes, entendiendo el impacto potencial que dichas vulnerabilidades pueden representar para la seguridad de una organización.
El alumno conocerá en profundidad las vulnerabilidades más comunes y relevantes según los estándares de la industria, explorando especialmente las que afectan aplicaciones web, tales como inyecciones de código, exposición de datos sensibles y errores de autenticación. A partir de esta base, se comenzará a trabajar con herramientas automatizadas y entornos simulados que permitirán la detección y el análisis técnico de amenazas reales.
Además, se fortalecerá el criterio ético en la gestión responsable de información sensible, así como el pensamiento crítico para priorizar y reportar vulnerabilidades con base en su severidad, contexto y riesgo asociado.

Contenido principal

- Fundamentos del análisis de vulnerabilidades
- Tipologías y clasificación de vulnerabilidades
- Estándares de referencia (como los listados más comunes en la industria)
- Ciclo de identificación, evaluación y reporte de vulnerabilidades
- Introducción al análisis de aplicaciones web y errores comunes de seguridad
- Uso básico de herramientas de escaneo y pruebas de penetración ética en sitios web
- Evaluación de riesgos y severidad (crítica, alta, media, baja)

Habilidades a Desarrollar

- Reconocimiento de patrones comunes de vulnerabilidades en sistemas y aplicaciones
- Análisis crítico del riesgo que representa cada debilidad encontrada
- Uso inicial de herramientas de escaneo automatizado
- Navegación e interacción con entornos de práctica orientados al pentesting web
- Redacción de reportes técnicos simples y organizados sobre vulnerabilidades detectadas

Actividades Prácticas

- Exploración de entornos seguros con aplicaciones web vulnerables
- Análisis guiado de ataques simulados como XSS, CSRF y SQLi
- Pruebas controladas de escaneo y detección de fallos de seguridad

Resultados esperados

Al finalizar este módulo, el estudiante podrá identificar vulnerabilidades comunes en aplicaciones y sistemas, utilizar herramientas básicas de análisis, y elaborar reportes de hallazgos técnicos con recomendaciones iniciales. Esta competencia es esencial tanto en contextos de evaluación interna como en pruebas de penetración más avanzadas. El alumno obtendrá un certificado digital gratuito que respalda formalmente su participación y dominio del análisis de vulnerabilidades a nivel introductorio-intermedio.

Módulo 3
Incluye certificado

Módulo 4: Pentesting Básico

Duración: Semanas 13 a 16 **Nivel: Intermedio**

Objetivo general

Este módulo tiene como objetivo introducir al estudiante en el mundo del pentesting (pruebas de penetración), es decir, la práctica de evaluar la seguridad de sistemas y redes mediante la simulación controlada de ataques reales. A través de este enfoque práctico, el alumno aprenderá a pensar como un atacante ético para identificar puntos débiles antes de que puedan ser explotados por actores maliciosos.

Durante estas semanas, se brindará una comprensión clara del ciclo de un test de penetración, desde la recopilación de información y el escaneo de objetivos hasta la explotación básica y la elaboración de reportes técnicos. Se trabajará en entornos virtuales diseñados especialmente para practicar con total seguridad, permitiendo al estudiante desarrollar habilidades ofensivas bajo una perspectiva ética y controlada.

Además, se cultivará la mentalidad analítica y la atención al detalle necesarias para llevar a cabo pruebas de seguridad exitosas, siempre con un enfoque basado en la responsabilidad profesional, la legalidad y el respeto por los datos y los sistemas.

Contenido principal

- Introducción al pentesting y sus objetivos
- Fases de una prueba de penetración: reconocimiento, escaneo, explotación, post-explotación y reporte
- Herramientas esenciales para pruebas de seguridad ofensiva
- Tipos de escaneo: puertos, servicios y vulnerabilidades
- Simulación de ataques comunes: fuerza bruta, inyección, escalamiento de privilegios
- Fundamentos de explotación ética en redes y servidores
- Elaboración de reportes técnicos con hallazgos y recomendaciones

Habilidades a Desarrollar

- Realización de escaneos dirigidos y análisis de resultados
- Reconocimiento de vectores de ataque y aprovechamiento de fallos de seguridad simulados
- Uso inicial de herramientas ofensivas de código abierto
- Aplicación del pensamiento ofensivo con enfoque defensivo
- Capacidad de documentar de manera clara los pasos realizados y hallazgos obtenidos

Actividades Prácticas

- Pruebas de reconocimiento y escaneo en laboratorios virtuales
- Simulación de ataques éticos sobre máquinas vulnerables controladas
- Desempeño de roles de atacante y defensor para desarrollar visión integral

Resultados esperados

Al concluir este módulo, el estudiante será capaz de ejecutar pruebas básicas de penetración en entornos simulados, documentar sus procesos, y comprender las implicaciones de seguridad que estos ataques pueden tener en un sistema real. Este conocimiento es clave tanto para aspirantes a roles ofensivos como defensivos dentro de la ciberseguridad. Se otorgará un certificado digital gratuito que valida las competencias desarrolladas en este nivel inicial de pentesting ético.

Módulo 4
Incluye certificado

Módulo 5: Seguridad en la Nube y Defensa de Sistemas

Duración: Semanas 17 a 20 **Nivel: Intermedio**

Objetivo general

Este módulo tiene como finalidad que el estudiante adquiera conocimientos y habilidades fundamentales en la protección de entornos en la nube, así como en la implementación de estrategias de defensa activa dentro de sistemas y redes. El avance de las tecnologías cloud ha transformado la manera en que las organizaciones almacenan y procesan datos, por lo que comprender sus riesgos y mecanismos de protección es clave para todo profesional en ciberseguridad.

El alumno explorará los principios de seguridad en la nube, enfocándose en modelos de responsabilidad compartida, control de acceso, monitoreo y gestión de usuarios. Asimismo, se le introducirá al enfoque del equipo azul (blue team), desarrollando capacidades para la detección, análisis y respuesta ante amenazas, reforzando el rol de defensor digital.

Durante estas semanas se combinarán conceptos teóricos con laboratorios prácticos, permitiendo al estudiante configurar medidas de protección, gestionar identidades y realizar análisis básicos de logs y eventos sospechosos.

Contenido principal

- Fundamentos de seguridad en la nube: modelos IaaS, PaaS y SaaS
- Principios de responsabilidad compartida en entornos cloud
- Control de accesos, autenticación multifactor y gestión de identidades
- Políticas de permisos y configuraciones seguras
- Fundamentos del equipo azul (blue team) y monitoreo de seguridad
- Introducción al análisis de eventos y respuesta ante incidentes
- Prácticas recomendadas para proteger servicios en la nube y recursos digitales

Habilidades a Desarrollar

- Comprensión de los riesgos específicos asociados a plataformas en la nube
- Aplicación de controles de seguridad para proteger accesos y recursos
- Monitoreo básico de sistemas mediante análisis de registros y alertas
- Desarrollo de un pensamiento defensivo, orientado a la prevención y mitigación de amenazas
- Evaluación de configuraciones seguras en servicios y entornos remotos

Actividades Prácticas

- Simulación de configuración de accesos y roles en servicios en la nube
- Lectura e interpretación de eventos de seguridad simulados
- Análisis de alertas y diseño de respuestas básicas ante incidentes

Resultados esperados

Al finalizar el módulo, el estudiante será capaz de aplicar principios de seguridad en entornos cloud, reconocer vulnerabilidades comunes en configuraciones remotas y responder ante eventos de seguridad básicos utilizando criterios de análisis y mitigación. El dominio de estos temas fortalecerá su perfil defensivo y lo preparará para escenarios reales de administración segura. Se otorgará un certificado digital gratuito que acreditará formalmente su participación y logros en esta etapa del programa.

Módulo 5
Incluye certificado

Módulo 6: Evaluación Final y Portafolio Profesional

Duración: Semanas 21 a 24 **Nivel: Avanzado**

Objetivo general

El objetivo de este módulo final es consolidar los conocimientos, habilidades y competencias desarrolladas a lo largo del programa, mediante la integración de todo lo aprendido en proyectos prácticos y evaluaciones finales. El estudiante tendrá la oportunidad de demostrar su capacidad de aplicar estrategias ofensivas y defensivas en escenarios simulados, evaluar riesgos de forma crítica y documentar adecuadamente sus procesos y resultados.

Además, se trabajará en la construcción de un portafolio profesional que reúna los logros obtenidos, los certificados adquiridos y evidencias prácticas de sus habilidades. Este portafolio será una herramienta clave para presentarse ante futuros empleadores o instituciones educativas, proyectando una imagen sólida y profesional dentro del ámbito de la ciberseguridad.

El cierre del programa no solo validará los conocimientos técnicos adquiridos, sino también la capacidad del alumno para organizar su aprendizaje, comunicar resultados técnicos y enfrentar retos reales con un enfoque crítico y ético.

Contenido principal

- Revisión integral de conceptos clave de ciberseguridad
- Integración práctica de habilidades ofensivas (pentesting) y defensivas (defensa de sistemas)
- Diseño y construcción de un portafolio profesional de ciberseguridad
- Documentación técnica de proyectos realizados y hallazgos encontrados
- Preparación para entrevistas técnicas básicas y simulaciones de retos de ciberseguridad

Habilidades a Desarrollar

- Capacidad de aplicar de manera conjunta herramientas y técnicas aprendidas
- Análisis crítico de escenarios de seguridad complejos
- Redacción de documentación técnica profesional
- Diseño y publicación de un portafolio público
- Preparación para procesos de selección profesional en ciberseguridad

Actividades Prácticas

- Elaboración de un reporte final que integre prácticas de análisis de vulnerabilidades y defensa de sistemas
- Presentación de un ejercicio de pentesting básico simulado
- Organización de todos los certificados digitales obtenidos en un repositorio personal
- Preparación de respuestas para preguntas comunes en entrevistas de ciberseguridad

Resultados esperados

Al concluir este módulo, el estudiante habrá reunido, organizado y presentado de forma clara y profesional las evidencias de su proceso de formación. El portafolio estructurado que construirá será una recopilación detallada de los certificados obtenidos, ejercicios prácticos realizados, proyectos desarrollados y aprendizajes clave alcanzados durante los seis módulos del programa. Este portafolio funcionará no solo como una muestra tangible de su progreso académico y técnico, sino también como una herramienta estratégica de posicionamiento profesional.

Dicho portafolio podrá ser utilizado en procesos de reclutamiento, entrevistas laborales, postulaciones a becas o certificaciones adicionales, así como en redes profesionales especializadas en tecnología y ciberseguridad. Contará con documentación técnica clara, capturas de prácticas en entornos simulados, resúmenes de habilidades por módulo y enlaces a credenciales verificables, facilitando así su validación por parte de empleadores o instituciones educativas.

Adicionalmente, el estudiante recibirá un certificado digital gratuito de finalización del programa completo, el cual reconocerá formalmente su recorrido formativo de seis meses, validando su dominio de los principios esenciales de la ciberseguridad, su manejo básico de herramientas técnicas, y su capacidad para participar en tareas de análisis, defensa y pruebas de seguridad. Este reconocimiento respaldará su transición hacia el entorno profesional, permitiéndole presentarse con fundamentos sólidos como candidato en el sector tecnológico o como base para continuar con certificaciones especializadas de nivel avanzado.

www.iaguard.com.mx

IA Guard Academy se reserva el derecho y tiene la facultad exclusiva de modificar, actualizar o cancelar cualquier parte del programa académico, incluyendo pero no limitado a cursos, contenidos, instructores, metodologías, fechas, horarios, evaluaciones, certificaciones y demás componentes relacionados con sus programas de formación. Estas modificaciones pueden realizarse en cualquier momento, sin previo aviso, con el fin de garantizar la mejora continua de la calidad educativa, adaptarse a nuevas tecnologías, requerimientos del mercado, cambios regulatorios o criterios institucionales. La continuidad en el uso de los servicios ofrecidos por IA Guard Academy implica la aceptación de estos términos por parte del estudiante o usuario.