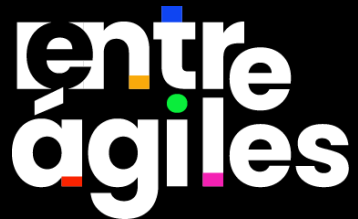


# Plan de Estudios

# Desarrollo Código Seguro

entre  
ágiles



Estamos emocionados de darte la bienvenida a la comunidad de **Entre Ágiles**, esperando que disfrutes con nosotros de nuestra pasión: compartir conocimiento y grandes experiencias.

Queremos contarte que este proyecto es el resultado de la suma de esfuerzos y nuestra experiencia a lo largo de más de 10 años, en los que tu participación y apoyo fueron la clave para alcanzar grandes logros, y justamente por eso queremos que hagas parte de esta nueva era: ¡porque sabemos que tienes mucho que aportar y que entre todos haremos crecer esta comunidad!

"La educación no es preparación para la vida; la educación es la vida en sí misma"-John Dewey

# Acerca del entrenamiento

El entrenamiento está diseñado para proporcionar una comprensión sólida y progresiva de las prácticas de **desarrollo seguro**, comenzando con los principios fundamentales de la seguridad en el ciclo de vida del **software**, avanzando hacia la identificación y prevención de vulnerabilidades comunes, y culminando con la **implementación de técnicas y estándares** para escribir código robusto, confiable y protegido contra amenazas.

## Modalidad

**Online**

(Clases en vivo)

## Duración

**30 Horas**

(10 Sesiones)

# Temas del curso

A decorative blue line graphic that starts from the left edge of the slide, moves horizontally to the right, then angles downwards to the right, and finally continues horizontally to the right edge of the slide.

- Introducción a la seguridad en el desarrollo de software
- OWASP Top 10 Fundamentos de CSSLP
- (Certified Secure Software Lifecycle Professional)
- Arquitectura y diseño seguro
- Validación y sanitización de entradas
- Autenticación y gestión de sesiones

# Temas del curso



- Gestión de credenciales y control de acceso
- Cifrado y protección de datos
- Pruebas de seguridad en software
- Gestión de Vulnerabilidades y Parches
- Control de Configuraciones Seguras
- Gestión del Ciclo de Vida de Software Seguro (SDLC)

# Temas detallados

## 1. Introducción a la seguridad en el desarrollo de software

- Definición de código seguro y su importancia
- Riesgos asociados a la falta de seguridad en el software
- Impacto de las vulnerabilidades de software en la seguridad empresarial
- Principios clave de desarrollo seguro

## 2. OWASP Top 10

- Introducción a OWASP (Open Web Application Security Project)
- Profundización en cada una de las vulnerabilidades del OWASP Top 10
- Inyección (SQL, OS, LDAP)
- Fallos en la autenticación
- Exposición de datos sensibles
- Entidades XML externas (XXE)
- Control de acceso roto
- Configuraciones de seguridad incorrectas
- Cross-Site Scripting (XSS)
- Inseguridad en deserialización
- Usar componentes con vulnerabilidades conocida
- Insuficiente monitoreo y registro
- Técnicas de mitigación para cada una de estas vulnerabilidades

# Temas

# detallados

## 3. Fundamentos de CSSLP (Certified Secure Software Lifecycle Professional)

- Introducción al CSSLP y su relevancia en el ciclo de vida del desarrollo de software seguro
- Revisión de los 8 dominios del CSSLP:
  1. Conceptos y requisitos de seguridad
  2. Diseño seguro del software
  3. Implementación/Programación segura
  4. Pruebas de software seguro
  5. Gestión de ciclo de vida
  6. Gestión de incidentes
  7. Prácticas de desarrollo seguro
  8. Aseguramiento de suministro de software
- Relación del CSSLP con estándares de la industria como ISO/IEC 27034

## 4. Arquitectura y diseño seguro

- Principios de arquitectura segura (defensa en profundidad, principio de privilegio mínimo, etc.
- Modelado de amenazas y análisis de riesgos
- Estrategias para evitar errores comunes en el diseño
- Aplicación de patrones de diseño seguro

# Temas detallados

## 5. Validación y sanitización de entradas

- Validación de datos en el lado del servidor y del cliente
- Técnicas para evitar inyecciones SQL y ataques de script cross-site
- Sanitización de datos y filtrado de entradas no confiables
- Controles específicos para APIs y servicios web

## 6. Autenticación y gestión de sesiones

- Diseño de sistemas de autenticación robustos
- Implementación de mecanismos de autenticación multifactor (MFA)
- Gestión segura de tokens de sesión
- Prevención de ataques como robo de sesión y fuerza bruta

## 7. Gestión de credenciales y control de acceso

- Prácticas recomendadas para almacenar y gestionar credenciales de manera segura
- Implementación de control de acceso basado en roles (RBAC) y basado en atributos (ABAC)
- Prevención de escalamiento de privilegios
- Manejo de claves y cifrado de contraseñas

# Temas detallados

## 8. Cifrado y protección de datos

- Principios y algoritmos de cifrado (AES, RSA, ECC)
- Encriptación en tránsito y en reposo
- Uso seguro de librerías criptográficas
- Implementación de protocolos como HTTPS y TLS/SSL
- Buenas prácticas en la gestión de claves criptográficas

## 9. Pruebas de seguridad en software

- Pruebas de penetración y escaneo de vulnerabilidades
- Herramientas automatizadas y manuales para pruebas de seguridad (ZAP, Burp Suite, etc.)
- Técnicas de fuzzing y análisis estático de código
- Pruebas de seguridad a nivel de integración y sistema

## 10. Gestión de vulnerabilidades y parches

- Proceso de identificación y gestión de vulnerabilidades
- Ciclo de vida de los parches y su integración en el SDLC
- Respuesta rápida ante vulnerabilidades descubiertas en producción
- Uso de herramientas automatizadas para la detección y mitigación de vulnerabilidades (SAST, DAST, etc.)

# Temas detallados

A thick blue line that starts horizontally from the left edge, then drops vertically, then diagonally down to the right, and finally continues horizontally to the right edge.

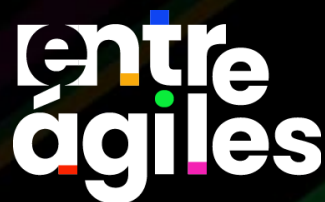
## 11. Control de configuraciones seguras

- Gestión segura de configuraciones de software
- Protección contra configuraciones inseguras por defecto
- Implementación de políticas de seguridad para entornos de producción

## 12. Gestión del ciclo de vida de software seguro (SDLC)

- Integración de prácticas de seguridad en cada fase del SDLC
- Planificación y revisión de código seguro en desarrollo ágil y DevOps
- Introducción a DevSecOps y cómo automatizar la seguridad en el pipeline deCI/cD
- Monitoreo continuo de seguridad en las aplicaciones

# Contáctanos



## Colombia

Teléfono: (+601) 768 32 57 - (+57) 305 812 0792

Dirección: Cra. 28 #73-30, Bogotá



## Estados Unidos

Teléfono: 1-9546558281

Dirección: 210 Ne 45Th Oakland Park

Fort Lauderdale, FL 33334



## España

Teléfono: (+34) 605366863

Dirección: Calle de Valle de Oro, 50,

28019 Madrid

