USIL EPG

Innovación, IA y Tecnología

PROGRAMA INTERNACIONAL EN

CIBERSEGURIDAD DEFENSIVA Y OFENSIVA

INICIO: 16 de setiembre

DURACIÓN:
72 horas

MODALIDAD:
Virtual sincrónica

HORARIO:
Martes y jueves
7:30 p. m. a 10:30 p. m.

CERTIFICACIÓN:
A nombre de la Escuela de Posgrado USIL

APLICACIÓN PRÁCTICA

Proyecto Integrador
Desarrollar un plan integral de ciberseguridad.

CONFERENCIA INTERNACIONAL

IA y su impacto en la transformación digital.

epg.usil.edu.pe

Descripción del programa

La ciberseguridad es crucial para proteger nuestros activos digitales y garantizar la continuidad de los negocios en un mundo cada vez más conectado. Nuestro programa está diseñado para equipar a profesionales con las habilidades necesarias para enfrentar los desafíos actuales y futuros en seguridad informática.

Cada curso se enfoca en proporcionar tanto conocimientos teóricos como aplicaciones prácticas, utilizando las últimas herramientas y tecnologías disponibles en el campo de la ciberseguridad. Desde la evaluación de riesgos hasta la protección de redes y sistemas, nuestros participantes aprenderán habilidades clave para identificar, prevenir y responder eficazmente a las amenazas cibernéticas.

Serás capaz de

1 **Adquirir conocimientos fundamentales:** Nuestro programa se enfoca en proporcionar a los participantes una comprensión sólida de los principios básicos de la ciberseguridad. Aprenderás conceptos fundamentales, identificarás amenazas comunes y aprenderás las mejores prácticas de protección.

2 **Desarrollar habilidades prácticas:** A través de aplicaciones prácticas y ejercicios simulados, adquirirás habilidades prácticas en el uso efectivo de herramientas y tecnologías actuales de ciberseguridad. Esto te permitirá identificar, prevenir y responder de manera efectiva a las amenazas cibernéticas.

3 **Fomentar la gestión estratégica:** El programa también se enfoca en equipar a los participantes con habilidades de gestión estratégica en ciberseguridad. Aprenderás a evaluar riesgos, desarrollar políticas y procedimientos, y planificar respuestas a incidentes. Esto garantizará que la seguridad informática esté alineada con los objetivos organizacionales.

4 **Promover la integración y aplicación:** se facilitará la integración de los conocimientos y habilidades adquiridos a través de un proyecto final integrador. En este proyecto, diseñarás e implementarás soluciones integrales de ciberseguridad en un entorno simulado. Esto consolidará tu comprensión y te preparará para enfrentar desafíos del mundo real con confianza y eficacia.

Perfil del participante

Nuestro programa de ciberseguridad está diseñado para profesionales de TI, gerentes de seguridad de la información, auditores de sistemas, consultores de seguridad y persona interesada en fortalecer la ciberseguridad de su organización.

Requisitos de admisión

- Copia o foto de DNI (ambos lados).
- Ficha de inscripción.
- Acuerdo de matrícula.
- Experiencia laboral mínima de un año.

Skills

Al finalizar el programa dominarás las siguientes competencias:

- **Análisis de riesgos:** Evaluar y gestionar riesgos de seguridad en sistemas y redes.
- **Cumplimiento normativo:** Aplicar normativas y estándares de seguridad cibernética.
- ***Ethical hacking:*** Desarrollar habilidades para identificar y explotar vulnerabilidades de manera ética.
- **Respuesta a incidentes:** Capacitarse en identificar, detectar, responder incidentes de ciberseguridad seguridad.
- **Seguridad en redes:** Proteger infraestructuras de redes contra amenazas cibernéticas.
- **Auditoría de seguridad:** Evaluar la eficacia de las medidas de seguridad implementadas.
- **Conocimientos en *frameworks* internacionales:** Conocer otros lineamientos de ciberseguridad a nivel general tales como *CIS Controls,* NIST CSF, ISO 19001, entre otros.

Por qué somos diferentes

El programa se centra en el desarrollo de habilidades técnicas y prácticas en áreas como *Ethical hacking*, respuesta a incidentes, y auditoría de ciberseguridad. Lo que permite a los participantes estar preparados para enfrentar desafíos del mundo real en ciberseguridad.

Docentes con amplia experiencia en el campo de la ciberseguridad, lo que garantiza que los participantes reciban una formación de alta calidad y relevante para las demandas actuales del mercado laboral.

Durante el programa, los participantes utilizarán herramientas y tecnologías de vanguardia utilizadas en la industria de la ciberseguridad, lo que les permite adquirir experiencia práctica con tecnologías reales.

Ruta de aprendizaje

1. Introducción al *Ethical Hacking* y *Pentesting*.
2. Respuesta y Gestión de incidentes de Ciberseguridad.
3. Ciberinteligencia, *Threat Hunting* y *Osint*.
4. Gestión y Plan de Auditoría de Ciberseguridad.

Proyecto Integrador
Desarrollar un plan integral de ciberseguridad.

Conferencia Internacional:
IA y su impacto en la transformación digital.

Potencia tu liderazgo y empleabilidad accediendo a los *workshops* exclusivos para nuestros estudiantes.

- Marca personal digital
- Networking
- LinkedIn
- Entrevistas efectivas

La Conferencia Internacional y los *workshops* son opcionales, a los que nuestros alumnos pueden acceder libremente hasta tres meses después de haber finalizado las clases de su programa.

Cursos

Introducción al *Ethical Hacking* y *Pentesting*

Este curso es ofensivo, por lo que da los fundamentos necesarios para responder eficazmente a incidentes de seguridad cibernética, incluyendo la detección, contención y recuperación de incidentes.

Fundamentos de *ethical hacking*

- Introducción al concepto y objetivos del *hacking* ético.
- Diferencias entre *hacking* ético, *black hat* y *grey hat*.
- Herramientas, metodologías y ciclo de vida de un test de penetración.

Ingeniería social

- Principios y técnicas de manipulación y persuasión.
- Análisis de ataques reales y sus consecuencias.
- Estrategias de defensa y concientización para prevenir ataques de ingeniería social.

Reconocimiento y enumeración

- Metodologías para la recopilación de información (OSINT).
- Técnicas de escaneo pasivo y activo.
- Herramientas para identificar sistemas, redes y servicios objetivo.

Escaneo de vulnerabilidades

- Diferencias entre escaneo y enumeración.
- Uso de herramientas de escaneo automatizado y manual.
- Análisis e interpretación de resultados para identificar puntos débiles.

Explotación de vulnerabilidades

- Métodos para aprovechar vulnerabilidades detectadas.
- Prácticas de explotación controlada en entornos seguros.
- Ejecución de exploits y evaluación de impactos.

Post-explotación y mantenimiento de acceso

- Técnicas para escalar privilegios y mantener el acceso.
- Recolección de información posterior a la explotación.
- Estrategias para evitar la detección y asegurar la persistencia en el sistema.

Evasión de medidas de seguridad

- Métodos para burlar sistemas de detección y prevención.
- Técnicas de ofuscación y encubrimiento de actividades.
- Análisis de casos y contramedidas adoptadas por las organizaciones.

Herramientas utilizadas:

- Kali Linux
- Metasploit
- Wireshark
- Nmap
- Burp Suite
- Y otras herramientas populares de *hacking* ético.

Trabajo aplicado: los participantes deberán realizar un *pentest* completo en un entorno simulado, aplicando todas las técnicas y herramientas aprendidas durante el curso para identificar y explotar vulnerabilidades, y presentar un informe detallado con recomendaciones de seguridad.

Respuesta y Gestión de Incidentes de Ciberseguridad

Este curso es defensivo, por lo que da los fundamentos necesarios para responder eficazmente a incidentes de seguridad cibernética, incluyendo la detección, contención y recuperación de incidentes con los objetivos estratégicos de la organización.

Introducción a la respuesta a incidentes y el marco MITRE ATTaCK

- Conceptos básicos de respuesta a incidentes.
- Introducción al *framework* MITRE ATTaCK y su aplicación práctica.

Gestión de incidentes según ISO 27035

- Principios y normas de la ISO 27035
- Procedimientos y mejores prácticas para la gestión de incidentes.

Plataforma de monitoreo de ciberseguridad

- Herramientas y tecnologías de monitoreo.
- Integración de sistemas de detección y análisis en tiempo real.

Práctica de detección de incidentes

- Ejercicios prácticos de identificación y análisis de eventos
- Simulaciones y uso de herramientas de monitoreo para detectar anomalías.

Teoría de contención, erradicación y recuperación

- Estrategias para contener y mitigar incidentes.
- Procedimientos para la erradicación de amenazas y la recuperación de sistemas.

Plan de respuesta a incidentes y desarrollo de *playbooks*

- Elaboración de un plan integral de respuesta a incidentes.
- Creación y personalización de *playbooks* para diversos escenarios.

Herramientas utilizadas:

- Excel, Word.
- Kali Linux.
- SIEM *(Security Information and Event Management)* WAZUH.
- Herramientas de detección de intrusiones WIRESHARK.
- Herramientas de análisis forense digital.

Trabajo aplicado: los participantes deberán desarrollar un plan de respuesta a incidentes para una organización simulada, incluyendo la detección, contención, recuperación y análisis de lecciones aprendidas de un incidente simulado.

Ciberinteligencia, *Threat Hunting y Osint*

Este curso tiene carácter defensivo por lo que proporciona fundamentos de la ciberinteligencia, incluyendo la recolección, análisis y uso de información para proteger activos digitales y prevenir ataques cibernéticos.

Introducción y ciclo de vida de la ciberinteligencia

- Definición y objetivos de la ciberinteligencia.
- Importancia en el contexto de la ciberseguridad.
- Etapas del ciclo de vida de la ciberinteligencia (planificación, recolección, procesamiento, análisis, difusión y retroalimentación).

Técnicas de recolección de información

- Fuentes abiertas (OSINT) y otras fuentes de datos.
- Métodos pasivos y activos de recopilación.
- Herramientas y técnicas para obtener información relevante.

Análisis de inteligencia

- Procesos y metodologías de análisis de datos.
- Evaluación y validación de la información recopilada.
- Identificación de patrones, tendencias y amenazas emergentes.

Uso de la inteligencia en la toma de decisiones

- Integración de la inteligencia en la estrategia de ciberseguridad.
- Ejemplos de aplicación en la respuesta a incidentes y gestión de riesgos.
- Elaboración de reportes y difusión de hallazgos para la toma de decisiones.

Herramientas utilizadas:

- Cyber Kill Chain
- MITRE ATTaCK *framework*.
- Otras herramientas de análisis de inteligencia.

Trabajo aplicado: los participantes deberán realizar un análisis de inteligencia sobre un caso práctico, aplicando las técnicas y herramientas aprendidas durante el curso para identificar posibles amenazas y proponer medidas de protección.

La EPG-USIL se reserva el derecho de cancelar o modificar las fechas de sus programas y comunicarlas con la debida anticipación.

Una vez iniciadas las clases no se podrá solicitar la devolución de la primera cuota.

Gestión y Plan de Auditoría de Ciberseguridad

Este curso tiene carácter defensivo por lo que proporciona los conocimientos y habilidades necesarios para llevar a cabo auditorías de ciberseguridad efectivas en organizaciones, garantizando el cumplimiento de normativas y estándares de seguridad.

Introducción a la auditoría de ciberseguridad

- Definición y objetivos de la auditoría de ciberseguridad.
- Importancia en la gestión de riesgos y protección de la información.
- Roles y responsabilidades de los auditores y equipos de seguridad.

Normativas y estándares de seguridad

- Revisión de normativas y marcos de referencia (ISO, NIST, GDPR, entre otros).
- Relación entre los estándares y la auditoría de ciberseguridad.
- Cómo aplicar estos marcos en la evaluación de la seguridad.

Planificación y ejecución de auditorías

- Definición del alcance, objetivos y metodología de la auditoría.
- Herramientas y técnicas para la recopilación de información y evidencias.
- Fases de la auditoría: preparación, ejecución y seguimiento.

Evaluación de riesgos y vulnerabilidades

- Identificación y análisis de riesgos en entornos tecnológicos.
- Metodologías para la evaluación de vulnerabilidades.
- Integración de los resultados de evaluaciones en la auditoría.

Análisis de hallazgos y elaboración de informes

- Procesamiento y análisis de la información recopilada.
- Redacción de informes claros y concisos: estructura y elementos clave.
- Recomendaciones, plan de acción y comunicación de resultados a la alta dirección.

Auditoría continua y mejores prácticas en ciberseguridad

- Concepto e importancia de la auditoría continua
- Implementación de un programa de auditoría continua
- Mejores prácticas en auditoría de ciberseguridad
- Auditoría y fomento de una cultura de seguridad
- Tendencias futuras en auditoría de ciberseguridad

Herramientas utilizadas:

- Herramientas de análisis de vulnerabilidades.
- Herramientas de auditoría de seguridad.

Trabajo aplicado: los participantes deberán realizar una auditoría de ciberseguridad en una organización simulada, aplicando las técnicas y herramientas aprendidas durante el curso. Presentarán un informe detallado con los hallazgos y recomendaciones para mejorar la seguridad de la organización.

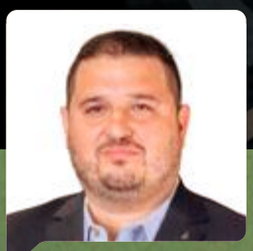
Proyecto Integrador Desarrollar un plan integral de ciberseguridad

En este proyecto integrador, los participantes aplicarán los conocimientos adquiridos a lo largo del programa para abordar un caso real de gestión de ciberseguridad. Utilizarán las metodologías, herramientas y técnicas aprendidas para analizar, diseñar e implementar soluciones de ciberseguridad efectivas.
Los participantes trabajarán en equipos para desarrollar un plan integral de ciberseguridad para una organización simulada, teniendo en cuenta aspectos como la evaluación de riesgos, la implementación de medidas de seguridad, la respuesta a incidentes y el cumplimiento normativo. Al finalizar, presentarán sus soluciones ante un panel de expertos, demostrando su capacidad para enfrentar desafíos reales en el campo de la ciberseguridad con foco en una implementación práctica.

El dictado de clases del programa se iniciará siempre que se alcance el número mínimo de alumnos matriculados establecido por USIL.

Para la entrega de certificados son requisitos indispensables alcanzar una nota mínima de 11 en cada uno de los cursos del programa, no haber superado el 30 % de inasistencias y haber cancelado la inversión económica total del programa.

Profesores *practitioners*



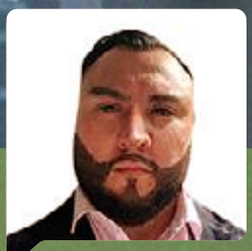
Sebastián Vargas Yañéz

Gerente general en TTPSEC SPA ® Consultoría de Estrategia, Tecnología y Ciberseguridad.

- Tiene más de 18 años de experiencia en el ámbito de la ciberseguridad y ha ocupado diversos cargos como OSI, CISO o CSO en el sector público, financiero y en empresas vinculadas con la infraestructura crítica de Chile.
- Máster en ciberseguridad industrial del Centro de Ciberseguridad Industrial en España.
- Máster en gestión de tecnologías de la información por la Universitat Oberta de Catalunya en España.
- Máster en ciberseguridad, ciberterrorismo y ciberguerra por la Universidad Pegaso en Italia.
- Ingeniero civil en informática e ingeniero en ciberseguridad por la Universidad Tecnológica de Chile.

Posee diversas certificaciones tales como:

- Certified Ethical Hacker (Practical).
- eLearnSecurity Certified Incident Responder (eCIR).
- eLearnSecurity Certified Digital Forensics Professional (eCDFP).
- eLearnSecurity Junior Penetration Tester (eJPT).
- MITRE ATT&CK Fundamentals.
- MITRE ATT&CK PurpleTeam.
- MITRE ATT&CK for Cyber Threat Intelligence.
- MITRE ATT&CK for Security Operations Center Assessments.
- MITRE ATT&CK for Adversary Emulation Methodology.
- MITRE ATT&CK for Threat Hunting Detection Engineering.
- Implementador y auditor de ISO 27001.
- C|CISO.



Julio Briones Navarro

Chief information security officer en Intervial Chile S. A.

- Más de 18 años de experiencia adquirida en seguridad de la información, ciberseguridad y continuidad operativa en el sector bancario, financiero e infraestructura crítica.
- Fundador de la comunidad de ciberseguridad Level 0 Sec y vicepresidente en la Fundación Sochisi (Sociedad Chilena de Seguridad de la Información).
- Magíster en ciberseguridad por la Universidad de Barcelona (España).
- Master en ciberterrorismo y ciberguerra por la Università Telematica Pegaso (Nápoles, Italia).
- Ingeniero en conectividad y redes de DUOC UC.

Posee diversas certificaciones tales como:

- Certified Information Security Manager.
- Cybersecurity Nexus.
- Certified Chief Information Security Officer.
- Certified Ethical Hacker v11.
- Computer Hacking Forensic Investigator.
- Certified Incident Handle.
- Certified Threat Intelligence Analyst.
- Certified Security Analyst.
- Certified SOC Analyst.

La EPG-USIL se reserva el derecho de modificar su plana docente, ya sea por motivos de fuerza mayor o por disponibilidad del profesor, sin afectar la calidad académica del programa.

Más información

981 458 741
informes.epg@usil.edu.pe
@usileducacionejecutiva
EPGUSIL

#EducaciónEjecutivaUSIL

epg.usil.edu.pe