

Oferta Práctcias Académicas externas - Curso 25-26

Referencia	Nome comercial	Web	Funcións	Prazas	Duración (en meses)	Xornada (horas semanais)	Dotación (brutos mes)	TFM
PR-25-26-1	ALTIA A Coruña/Vigo	https://www.altiacompany.co	•Consultoría: Adaptación a normativa de empresas privadas y administraciones públicas, planes directores y/o auditorías. •Defensivo: Mejora de la pila de Software de Ciberseguridad: SIEM, SOAR... Mejora de tareas de automatización de operaciones de seguridad. •Consultoría: Análisis código estático/dinámico de aplicaciones web, móviles y/o Test de penetración.	3			6€/h	Si
PR-25-26-2	2MARES (Vigo)	https://2mares.com/en/	•Diagnóstico e implementación de un plan de acción para la mejora integral de la seguridad de la información en los productos y procesos de la empresa. •Participación e incorporación transversal a flujos de gestión e innovación en el área de Data Analytics: Inteligencia Artificial (Machine Learning, Natural Language Processing, IA Ética) •Arquitecturas Software Cloud •Interfaces Avanzados Responsive •Big Data	1		30	300 € / jornada 8:00 a 14:00	Si
PR-25-26-3	ABANCA CORPORACIÓN BANCARIA S.A. (A Coruña)	https://www.abanca.com/es/	-Diseño de Reporting Estratégico: Creación y evolución de dashboards de ciberseguridad, integrando métricas técnicas (vulnerabilidades, eventos) para ofrecer una visión 360° del estado de ciberseguridad. -Automatización de GRC: Impulsar la eficiencia operativa mediante la automatización del ciclo de vida del reporting y los indicadores de riesgo (KRI/KPI), eliminando procesos manuales. Utilización de herramientas ofimáticas e IAs corporativa. -Gobernanza y Control: Evaluar la efectividad del entorno de control, identificando brechas (gaps) y colaborando con equipos para asegurar una remediación real y efectiva. -Análisis de Riesgos de Ciberseguridad: Participar en la identificación de debilidades en activos y proponer mejoras que fortalezcan nuestro modelo de GRC bajo estándares internacionales.	1	2	27.5	800 €	No
PR-25-26-4	ABANCA CORPORACIÓN BANCARIA S.A. (A Coruña)	https://www.abanca.com/es/	Prácticas para desempeñar actividades relacionadas con la gestión de riesgos TIC y la resiliencia digital (p.e. DORA), aspectos de gran trascendencia en el sector financiero que se acabarán extendiendo a otros sectores de actividad. Dada la naturaleza y actividades asociadas a la función de Riesgo Tecnológico (RT), la cual dispone de una visión 360 de múltiples ámbitos de control, se valorará muy positivamente el "background tecnológico" (p.e. TIC, Cyber) y complementariamente el "background normativo". Si bien parte de los servicios y actividades de RT dentro del alcance son de tipo normativo/consultivo, la gran mayoría y más importantes son de tipo tecnológico/operativo dada la interacción y supervisión que realiza la función de RT con/sobre otras áreas especialistas que conforman el Marco de Gestión de Riesgos TIC (p.e. TI, Seguridad, Continuidad, etc.).	1	2	27.5	800	No
PR-25-26-5	ALDABA (A Coruña)	https://www.aldaba.es/	El/la alumno/a pasará a formar parte del equipo de Ciberseguridad, integrándose en actividades orientadas a la protección de entornos corporativos y servicios en la nube. El/la estudiante conocerá el área a un nivel profundo y tendrá interacción directa con clientes. Algunas de las actividades en las que tomará parte serán las siguientes: • Participación en proyectos de ciberseguridad para grandes clientes de distintos sectores, utilizando tecnologías punteras. • Asimilación y aplicación de la metodología de trabajo del área, con el acompañamiento continuo de un/a tutor/a. • Gestión de la seguridad en entornos cloud (Microsoft 365, Azure, entornos híbridos), incluyendo monitorización y protección de servicios. • Configuración y gestión de soluciones de seguridad como firewalls, herramientas EDR/XDR y sistemas de detección de amenazas. • Monitorización de eventos de seguridad y análisis de logs (correo, endpoints, identidades y cloud), mediante herramientas como Microsoft Defender y registros de auditoría. • Participación en auditorías de seguridad, revisión de configuraciones y análisis de vulnerabilidades. • Apoyo en tareas de respuesta ante incidentes de seguridad, incluyendo investigación, análisis y documentación de los mismos. • Análisis de vulnerabilidades en aplicaciones web, incluyendo identificación de posibles fallos de seguridad y apoyo en pruebas de hacking ético.	2	3	30	900 euros por 30h/semanales. Pero tanto la jornada semanal, como la duración total, sería a convenir con la persona. La retribución sería proporcional a la jornada semanal siguiendo la proporción 40h-1200 euros/brutos mes.	No

PR-25-26-6	ALTER TECHNOLOGY (Madrid)		Tareas del Laboratorio de ensayos o equipo de proyectos, participando directamente en los servicios de ensayos y gestión de proyectos que ofrece ALTER. Referir a nuestra web para el tipo de servicios que ofrecemos en ALTER: Certificación de equipos electrónicos	1		A valorar	A valorar	Si
PR-25-26-7	ATLANTIC (Vigo)	https://teleco.uvigo.es/documentos/ofertas/ofertas-municipis/oferta-practicas-municipis-atlantic-2026-2027/					Non	
PR-25-26-8	Balidea Consulting & Programming S.L. Santiago (posibilidad teletrabajo)	https://www.balidea.com/	O Estudiante realizará actividades englobadas en distintos bloques ou módulos dentro do departamento de Ciberseguridade de Balidea, De carácter interno como: - Revisión e monitorización de cumprimento das normativas do ENS e ISO 270001 - Revisión e monitorización do sistema de seguridade perimetral de Balidea - Lanzamento de campañas de simulación de phishing aos usuarios de Balidea - Revisión, monitorización e tuneado de políticas do noso ICES (Integrated Cloud Email Security) E (Universidade de Vigo-Universidade da Coruña) - Integración e posta en marcha do xestor de contrasinais para os distintos departamentos de Balidea - Actividades en laboratorio coa nosa ferramenta SAST para análise de código estática e SCA para librerías de terceiros - Revisión e monitorización do noso sistema de parcheo de sistemas e aplicacións de terceiros De carácter externo como: - Estudo de alternativas ás solucións de ciberseguridade coas que se traballa en Balidea - Charla sobre algún tema de interese nas Balidea CyberTalks - Revisión das actividades que realizan os distintos grupos de Balidea para clientes públicos e privados en específico polo grupo de monitorización e implantación da ciberseguridade dunha administración pública que da servizo a case 100.000 habitantes. Os responsables explicarán ao estudante cales son as responsabilidades do grupo co cliente e as actividades que se realizan dentro do contrato para ensinar ao estudante as tarefas que pode ter que realizar unha vez finalizado o período de prácticas e se pretende formalizar unha relación contractual entre o estudante e Balidea. - Revisión e tradución de vulnerabilidades de seguridade, clasificación e reporte das mesmas.	2	2	30	900€ brutos a jornada completa	Si
PR-25-26-9	Centro Tecnológico ITG (Santiago)	www.itg.es	Buscamos un/a estudiante interesado/a en realizar sus prácticas en el área de seguridad cuántica y post-cuántica, colaborando en proyectos de I+D y contribuyendo al diseño, implementación y validación de soluciones de comunicación segura en entornos reales. Tus principales tareas serán: - Apoyar en el diseño e implementación de prototipos que integren algoritmos post-cuánticos, mecanismos de intercambio seguro de claves y protocolos QKD. - Colaborar en la configuración, securización y validación de la red cuántica experimental de ITG. - Analizar amenazas, riesgos y posibles vectores de ataque en arquitecturas híbridas PQC/QKD. - Evaluar la integración de tecnologías post-cuánticas en servicios de comunicación como TLS, VPN, APIs seguras o sistemas de gestión de claves. - Participar en pruebas de seguridad, validación funcional y documentación técnica de los sistemas desarrollados. - Analizar estándares y recomendaciones actuales sobre criptografía post-cuántica, comunicaciones seguras y gestión criptográfica. - Contribuir con ideas y desarrollos a proyectos de investigación en curso desde una perspectiva de ciberseguridad aplicada.	1	3	20	650	Si
PR-25-26-10	CESGA (Santiago)	https://www.cesga.es	Colaboración para la securización de las infraestructuras críticas del centro	1	6	39	No remunerar	No
PR-25-26-11	CESGA (Santiago)	https://www.cesga.es	Implementar medidas organizativas orientadas a la consecución e implantación del ENS	1	3	20	0	No
PR-25-26-12	COINSCRAP (Ourense)		Colaboración con el equipo de seguridad y sistemas de la compañía en el roadmap de seguridad en temas de sistemas (Kubernetes), Cloud (AWS), Prueba de caja gris, penetración, Testing. También se tendrá accesos y parte en las tareas relacionadas con la certificación ISO27001 que la empresa tiene hace varios años.	2			Non	Si
PR-25-26-13	CRTVG (Santiago)	https://crtvg.gal/	Cumplimiento de la CRTVG con el Esquema Nacional de Seguridad. Adecuación del marco normativo (normas, procedimientos corporativos- plan respuesta a incidentes, etc.) y operacional (controles de acceso, plataformas Cloud, etc.). Implementación de medidas tecnológicas de protección.	1			Si	A valorar
PR-25-26-14	ENXENIO (A coruña)	https://www.enxenio.es/	1. Análisis de eventos de seguridad con herramientas como SIEM, EDR, DLP, etc. 2. Afinamiento de herramientas de seguridad como SIEM, EDR, DLP, etc. 3. Apoyo en el proceso de gestión de vulnerabilidades. 4. Análisis de campañas de phishing.	1	2	37	1300€ para las 225h (prorratable al mes en función de la jornada semanal acordada)	No

PR-25-26-15	Forensic & Security S.L. A Coruña	www.forensic-security.com	• Monitorizar y analizar alertas de seguridad en tiempo real para identificar amenazas potenciales. • Investigar y documentar incidentes de seguridad, proporcionando informes detallados. • Asistir en la implementación y configuración de herramientas de seguridad. • Ser proactivo en las tareas diarias. Formación y aprendizaje continuo.	2	2	35	850	No
PR-25-26-16	GRADIENT (Vigo)	https://gradient.org/	1. Integración de middleware criptográfico con Apache Fineract: En el contexto de una iniciativa para construir una solución financiera completa, disponemos de un middleware criptográfico que actúa como capa de abstracción entre aplicaciones financieras y módulos de hardware seguro (HSM). Las prácticas consistirán en investigar la plataforma de core bancario Apache Fineract y diseñar un mecanismo de integración entre ambos sistemas. El estudiante analizará los puntos del flujo bancario donde intervienen operaciones criptográficas, propondrá y desarrollará prototipos de integración mediante API o extensiones de Fineract, y validará su funcionamiento mediante pruebas de concepto. Java (requerido), Docker (aconsejable) 2. Análisis de los peligros, limitaciones y retos en la detección de imágenes obtenidas mediante IA generativa. Hoy en día la IA generativa es capaz de generar imágenes de gran realismo e imposibles de identificar como sintéticas por cualquier operario humano. En paralelo, el desarrollo de sistemas capaces de identificar si una imagen es real o ha sido generada por IA es un problema cada vez más complejo de resolver. La literatura científica aborda este problema utilizando otras IAs o arquitecturas de deep learning que se supone puedan ser capaces de detectar contenido generado por una IA generativa. Por ello, en esta práctica se propone explorar los posibles límites que pueden existir a la hora de detectar imágenes sintéticas, además de tratar de abordar el problema de la detección de dichas imágenes utilizando de forma innovadora las arquitecturas de IA existentes en la actualidad. Python PyTorch/TensorFlow, visión por computador (CNNs), procesamiento de imagen, buenas prácticas de ML y experimentación, investigación. 3. Mejora de algoritmos avanzados para la detección de imágenes manipuladas por IA El/la estudiante participará en la revisión y análisis del estado del arte en técnicas de detección de imágenes manipuladas mediante modelos de IA. Su trabajo consistirá en entrenar, ajustar y validar modelos existentes para mejorar su robustez frente a nuevos generadores y escenarios adversos. Además, contribuirá al diseño de pipelines de preprocesado, evaluará el rendimiento del sistema con distintos datasets públicos y privados, y documentará los resultados obtenidos junto con recomendaciones de mejora. Python PyTorch/TensorFlow, visión por computador (CNNs, ViTs), procesamiento de imagen, buenas prácticas de ML y experimentación. 4. Mejora de algoritmos avanzados para la detección de vídeos manipulados por IA El/la estudiante llevará a cabo un análisis de técnicas de detección de vídeo manipulado mediante IA, estudiando tanto aproximaciones basadas en frames individuales como métodos que explotan la coherencia temporal. Sus tareas incluirán el entrenamiento de modelos espacio-temporales, la optimización del pipeline de extracción de frames y características, y la evaluación de la robustez del	4			Si	Si
PR-25-26-17	Ikerlan S.Coop Arrasate / Mondragón	https://www.ikerlan.es/	Participar en proyectos aplicados a los retos reales de la organización.	3	6	35	1174	Si

PR-25-26-18	Inprosec // InprOTech (Vigo)	https://www.inprosec.com/ https://inprotech.es/	Inprosec: Apoyo en proyectos de ciberseguridad reales Apoyo en tareas de Gobierno, riesgo y cumplimiento en seguridad de la información. Apoyo en tareas de seguridad ofensiva y pruebas de penetración. Apoyo en tareas de arquitectura de seguridad. Apoyo en ejercicios de concienciación y cultura en seguridad. Lanzamiento de campañas de ingeniería social en entornos reales. InprOTech El estudiante participará en una línea de investigación y desarrollo orientada a la incorporación de nuevos mecanismos o mejoras de los mismos, de: - visibilidad, - detección de anomalías - y/o inteligencia de amenazas en una plataforma real de protección de activos ciberfísicos (CPS PP) para entornos industriales. Posibles tareas (podrá ser un subconjunto de estas u otras a convenir con el alumno): Definición e integración de nuevas reglas programáticas de detección de anomalías Creación de un sistema para la automatización de reglas en base a parámetros conocidos del sistema Integración del framework MITRE ATT&CK Integración de fuentes europeas de inteligencia de amenazas y enriquecimiento de alertas de seguridad Bloqueo de conexiones maliciosas en redes 5G privadas Mejora de inventario de activos y mapa de red Generación de informes de servicio mediante LLMs	2	1.5	39.75	675 brutos/mes	Si
PR-25-26-19	ITELSYS (Arteixo/A Coruña)	https://www.itelsis.com/	*Gestión, supervisión y desarrollo SIEM. *Análisis de vulnerabilidades de equipos y sistemas. *Auditoría de sistemas y procesos	1			Si	Si
PR-25-26-20	KREIOS SPACE (Vigo-Nigrán)	https://www.kreiosspace.com	Departamento de Propulsión, Telecomunicaciones *Aprendizaje para la realización del análisis de enlaces de comunicaciones espaciales en escenarios tierra-espacio y espacio-espacio dentro del ámbito de las telecomunicaciones. *Participación en el análisis y modelado de sistemas de comunicación en entornos espaciales. *Aprendizaje para diseñar, evaluar y optimizar parámetros de antenas según los requisitos del sistema *Desarrollo de estudios de emisión y recepción de señales considerando limitaciones técnicas y operativas. *Elaboración de documentación técnica y soportar la toma de decisiones con argumentos basados en rendimiento, viabilidad y requisitos de negocio en el sector telecom. *Colaboración con otros equipos de ingeniería para asegurar la coherencia entre diseño, modelado y necesidades comerciales	5			A valorar	Si
PR-25-26-21	NAVANTIA (Ferrol)	https://www.navantia.es/en/	*Apoyo técnico en tareas de análisis y revisión de arquitecturas de ciberseguridad en entornos IT/OT y Cloud. * Colaboración en la identificación y análisis de desviaciones en la aplicación de marcos normativos (ENS, ISO/IEC 27001). * Apoyo en la aplicación de medidas de ciberseguridad en proyectos industriales conforme a IEC 62443. * Análisis y comprobación de medidas de ciberseguridad implantadas a nivel de activos IT/OT.	2			A valorar	A valorar

PR-25-26-22	NTT DATA (A Coruña/Vigo)	https://es.nttdata.com/	Hacking / Pentesting (2 plazas) • Ejecución de pruebas de seguridad en aplicaciones web, móviles y APIs. • Soporte en campañas de Ethical Hacking y análisis de vulnerabilidades. • Uso de herramientas de pentesting y metodologías OSSTMM/OWASP. • Elaboración de evidencias y apoyo en reporting técnico. GRC – Gobierno, Riesgo y Cumplimiento (2 plazas) • Identificación y análisis de riesgos de ciberseguridad. • Soporte en marcos de cumplimiento: ISO 27001, ENS, NIST CSF. • Preparación de documentación y planes de mejora. • Apoyo en auditorías internas y externas. Arquitectura de Seguridad / Cloud / DevSecOps (3 plazas) • Análisis de arquitecturas técnicas y diseño de controles de seguridad. • Soporte en iniciativas de "Secure by Design" y SSDLC. • Evaluación de configuraciones en nubes públicas (Azure, AWS, GCP). • Automatización de controles y seguridad en pipelines CI/CD. IAM – Identity & Access Management (1 plaza) • Gestión de identidades, roles, privilegios y accesos. • Apoyo en proyectos de federación, SSO, MFA y ciclo de vida de cuentas. • Uso de tecnologías líderes del mercado (Okta, Azure AD, etc.). Ciber Cross – Servicios Transversales. Este bloque permitirá exposición y rotación por distintas áreas (2 plazas) • Apoyo en gestión de vulnerabilidades y análisis de superficies de ataque. • Participación en actividades de Threat Intelligence. • Soporte en documentación, métricas, reporting y PMO técnica. • Conocimiento global del ecosistema de ciberseguridad de NTT DATA.	10			480€/mes por 20h/semanales	Si
PR-25-26-23	ODEENE Security (A Coruña)	https://odeenesecurity.com/	Análisis y supervisión en ciberseguridad	2	3	40	900	No
PR-25-26-24	QBITIA (Vigo)	https://qbitia.com/en/	El alumno/a formará parte del equipo de trabajo de ciberseguridad dependiente del Comité de Continuidad de Negocio. Entre las tareas estará: • Apoyo en la actualización de las políticas y protocolos de ciberseguridad de la compañía: Implementación de "la ciberseguridad como un proceso continuo" • Implementación de protocolos y configuraciones derivadas de las mismas • Apoyo en la validación del cumplimiento de los estándares OWASP /OSSTMM en los proyectos • Coordinación apoyo en los trabajos de auditoría de seguridad externas: (Validación plan director de seguridad/ Pen-tests/ hardware hacking / Hardening de sistemas)	1			Si	A valorar
PR-25-26-25	SPARKS, CIRCUITS AND ROBOTICS SL (Vigo)	https://srobotics.es/	Diseño e implantación de PKI para soluciones IoT	1			A partir de 264h	A valorar