

RELACIÓN DE EMPRESAS Y PLAZAS OFERTADAS PARA EL MASTER DE CIBERSEGURIDAD CURSO 22-23 (1)

NOTAS:

- 1) Verano: Significa que sí se pueden hacer en verano, aunque la mayoría de las empresas admiten otras épocas del año.
- 2) TFM: Significa que hay posibilidades de que el trabajo realizado se pueda convertir en un TFM.
- 3) Las empresas están colocadas por orden alfabético.

EMPRESA (Lugar de Trabajo)	Nº PLAZAS	TFM	VERANO	BOLSA	ACTIVIDAD
2MARES (Vigo) may@2mares.com	1	Si	Si	300€ Jornada de 8 a 14h	<ul style="list-style-type: none"> • 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). Arquitecturas Software Cloud. Interfaces Avanzados Responsive. Big Data.
ABANCA (Vigo) amartinezf@abanca.com	2	No	Si	800€/mes	El/la estudiante colaborará y dará apoyo en: -El control de las comunicaciones y sistemas de comunicación del banco. –La verificación de la conectividad y comunicación de los aplicativos del banco – La gestión de datos en la nube. –Etc.
BALIDEA (Santiago) juan.fernandez@balidea.com	1	Si	Si	864€ Jornada completa	<p>En consonancia con el Security Manager de Balidea, la persona seleccionada será partícipe de todo el proceso de gestión de un proyecto de implantación de la Ciberseguridad dentro de un organismo con miles de usuarios administración pública.</p> <p>Sus funciones principales serán:</p> <ul style="list-style-type: none"> • Monitorizar, crear y modificar alertas de seguridad y actuar en consonancia. • Gestión de vulnerabilidades y gestión de auditorías de seguridad sobre activos del cliente. • Tareas de explotación, más asociadas a Red Team para confirmar vulnerabilidades en algún activo del cliente de manera controlada. <p>Los distintos servicios de seguridad que se proveen en este entorno darán al estudiante una visión general de un proyecto de seguridad, sus posibilidades de crecimiento y los retos a los que nos enfrentamos diariamente.</p> <p>Este proyecto matriz se podrá paralelizar al proyecto interno de Ciberseguridad del departamento con herramientas específicas de seguridad y formación adicional centrada en las necesidades para trabajar tanto en empresa pública como privada.</p>
CODISOIL (Porriño) michaella@codisoil.com	1	Si	Si	300€	Nuestra organización, el pasado año, comenzó un proceso de transformación, hemos estado trabajando de manera externalizada, en procesos de Ciberseguridad que buscamos definir de manera precisa y adaptar para poder conseguir una certificación ISO 27000. Contamos en la organización con mecanismos de acceso a equipos MFA, Firewall, sistema de antivirus,... todos con Watchguard. El proyecto es a largo plazo, por lo que podría ser un puesto estable.
COINSCRAP FINANCE SL. (Remoto-Orense) oscar.barba@coinscrap.com	2	Si	Si	600€	Colaboración con trabajos relacionados con seguridad en la nube: Waf, auditorías de caja gris, mecanismos de autenticación de usuarios... Trabajos relacionados con requisitos de la ISO 27001, implantada en la empresa. Participación en informes de seguridad que requieren nuestros clientes: bancos y aseguradoras a nivel internacional.
CTAG (Porriño) sonia.llanes@ctag.com	2	Si	Si	Si y contrato laboral	<ul style="list-style-type: none"> • Dirección TIC y Operaciones: Este área transversal es la encargada de velar por el funcionamiento correcto de toda la infraestructura TI de CTAG, así como velar por la seguridad, integridad, disponibilidad de la información de la empresa. El/La estudiantes del master, podrá realizar tareas de seguridad de la información que gestiona el ISMS, análisis de seguridad de los servicios, seguimiento de eventos de seguridad y detección de los mismos, así como de su investigación y resolución a través de las distintas herramientas disponibles. EDR, SIEM, FW, AV, ect. En cuanto a los ISMS CTAG está alineado con la normativa de VDA con sus correspondientes auditorías y registro TISAX. • Ciberseguridad: Para que el vehículo del futuro esté más conectado con nuestro ecosistema, es necesario que sea seguro. El estudiante podrá aprender como se establece un sistema de ciberseguridad en un vehículo para una función concreta, desarrollando un sistema de protección junto con el equipo de desarrolladores.
GRADIANT (Vigo) rrhh@gradient.org	https://careers.gradient.org/jobs/1624786-empieza-tu-carrera-profesional-en-gradient				
INPROSEC (Vigo) rr.hh@inprosec.com	3	Si	Si	A Valorar	<ul style="list-style-type: none"> • Participar en la ejecución de proyectos relacionados con el Área de Seguridad de la Información (IS). • Realización de auditorías de seguridad en base a estándares y normas diversos (ISO 27001, NIST, ENS, VDA-ISA,). • Definición, Planificación y Desarrollo de Planes directores de Seguridad. • Definición e implantación de Sistemas de Gestión de Seguridad de la Información (SGSI) • Realización de Inventariado de Activos, Análisis de Riesgos y definición e implantación de Políticas y Procedimientos. • Preparación y organización y posible impartición de sesiones de formación y concienciación en Seguridad de la Información. • Realización e implantación de Planes de Continuidad TIC y/o de Seguridad de la Información. • Realización de presentaciones e informes ejecutivos sobre el estado de la seguridad en las organizaciones. • Elaboración de documentación de procesos, manuales, mejores prácticas en el área de la Seguridad de la Información y Seguridad Informática.
MOONOFF (Santiago) maria.gonzalez@moonoff.com	1	A Valorar	Si	Si	DEPARTAMENTO DE I+D - Verificación Automático de dispositivos en de Redes 5G.
PLEXUS (Teletrabajo) diego.penarivas@plexus.es	2	Si Empezar Abr./May	Si	A valorar	Gestión y configuración de herramientas defensivas para la gestión y automatización de respuestas a incidentes de seguridad
POSSIBLE (Vigo) administracion@espossible.com	1	Si	Si	A partir de 240h	<ul style="list-style-type: none"> • Departamento de ingeniería y desarrollo de software. • Formación en metodología Scrum para desarrollos iterativos. • Formación en Django python para poder desarrollar proyectos de extracción de conocimiento con elastic search, técnicas de estadística avanzada y algo de machine learning (básico).

					<ul style="list-style-type: none"> • Formación en React.js y Vue.js con componentes javascript para desarrollo de interfaces. • Aprendizaje de herramientas de gestión de proyectos colaborativos: youtrack, git, planner • Aprendizaje de herramientas de CI-CD: Rancher, jenkins, docker y kubernetes, sonarcube Testing automatizado con selenium
QBITIA (Vigo) rrhh@qbitia.com	1	Si	Si	Si	El alumno/a formará parte del equipo de trabajo de ciberseguridad dependiente del Comité de Continuidad de Negocio. Entre las tareas estará: <ul style="list-style-type: none"> • 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 auditoria de seguridad externas: (Validación plan director de seguridad/ Pen-tests/ hardware hacking / Hardening de sistemas).
SPARKS, CIRCUITS AND ROBOTICS SL (Vigo) x.crespo@scrobotics.es	1	Si	Si	No	Análise de vulnerabilidades en productos IoT
TARLOGIC (carolina.garcia@tarlogic.com) Remoto/Teo (A Coruña)	3	A Valorar	Si	600€	Tendríamos tres áreas posibles para que pudieran realizar las prácticas: <ul style="list-style-type: none"> • Prácticas Threat Hunter: Buscamos un estudiante que quiera aprender con nuestro área de Threat Hunting. Si quieres saber cómo realmente funciona el malware, además de analizar amenazas, APTs y TTPS, este es tu sitio. El estudiante podrá realizar técnicas de reversing en nuestro laboratorio y aprender a analizar técnicas, tácticas y procedimientos a bajo nivel. • Prácticas Red Team: Como miembro del Red Team, el estudiante se sumergirá en la operativa diaria del equipo participando, de forma activa y bajo supervisión, en las distintas fases de una intrusión en entornos reales. Así mismo, colaborará en el desarrollo de herramientas para uso interno, en la investigación de vulnerabilidades y tecnologías, y en la redacción y documentación de resultados. • Prácticas Ciberseguridad: El estudiante colaborará y dará apoyo en seguridad informática y hacking ético. Se familiarizará con metodologías y herramientas con las que realizar análisis de seguridad de aplicaciones web, aplicaciones móviles, así como realizar tareas de ingeniería inversa y hardware hacking.
TECHNICA-ENGINEERING (Vigo) Diego.Lomba@technica-engineering.de	De 1 a 3	Si	Si	Si	Desarrollo de módulos de algoritmos, que con ayuda de AI, permita encontrar incoherencias o errores en la implementación de protocolos de ciberseguridad en los componentes electrónicos integrados en los vehículos de las gamas Premium.