



Ildefonso González Sánchez

Fecha nacimiento : 27/12/1988

Madrid, España

Tel: 659109167

E-mail: fonso.gonzalezsan@gmail.com

ESTUDIOS

2022.
Madrid-España

Título: Máster en Ciberseguridad ofensiva (OSCP)
*Universidad Catolica de murcia,
campusinternacionaldeciberseguridad, T_Tech*

2019.
Madrid-España

Título: Máster en Ciberseguridad
*Universidad Camilo Jose Cela, IMF Business Madrid, Deloitte
Cybersoc*

2015.
Madrid-España

Título: Ingeniero Técnico en Informática de Sistemas
Universidad Rey Juan Carlos

Perfil con 13 años de experiencia. En la actualidad orientado a la seguridad informática a nivel:

- *Ciberseguridad ofensiva.*
- *Arquitectura de seguridad y sistemas.*
- *Desarrollo en múltiples lenguajes de programación.*
- *Sistemas operativos / servicios.*
- *Infraestructuras y redes.*
- *Gestión de incidentes / mánager de proyectos.*

EXPERIENCIA LABORAL

De 28/ 05/ 2022 a actualidad (Granada- España)
Jtsec Beyond Security / CCN, CNI
Hacker Ético y Evaluador de Productos

Desde e laboratorio, se evalúa la seguridad en productos para CCN y CNI, en certificaciones de seguridad.

Realizando test de penetración, sobre servicios web y servicios *SaaS on cloud* evaluando el nivel de seguridad, según la declaración del *standard* definido para el producto, en cuestión.

Procesos de *reversing* sobre dispositivos móviles.

Pruebas de deepfake.

Proyectos: video Identificación y aplicaciones para dispositivos Android.

De 16/ 12/ 2021 a 1/ 03/ 2022 (Madrid-Alemania)
Freelance / Univention, Sector Servicios
Consultor IT

Desarrollo de producto de seguridad, en el equipo de UCS.

Ildefonso González Sánchez

Solución de Bugs, debug y revisión de producto en python3.
UDM ,UCS, LDAP, SAMBA y conectores.

De 01/ 02/ 2021 a 15/12/2021 (Madrid-España)
ALTEN / Airbus, Sector Aeroespacial y Defensa
Lider de Equipo En Ciberseguridad

Líder de equipo de tres unidades de negocio proporcionando soluciones de Ciberseguridad para cliente final, en el área de productos de seguridad.

Las unidades de negocio, se definen en los siguientes campos:

- Análisis de software de seguridad: funciones de análisis técnico, propuestas de cambio, desarrollo de pruebas de concepto, diseño de pruebas funcionales, de regresión y unitarias en entornos de desarrollo y validación de cumplimiento adaptado a requisitos de seguridad.
- Arquitectura y análisis de riesgos: Ejecución del cargo en funciones, centrado en la evaluación, definición y diseño de arquitectura de software orientado a la creación de producto final y evolutivos.
- Análisis de vulnerabilidades: dirección de equipo y gestión de tareas asociadas y definidas en el entorno del análisis de vulnerabilidades sobre sistemas e infraestructuras en las que se despliega el producto final. Seguimiento y evolución del ciclo de vida de las vulnerabilidades, propuestas de nuevas configuraciones, cambios y parches sobre los mismos.

Generación y actualización de documentación técnica detallada para el ciclo de vida de seguridad orientada a la certificación de productos en el área de Defensa, OCCAR restricted-confidential.

De 01/ 06/ 2019 a 31/01/2021 (Madrid-España)
Sotec / Santander Tecnología, Sector Bancario
Arquitecto de Seguridad

Securización de micro-servicios estructurales a nivel desarrollo de software, en autenticación autorización: Java/Springboot.

Desarrollo de software de seguridad, orientado a criptografía, PKI, certificados, confidencialidad e integridad de acceso a la información "CIA triangle".

A nivel arquitectura, implantar y liderar proyecto de gestión de identidades corporativo: Java/Springboot.

Desarrollo de micro-servicios de administración de identidades y grupos en repositorios corporativos: Java/Springboot/Angular/relational Db.

Generación de POCs, sobre nuevas tecnologías.

Integración de código en el ALM/SDLC.

Implantación, administración y configuración de servicios en PaaS "arquitectura híbrida": Openshift, Docker, kubernetes.

Reporte de vulnerabilidades detectadas a nivel de código y sistemas.

De 01/09/2018 a 01/06/2019 (Mallorca-España)
Brújula/ Meliá Hotels International, Sector Servicios
Consultor de Ciberseguridad

Líder técnico en definición e implementación de soluciones de ciberseguridad. Management de proyectos de seguridad con partners.

Desarrollo de SIEM para entorno PCI con las siguientes tecnologías:

- Ossec, Rsyslog, Elasticsearch, Kibana, Logstash.

- Monitoring, alerting, reporting, ad-hoc.

Integración con Akamai, para proyecto de detección de anomalías on real time:

- AWS, kibana, Elasticsearch, machine learning.

Integración con Equipo de Desarrollo:

- Pentesting aplicaciones web: *melia.com.
- Pentesting aplicaciones móviles (Android): *melia.com/meliarewards.

Integración con SDLC: desarrollo de un sistema ad-hoc que realiza ataques automatizados con ZAP Proxy de OWASP mediante APIS.

- Integrado con una web J2ee, para administración.
- Integrado con Jenkins para automatización de escaneo de vulnerabilidades en el SDLC (ciclo de vida del SW en integración continua).

Integración con Equipo de Sistemas Dev-ops:

- Administración de sistemas on Cloud AWS
- Administración de redes VPCs, configuraciones, FW Shorewalls, iptables, perimetrales, hardening de sistemas

Impulso de proyectos internos, en integración continua de la seguridad, para distintos departamentos de la compañía.

De 01/03/2016 a 01/09/2018 (Madrid-España)

Cognicase Management Consulting, Sector Consultoría

Arquitecto de Sistemas

Jefatura de proyectos, dirigidos para dos divisiones diferentes dentro de la compañía.

Jefe De proyectos de nueva implantación, así como de servicio en mantenimiento/ soporte de Gestión de identidades en clientes:

- Laboratorios Normon.
- Universidad Autónoma de Madrid.
- Cepsa.

Especialización en productos suite Oracle: gestión de identidades, gestión de accesos y cuentas privilegiadas.

Gestión de proyectos, equipos, e identificación de nuevas oportunidades.

Líder técnico en implantaciones de arquitectura, definición de requisitos administración de sistemas, integración con recursos externos, desarrollo de software de seguridad para múltiples sistemas, sobre tecnología Java y o C.

IRM arquitectura, actualización de infraestructura

- Tecnologías: prot-on Cliente final: Endesa.
- Soporte IRM prot-on 12x7 APP-SEC, Endesa – Enagas.

Soporte en herramientas de seguridad:

- Tecnologías: Power Broker, deepnet. Cliente final: DISA.

Desarrollo y migración Oracle forms & reports.

De 01/03/2015 a 01/03/2016 (Madrid-España)
CORE NETWORKS, sector Consultoría
Ingeniero de SW de Seguridad y Soporte

Ingeniero de SW sobre OIM y OAM en un proyecto para Vodafone

Funciones:

- Desarrollo de SW en Java relacionado con GDI.
- Desarrollo SW ADF Framework, orientado a GDI.
- Desarrollo e implantación de workflows con SOA suite, para integración con GDI.
- Administración de servidores y repositorios de usuarios AD, LDAP.
- Administración y desarrollo de BD Oracle.

Diagnóstico de incidentes, en redes y servidores, trabajo con soporte de partners.

Soporte 24x7, guardias por turnos en productos de Oracle Identity Manager y Oracle Access Manager.

De 01/08/2014 a 01/03/2015 (Madrid-España)
Bilbomática, sector Consultoría
Desarrollador web

Desarrollador Junior Full Stack para el ministerio de Economía.

Tecnologías utilizadas JEE: Tiles, Struts, Spring, Ibatis, Javascript, JQuery, Ajax, HTML, Jasper, Bases de Datos, SVN y Tomcat.

Trabajo en equipo, bajo metodologías ágiles.

De 01/08/2014 a 01/03/2015 (Madrid-España)
Logix5, sector Docencia
Profesor de robótica educativa

De forma simultánea con el puesto anterior, profesor de robótica educativa en dos institutos privados de Madrid, a niños de entre 7 y 14 años.

De 01/12/2013 a 01/07/2014 (Madrid-España)
Universidad Rey Juan Carlos, sector Docencia
Becario en Departamento de Desarrollo de SW

Desarrollo FrontEnd: HTML, CSS, JavaScript, Ajax.

Desarrollo Backend: PHP, PL/SQL para Oracle y MySQL.

Frameworks: ZendFramework2.

Repositorios: Git Server.

Migración de sistemas: Weblogic/ NodeMnager/ Publisher 10g to 11g.

De 01/11/2011 a 01/09/2013 (Madrid-España)
GMV, Sector Servicios
Soporte Técnico Nivel 1 SOC 24x7

Soporte técnico de nivel 1 a empresas, recepción de incidentes, mediante diferentes vías, herramientas de ticketing, llamadas y/o correos electrónicos:

- Gestión del ciclo de vida de los incidentes.
- Creación, resolución y/o escalado de los mismos.
- Toma de decisiones para el procedimiento de actuación en función de la criticidad del incidente, tipo de contrato del cliente, SLA definido, así como el horario en el que el mismo se produce.

Los tipos de incidentes subdividían en los siguientes grupos. Redes o Infraestructura, Seguridad y Desarrollo.

Administración de servidores / servicios y BD.

Monitorización avanzada con Nagios y resolución proactiva de incidentes.

Generación de reportes e informes mensuales de servicio, para clientes en función de los incidentes detectados o trabajos realizados.

- Diagnóstico de incidentes con sistemas.
- Shell scripting.

Toma de decisiones y autosuficiencia, en labores de servicio 24x7 (Fines de semana turnos 12 horas, rotativos).

De 01/07/2011 a 01/08/2011 (Madrid-España)
Cepsa / HP/ Isoin, Sector Servicios
Soporte Técnico Nivel 2

Soporte técnico en administración de sistemas, siguiendo procedimientos documentados, cubriendo una baja temporal como toma de contacto con el mundo laboral, a nivel informático (45% de la carrera).

Ildefonso González Sánchez

REFERENCIAS LABORALES

<https://f0ns1.github.io/> (Recomendable)

Se adjuntan cartas de recomendación.

IDIOMAS

Español: Nativo.

Inglés: B1-B2.

FORMACIONES ADICIONALES

Certificaciones Nivel Alto: (Recomendable)

- OSCP: Offesnvie Security Certified Professional"

Certificaciones Nivel intermedio:

- Hacking con Python.
- Certificación en CSIO (Hacking ético)
- Certificación CSCE (Exploiting)

Certificaciones Nivel básico:

- Introducción al Hacking ético.
- Introducción al Hacking en redes Wi-Fi.

Linkedin: (Recomandable)

<https://www.linkedin.com/in/ildefonso-gonz%C3%A1lez-s%C3%A1nchez-0b693555/?originalSubdomain=es>

GitHub: (Recomandable)

<https://github.com/f0ns1/>

Amplia variedad de proyectos propios en Github orientados a:

- Sistemas Operativos.
 - Criptografía.
 - Software de seguridad Python/ malware y herramientas de hacking.
 - Criptografía en comunicaciones
-
- **SIEM:** Proyecto final máster en ciberseguridad.
 - **Robótica y Aplicaciones:** Proyecto final de carrera.
 - **Blogs:** asociados a mi usuario de Gmail.: <https://roadtooscp-f0ns1.blogspot.com/>
-
- Canal de twitch: https://www.twitch.tv/f0ns1_mad
 - Canal de youtube: <https://www.youtube.com/xiquifonso> (Recomendable)