# Ignacio Valverde

**ESPECIALISTA EN CIBERSEGURIDAD**

Madrid, Espana
i.valverde@gmail.com
+34 679 542 138
linkedin.com/in/ignaciovalverde

Especialista en ciberseguridad con ocho anos de experiencia protegiendo infraestructura critica y respondiendo a incidentes de seguridad en entornos corporativos. Actualmente en Repsol como responsable de deteccion y respuesta (Blue Team), gestionando la seguridad de una red con 24.000 endpoints en 14 paises. Anteriormente en el INCIBE (Instituto Nacional de Ciberseguridad) y S21sec.

## EDUCACIÓN

**Master en Ciberseguridad in Seguridad Informatica**
Universidad Politecnica de Madrid, Madrid
*Sept 2015 – Jun 2016*
TFM: *Deteccion de movimiento lateral en redes corporativas mediante analisis de trafico con machine learning*. Nota: 9,0/10.

**Grado en Ingenieria Informatica in Computacion**
Universidad de Leon, Leon
*Sept 2011 – Jun 2015*
Nota media: 7,7/10.

## HABILIDADES

- SIEM (Splunk, QRadar)
- SOAR (Cortex XSOAR, Phantom)
- EDR (CrowdStrike, Carbon Black)
- MITRE ATT&CK Framework
- Analisis forense digital
- Threat Intelligence
- Python (scripting de seguridad)
- Networking avanzado (Wireshark, tcpdump)
- ISO 27001 / ENS
- Gestion de vulnerabilidades (Qualys, Nessus)

## CERTIFICACIONES

**CISSP (Certified Information Systems Security Professional)**
(ISC)2
*May 2022 – May 2025*

**GIAC Certified Incident Handler (GCIH)**
SANS Institute
*Mar 2020 – Mar 2024*

**CEH (Certified Ethical Hacker)**
EC-Council
*Nov 2018*

## IDIOMAS

- Espanol (nativo)
- Ingles (C1 Advanced)

## REFERENCIAS

**Fernando Urdiales**
CISO, Repsol
f.urdiales@repsol.com, +34 608 712 493

**Marta Ballesteros**
Coordinadora CERT, INCIBE
m.ballesteros@incibe.es, +34 663 284 501

## EXPERIENCIA

**Senior Cybersecurity Analyst - Blue Team Lead**, Repsol, Madrid *Mar 2021 – Presente*
Lider del equipo de deteccion y respuesta a incidentes (Blue Team) del SOC corporativo de Repsol.

- Dirijo un equipo de **6 analistas** que monitorizan la seguridad de 24.000 endpoints en 14 paises
- Gestionse la respuesta a **3 incidentes criticos** en 2024 (ransomware intento, compromiso de credenciales VIP, ataque a cadena de suministro) sin impacto en operaciones
- Implemente deteccion basada en **MITRE ATT&CK** con 340 reglas de correlacion en Splunk, aumentando la tasa de deteccion un **47%**
- Reduje el tiempo medio de respuesta a incidentes de **4,2 horas a 38 minutos** mediante automatizacion con SOAR (Cortex XSOAR)

**Analista de Ciberseguridad**, INCIBE, Leon *Sept 2018 – Feb 2021*
Instituto Nacional de Ciberseguridad. Equipo de respuesta a incidentes (CERT) para empresas y ciudadanos.

- Gestionse **420+ incidentes de seguridad** anuales incluyendo phishing masivo, ransomware y fraude del CEO
- Desarrolle **12 alertas tecnicas** publicadas en la web del INCIBE sobre vulnerabilidades criticas
- Coordine la respuesta a la campana de ransomware **Emotet** que afecto a 180 empresas espanolas en 2020

**Junior Security Analyst**, S21sec, Madrid *Ene 2017 – Ago 2018*
Empresa de servicios de ciberseguridad. Analista SOC en turno rotativo 24×7.

- Monitorizacion y triaje de alertas de seguridad para **8 clientes** del sector financiero y energia
- Analice **15.000+ alertas mensuales** con QRadar y Splunk, escalando un promedio de 34 incidentes reales

## PROYECTOS

**Implantacion SOAR - Repsol** *Jun 2022 – Mar 2023*
Implantacion de la plataforma de orquestacion y respuesta automatizada Cortex XSOAR.

- Automatizacion de **23 playbooks** de respuesta a incidentes (phishing, malware, credenciales comprometidas)
- Reduccion del MTTR de **4,2 horas a 38 minutos**
- Integracion con Splunk, CrowdStrike, VirusTotal y **Active Directory**

**Deteccion MITRE ATT&CK - Repsol** *Sept 2021 – May 2022*
Mapeo de capacidades de deteccion al framework MITRE ATT&CK y cierre de gaps.

- Auditoria de cobertura: de **34% a 78%** de las tecnicas relevantes para el sector energia
- Creacion de **340 reglas de correlacion** en Splunk alineadas con tecnicas ATT&CK

## ACTIVIDADES EXTRACURRICULARES

**Ponente - RootedCON Madrid** *Mar 2023 – Mar 2023*
Charla 'Automatizando la respuesta a incidentes en infraestructura critica' en RootedCON 2023, la mayor conferencia de ciberseguridad de Espana, con 2.500 asistentes.

**Jugador CTF - Equipo H-c0n** *Ene 2019*
Miembro del equipo espanol de Capture The Flag. Top 15 en el CTF europeo de ENISA 2024. Especialidad: forense digital y analisis de malware.