

EDWIN GUAJALA

Especialista en Seguridad de Redes y Ciberseguridad

Quito, Ecuador | edwinguajala3@gmail.com | 0983513119 | linkedin.com/in/e-guajala-cybersec4you | www.cybersec4you.net

PERFIL PROFESIONAL

Ingeniero en Electrónica y Computación con Maestría en Seguridad Telemática con experiencia en redes y seguridad perimetral en entornos críticos (ECU 911, SRI). Experiencia en segmentación y segregación de redes, administración y optimización de políticas de firewall (Check Point, FortiGate), IPS TippingPoint, WAF F5, AntiDDoS F5 y Proxy Symantec, además de correlación de eventos y respuesta a incidentes. Automatizo el análisis de indicadores de compromiso con Python y APIs de inteligencia de amenazas. Busco aportar en el gobierno de seguridad de red y sigo ampliando mi conocimiento en gestión de políticas con AlgoSec y en seguridad de redes de telecomunicaciones.

EXPERIENCIA PROFESIONAL

Servicio de Rentas Internas (SRI)

Abril 2026 – Presente

Seguridad de redes e infraestructura

- Optimización de reglas en firewall Check Point; gestión de reglas internas, NAT y accesos VPN para entidades externas que consumen servicios del SRI, bajo criterio de mínimo privilegio.
- Administración del IPS TippingPoint, WAF F5 y AntiDDoS F5; gestión de certificados digitales de los servicios expuestos a internet y su aplicación en IPS y AntiDDoS.
- Threat hunting proactivo: correlación de logs de firewall (Threat Prevention), proxy, antivirus y DLP para detectar actividad anómala; identificación de equipos comprometido con comunicación C&C, aislado y sanitizado. Búsqueda de IOC provenientes de reportes de CSIRT gubernamentales y análisis automatizado de IPs sospechosas con Python (VirusTotal, AbuseIPDB, GreyNoise). Análisis de reportes de bloqueos sospechosos de cuentas de contribuyentes.
- Implementación y administración de WSUS para la gestión de parches críticos y de seguridad en Windows.
- Administración del Sistema de Gestión de Identidades - IBM: Asignación y revocación de accesos, análisis de flujos entre sus componentes (AD, Mesa de Servicio, BD).

Servicio Integrado de Seguridad ECU 911

Abril 2013 – Abril 2026

Redes y seguridad perimetral

- Segmentación de red de una operación de misión crítica sobre firewall FortiGate y H3C, separando la red administrativa, la red cableada, la red inalámbrica y los accesos de instituciones articuladas, para limitar el movimiento lateral y proteger los activos críticos.
- Definir políticas de conectividad para instituciones externas articuladas, restringiendo el acceso a lo estrictamente necesario (mínimo privilegio).
- Migración de un firewall Mikrotik a FortiGate, adaptándolo a la red troncal H3C existente.
- Administración de equipos de networking H3C y Mikrotik, y de la seguridad perimetral: firewalls, UTM, IPS, anti-DDoS, VPN (OpenVPN) y endpoints (Kaspersky).
- Administración del acceso a Internet de los usuarios mediante reglas y perfiles de seguridad (Control de aplicaciones, filtrado web, antivirus e inspección de contenido).
- Diseñar y administración de proyectos de redes, ciberseguridad y videovigilancia; administración de servidores Linux y Windows.

Schlumberger

Noviembre 2011 – Abril 2013

Soporte e infraestructura de TI

- Instalación y administración de equipos de networking, Active Directory, impresoras y soporte en sitio.

Telconet S.A.

Febrero 2011 – Noviembre 2011

Operador de telecomunicaciones

- Instalación y configuración de equipos de networking, enlaces inalámbricos y fibra óptica; soporte técnico a usuarios corporativos.

COMPETENCIAS TÉCNICAS

Seguridad de redes: Check Point, FortiGate, H3C, Mikrotik, IPS (TippingPoint), AntiDDoS (F5), WAF (F5), Proxy Symantec ProxySG, VPN, NAT, análisis y optimización de reglas de firewall

Networking: TCP/IP, DNS, routing y switching, VLANs, VPN, NAT, segmentación y segregación de redes; OSPF y BGP (Cisco, entornos de laboratorio)

Gobierno y accesos: Mínimo privilegio, gestión de identidades y accesos, certificados digitales

Amenazas y vulnerabilidades: Correlación de eventos, IOC, threat hunting, gestión de vulnerabilidades, automatización con Python y APIs (VirusTotal, AbuseIPDB, GreyNoise)

Sistemas: Windows Server, Linux, WSUS, Kaspersky, Symantec

En desarrollo: AlgoSec, MITRE ATT&CK, SS7 / Diameter y seguridad en redes móviles 4G/5G

FORMACIÓN

- **Maestría en Seguridad Telemática**, ESPOCH (2014 – 2018). Investigación: método para la detección de ataques web mediante la parametrización de un proxy reverso basado en software libre.
- **Ingeniería en Electrónica y Computación**, ESPOCH (2002 – 2010). Tesis: estudio comparativo entre sistemas VPN (OpenVPN, OpenSWAN, PopTop).

CURSOS Y CERTIFICACIONES

- IBM Cybersecurity Certificate: Governance, Risk, Compliance and Data Privacy; Vulnerability Management; System and Network Security; Cloud Security; SOC, IR and System Forensics.
- Preparación CIH (Certified Incident Handler), ECForensics. CCNA Exploration, Cisco.
- Fortinet 7.x, Ciberseguridad Defensiva, LPI Security Essentials (Udemy). Criptografía y Ciberseguridad para Gerentes y Directivos (Platzi).
- IBM Linux System Administration.

IDIOMAS

Español: nativo | Inglés: B1 (B2 en proceso)