Yan Carlos Leon Trigos

Ingeniero de Sistemas – 091122-0745056 CNDC

Bogotá, Colombia
juan_12086@hotmail.com
Tel: +57 350 642 7231

Gestión de vulnerabilidades, hardening, ciberinteligencia y auditoría continua

Perfil Profesional

Ingeniero de Sistemas con enfoque especializado en **Ciberseguridad** y **Gestión de Servicios de TI**, con experiencia comprobada en la protección de infraestructuras críticas, gestión de vulnerabilidades, hardening de sistemas y cumplimiento normativo (ISO 27001, CIS Benchmarks). Me motiva la adopción de tecnologías innovadoras que fortalezcan la comunicación, mejoren la colaboración y optimicen la gestión de la información. Trabajo orientado a la excelencia, la eficiencia operativa y la mejora continua, cuidando la precisión en la comunicación escrita y promoviendo prácticas sostenibles.

Formación Académica

2026 **ESPECIALIZACION EN CIBERSEGURIDAD**, *CUN*, Colombia, en formación

2023 **Ingeniería de Sistemas**, *CUN – Corporación Unificada Nacional de Educación Superior*, Colombia
Matrícula: 091122-0745056 CNDC

2017 **Tecnólogo en Análisis y Desarrollo de Sistemas de la Información**, *SENA*, Colombia
Matrícula: 54967-062666

2014 **Técnico en Mantenimiento de Equipos de Cómputo**, *SENA*, Colombia

Certificaciones

PeopleCert	ITIL Foundation Certificate in IT Service Management
Microsoft	Azure Fundamentals (AZ-900)
Platzi	Certificación en Seguridad Informática
Google Cloud	Cloud Digital Leader

Cursos Relevantes

Tenable	Vulnerability Exposure
Tenable	Engineer Cloud Security
Qualys	Vulnerability Management Detection and Response Certification (VMDR)
Qualys	CyberSecurity Asset Management (CSAM)
SENA	Introducción a la Ciberseguridad
MinTIC	AWS Cloud Practitioner Essentials
Platzi	Inteligencia para la Ciberseguridad
Platzi	Administración de Servidores Linux
Platzi	Curso Profesional de Git y GitHub
Platzi	Serverless Framework en AWS
Platzi	Análisis de Malware para Dispositivos Móviles

Udemy Curso Avanzado en Power BI

Udemy Curso de Preparación para la Certificación en la Norma ISO

Experiencia Laboral

Ene. 2026 – Actualidad **Especialista de Ciberseguridad Senior**, *WEXLER SAS*, Bogotá, Colombia

- Liderazgo técnico en la gestión integral de vulnerabilidades sobre infraestructura, aplicaciones y entornos híbridos (*On-Premise y Cloud*), ejecutando evaluaciones periódicas y análisis de exposición al riesgo.
- Análisis, validación y priorización de vulnerabilidades utilizando métricas como **CVSS**, **EPSS** y contexto operacional para definir estrategias de remediación basadas en riesgo.
- Elaboración de reportes técnicos y ejecutivos con indicadores de riesgo, tendencias, cumplimiento y seguimiento de planes de remediación.
- Coordinación con equipos de infraestructura, desarrollo y operaciones para la corrección de vulnerabilidades y validación de la efectividad de las remediaciones implementadas.
- Administración y mantenimiento del inventario de activos tecnológicos evaluados dentro del programa de gestión de vulnerabilidades.
- Diseño, implementación y mantenimiento de políticas de **Hardening** para sistemas Windows, Linux, bases de datos, dispositivos de red, contenedores y plataformas Cloud.
- Evaluación continua del cumplimiento de configuraciones seguras mediante estándares como **CIS Benchmarks**, **NIST**, **ISO/IEC 27001** y **DISA STIG**.
- Fortalecimiento de configuraciones de servicios críticos (**SSH, RDP, TLS, permisos, autenticación y registros de auditoría**) para reducir la superficie de ataque.
- Coordinación de procesos de **Patch Management**, análisis de boletines de seguridad y evaluación del impacto de vulnerabilidades (**CVE**) sobre los activos corporativos.
- Desarrollo e implementación de automatizaciones mediante scripts y herramientas para la ejecución de escaneos, validaciones de hardening y generación de reportes técnicos.
- Participación en auditorías internas y externas, proporcionando evidencias técnicas y apoyando iniciativas de cumplimiento de marcos como **ISO 27001**, **PCI DSS** y **SOC 2**.
- Revisión de arquitecturas tecnológicas desde la perspectiva de ciberseguridad, proponiendo controles preventivos y mejores prácticas de configuración segura.
- Capacitación y acompañamiento a equipos técnicos sobre gestión de vulnerabilidades, hardening y buenas prácticas de seguridad informática.
- Monitoreo continuo de amenazas emergentes, exploits y tendencias de ataque para evaluar su impacto sobre el entorno corporativo y definir acciones preventivas.
- Todas las actividades son ejecutadas bajo el enfoque del **NIST Cybersecurity Framework (Identify, Protect, Detect, Respond y Recover)**, fortaleciendo la postura de seguridad y la resiliencia organizacional.
- **Controles aplicados ISO 27001:** A.8.8 "Gestión de vulnerabilidades técnicas", A.8.9 "Gestión de la configuración", A.5.24 "Planificación y preparación para incidentes", A.5.31 "Cumplimiento de requisitos legales y regulatorios".

Oct. 2022 – Ene. 2026 **Especialista en Seguridad Informática 2**, *SONDA de Colombia*, Bogotá, Colombia
Contacto: Autopista Nte. #118–68, Bogotá **Tel.:** +57 601 646 6565

- Liderazgo técnico en la identificación, análisis y gestión de vulnerabilidades en infraestructura, sistemas y aplicaciones, utilizando **Tenable, Qualys y Rapid7**.
- Coordinación con equipos de desarrollo, infraestructura y proveedores para definir, implementar y dar seguimiento a planes de remediación.
- Análisis de riesgo y priorización de vulnerabilidades según impacto en el negocio, criticidad técnica y contexto operativo.
- Supervisión y optimización del proceso de gestión de vulnerabilidades, asegurando cumplimiento de políticas y buenas prácticas (**ISO 27001**).
- Apoyo en iniciativas de arquitectura segura y desarrollo seguro; capacitación en prácticas seguras de codificación.
- Integración con plataformas **SIEM y EDR** (*IBM QRadar, SentinelOne*) para correlación de eventos y respuesta temprana a incidentes.
- Monitoreo de amenazas y tendencias de ciberseguridad; propuesta de controles preventivos, correctivos y de mejora continua.
- Gestión de proveedores y servicios de ciberseguridad relacionados con remediación y escaneo de vulnerabilidades.
- Participación en auditorías internas/externas; elaboración de reportes ejecutivos y contribución al **SGSI**.
- Planeación, administración y evaluación periódica de procesos de seguridad de la información y cumplimiento normativo.
- **Hardening** de sistemas operativos y equipos cliente con lineamientos técnicos y buenas prácticas.
- Revisión, ajuste y reforzamiento de configuraciones en Windows y Linux: servicios, puertos, políticas locales, control de privilegios y desactivación de funciones innecesarias.
- Validación del cumplimiento de estándares (**ISO 27001, CIS Benchmarks**) para operación segura en ambientes productivos.
- Todas estas actividades se ejecutan alineadas a las 5 funciones del NIST CSF **(Identify, Protect, Detect, Respond y Recover)** para garantizar una gestión integral y continua de la ciberseguridad en la organización.
- **Controles aplicados ISO 27001** A.8.8 "Gestión de vulnerabilidades técnicas" A.5.25 "Detección y respuesta ante incidentes" A.5.24 "Planificación de la seguridad de la información" A.5.31 "Revisión de seguridad de la información"

May. 2022 – Oct. 2022 **Técnico en Seguridad Informática**, *Infotrans Colombia*, Bogotá, Colombia
Contacto: Cra 50 #114–17, Bogotá **Tel.:** +57 601 743 3281

- Gestión de calidad de imágenes (masterización) de sistemas operativos antes del despliegue a producción.
- Escaneos de vulnerabilidades con **Tenable/Nessus** y análisis de resultados para escalación o remediación.
- Administración y monitoreo de consolas antivirus corporativas; actualización de firmas y protección de endpoints.
- Aplicación de lineamientos de **hardening** en equipos de usuario final, basados en buenas prácticas y estándares institucionales.
- Configuración e implementación de mecanismos de autenticación **2FA/MFA** en plataformas corporativas.
- Generación de reportes técnicos y de cumplimiento desde plataformas de MFA y antivirus, para control y auditoría.
- Apoyo en estrategias de protección de archivos, cifrado y aseguramiento de endpoints.
- Validación de cumplimiento de **ISO 27001** y **CIS Benchmarks** en entornos productivos.

Nov. 2017 – Abr. 2022 **Técnico de Soporte Nivel 2**, *Secretaría de Educación – Proyecto REDP*, Bogotá, Colombia
COMWARE – Cra. 13 No. 97–98, Bogotá **Tel.:** (57) 1 6382100
SELCOMP Ingeniería SAS – – Av. Carrera 28 No. 35–40, Bogotá **Tel.:** (1) 338 2828
UT ADMINISTRATIC 2021 – – Av. Carrera 28 No. 35–40, Bogotá **Tel.:** (1) 338 2828
Soluciones TI PS–GD – – Carrera 12 #96–81 Piso 6, Edificio Parque 96, Bogotá **Cel.:** 3185605017 – 3164485237

Funciones

- Atención y gestión de incidentes y requerimientos por canales (teléfono, web, chat, correo) conforme a ANS.
- Soporte tecnológico a usuarios; mantenimiento preventivo y correctivo de equipos.
- Ejecución de respaldos y *backups* periódicos de información.
- Configuración de redes LAN y soporte a redes inalámbricas de larga distancia.
- Gestión de mantenimiento de infraestructura tecnológica.
- Documentación de casos en mesa de ayuda; escalamiento según protocolos.
- Elaboración de manuales de instalación, configuración de aplicativos y procedimientos.
- Diagnóstico de problemas con base en información del primer nivel de soporte.
- Aplicación de políticas de seguridad en la configuración de equipos.
- Mantenimiento y actualización de la base de conocimiento.
- Participación en planes de mejora y actividades internas alineadas con el cargo.

May. 2016 – Dic. 2016 **Tecnólogo en Desarrollo de Software**, *Masanty S.A*, Cúcuta, Colombia
Contacto: Av. 2E #11–36 L.09, Cúcuta **Tel.:** +57 575 6686

- Apoyo al equipo de desarrollo en tareas de codificación, diseño y mantenimiento de software.
- Programación desde cero y mantenimiento de código para optimizar rendimiento.
- Identificación y resolución de errores mediante pruebas y análisis de funcionamiento.
- Atención a solicitudes técnicas del equipo de desarrollo y retroalimentación de usuarios.
- Interacción con clientes para evaluar experiencia de usuario y recopilar mejoras.
- Pruebas funcionales de software para asegurar calidad y estabilidad antes de su liberación.
- Elaboración de documentación técnica.

Conocimientos Técnicos

Ciberseguridad	Gestión de vulnerabilidades, remediación, hardening, ISO 27001.
Redes	LAN, WiFi empresariales, Ubiquiti MAN.
Virtualización	VMware vSphere/vCenter, Veeam.
Colaboración	Google Workspace, Microsoft 365, Teams.
Bases de Datos	MySQL, PostgreSQL, SQL Server, Access.
Ofimática	MS Office, Power BI, iWork.

Intereses

Ciberseguridad avanzada, certificaciones internacionales, inglés B1.

Referencias

Duván José Botello	Senior Software Engineer	Cel.: 318 495 2544
Samuel Pérez Ascanio	Ingeniero de soporte	Cel.: 320 850 9760