

Cristian Salazar

Cyber Security Engineer
✉cristian.salazar@outlook.com +57 310 262 2612 Bogotá, Colombia
https://www.linkedin.com/in/cristian-salazar88

Perfil profesional

Ingeniero de Sistemas, especialista en Seguridad Informática, con más de 6 años en ciberseguridad en entornos corporativos regulados (financiero, Software Factory y e-commerce). Experiencia en gestión de incidentes (detección, contención, erradicación y recuperación), monitoreo en SIEM, ciberinteligencia y monitoreo de superficie de ataque, gestión de vulnerabilidades e IAM. Diseño e implementación de controles de seguridad bajo ISO 27001 y NIST CSF, con automatización tipo SOAR mediante scripting, n8n e inteligencia artificial.

Habilidades

Operaciones de seguridad
SIEM, SOC, SOAR, Gestión de incidentes, Threat Hunting (cacería de amenazas), MITRE ATT&CK, Ciberinteligencia

Identidades y accesos
IAM, IGA, RBAC / ABAC, SoD, Revisión de accesos, Zero Trust

Riesgo y cumplimiento
Gestión de vulnerabilidades, Controles de seguridad, Security by design, ISO 27001, NIST CSF, ISO 22301, DLP

Habilidades interpersonales
Pensamiento analítico, Resolución de problemas, Comunicación con áreas de negocio

Herramientas

Wazuh (SIEM) / FortiSIEM (SIEM) / Microsoft Defender for Endpoint (EDR) / Microsoft Entra ID / Okta / CyberArk / SOCRadar (Ciberinteligencia) / Axur (Protección de marca) / Nessus / OpenVAS / Acunetix (Vulnerabilidades) / Safetica (DLP) / Google Workspace Admin / Slack Admin / Atlassian Admin / 1Password Admin / n8n / Power Automate / Zapier (Automatización SOAR) / Power BI / Looker

IA: Claude Code / Gemini CLI / Google Antigravity / MCP / Agentes de IA

Experiencia

MercadoLibre Cyber Security Engineer (Bogotá - Colombia) junio de 2023 – febrero de 2026

- **Estandarización de Identidades (IAM):** Lideré la estandarización de procesos IAM y del modelo de roles y perfilamiento de accesos (RBAC, ABAC, SoD), definiendo matrices por función de negocio bajo los principios de Zero Trust y menor privilegio.
- **Gobernanza y Procesos AMBR:** Dirigí proyectos estratégicos de **Gobernanza de Identidades (IGA)**, incluyendo la ejecución de procesos **AMBR (Access Management Business Review)** y la integración técnica de nuevos sistemas bajo controles robustos de acceso.
- **Gestión de Certificados:** Responsable de la gestión integral del ciclo de vida de **certificados digitales (Soluti, DigiCert, VISA, Mastercard)**, garantizando la continuidad operativa y la seguridad en las comunicaciones de los servicios críticos.
- **Seguridad en Ecosistemas SaaS:** Administré la postura de seguridad y políticas de acceso en plataformas colaborativas (**Google Workspace, Slack, Atlassian**), mitigando riesgos de fuga de datos y accesos no autorizados.
- **Gestión de incidentes:** Gestioné incidentes de ciberseguridad asociados a identidades y accesos: detección, análisis, contención y recuperación ante accesos no autorizados.
- **Controles de seguridad (security by design):** Diseñé e implementé controles de seguridad sobre identidad, nube y aplicaciones SaaS en la integración de nuevos sistemas.
- **Eficiencia y Automatización (SOAR):** Automaticé procesos de respuesta y operación de seguridad con n8n, Power Automate, scripting y agentes de IA (Claude Code, MCP), eliminando errores manuales en aprovisionamiento masivo y reduciendo tiempos de respuesta.

Sophos Solutions - GFT Technologies (Bogotá - Colombia) febrero de 2020 – junio de 2023
Cybersecurity Senior Analyst marzo de 2022 – junio de 2023

- **Implementación y evaluación de controles:** Lideré la implementación de controles de seguridad y auditorías internas basadas en **ISO 27001/27002** y **NIST Cybersecurity Framework**, evaluando su efectividad y asegurando el cumplimiento normativo.
- **SIEM y SOC:** Monitoreo y correlación de eventos de seguridad en **SIEM (Wazuh, FortiSIEM)** y **Microsoft Defender for Endpoint**, con escalamiento, respuesta a incidentes y elaboración de playbooks de respuesta.
- **Cacería de amenazas (threat hunting):** Búsqueda proactiva de amenazas basada en **MITRE ATT&CK** sobre eventos de endpoint y SIEM.
- **Ciberinteligencia:** Monitoreo de superficie de ataque con **SOCRadar**: identificación de exposición de marca, credenciales filtradas y amenazas externas.
- **Gestión de vulnerabilidades:** Ciclo completo con **Nessus, OpenVAS y Acunetix**: identificación, priorización por CVSS, seguimiento de remediación y validación.
- **Seguridad en la Nube y DLP:** Administré el ecosistema de **Microsoft Security** (Defender for Endpoint, Azure Security) y estrategias de **DLP** para la protección de la marca y activos críticos en la nube.
- **Continuidad del Negocio:** Desarrollé y mantuve procesos de **Continuidad del Negocio (ISO 22301)**, coordinando la respuesta técnica ante incidentes para garantizar la resiliencia operativa.
- **Concientización:** Lideré campañas de **Ingeniería Social** para fortalecer la cultura de seguridad.

Analista de Seguridad de la Información febrero de 2020 – marzo de 2022

- **Mitigación de Riesgos:** Identifiqué y mitigué riesgos en activos de información mediante el desarrollo de políticas de seguridad y normas técnicas orientadas a reducir debilidades en la plataforma tecnológica.
- **Respuesta a Incidentes:** Operé como primer nivel de respuesta ante incidentes de seguridad, aplicando protocolos de contención y los estándares de protección de la organización.
- **Aseguramiento de Procesos:** Implementé y mantuve procesos de seguridad enfocados en la integridad de los activos tecnológicos y el cumplimiento de las normas de seguridad de la información.

Redeban Técnico de Producción (Bogotá - Colombia) diciembre de 2019 – febrero de 2020

- Monitoreo de microservicios críticos y gestión de flujos transaccionales para la alianza DaviPlata-Rappi.

Ministerio de Hacienda y Crédito Público - Comware Ingeniero de Soporte (Bogotá - Colombia)
septiembre de 2015 – septiembre de 2019

- Gestión técnica de incidentes (SLA), mantenimiento de infraestructura y administración de CMDB.

Educación

Universidad Piloto de Colombia Gestión de Seguridad Informática (Diplomado) 2013
Universidad Piloto de Colombia Seguridad Informática (Especialización) 2012 – 2013
Corporación Unificada Nacional CUN Ingeniería de Sistemas (Pregrado) 2006 – 2012

Certificaciones

Gestión de incidentes e Informática Forense 2023
Lead Cybersecurity Professional Certificate (LCSPC) 2022
CertiProf
Auditor Interno ISO 22301: Continuidad de Negocio 2021
SGS
Apple Certified Macintosh Technician (ACMT) 2019
Apple
Microsoft Windows Server MCSA 70-740, 70-741 2018
Microsoft
Auditor Interno ISO 27001: Seguridad de la Información 2016
SGS Colombia