



Anderson Pinheiro Aderaldo

Ingeniero Sênior de Ciberseguridad

Río de Janeiro, Brasil · Ciudadano  brasileño y de la  UE

 andersonaderaldo@gmail.com

 linkedin.com/in/andersonaderaldo

 Trabajo en remoto

Ingeniero Sênior de Ciberseguridad con 15 años protegiendo telecomunicaciones, fintech y comercio electrónico a escala nacional. Construyo programas de seguridad desde cero — SOC, DFIR, seguridad en la nube, Zero Trust y DevSecOps — y los opero en producción.

15

años en ciberseguridad

2

programas creados desde
cero: SOC y DevSecOps

ISO 27001

recertificación sostenida

2018–2020

elecciones brasileñas y
Rock in Rio 2019
protegidos

EXPERIENCIA



Senior Security Engineer

VTEX

oct. 2026 - actualidad · Brasil

Plataforma global de comercio composable, cotizada en la NYSE.

Miembro del equipo de Cloud Security, protegiendo la infraestructura en la nube detrás de la plataforma de comercio digital de VTEX.

- **Gestión de la postura en la nube:** monitoreo de las cuentas en la nube en busca de configuraciones incorrectas y seguimiento de la corrección con los equipos responsables.
- **Protección de cargas de trabajo:** seguridad de contenedores, hosts y servicios gestionados, incluida la gestión de vulnerabilidades de imágenes y servidores.
- **Identidad y acceso:** revisión de roles y permisos en la nube y aplicación del mínimo privilegio.
- **Guardrails de seguridad:** definición de baselines seguras y revisión de la infraestructura como código antes de llegar a producción.
- **Detección y respuesta:** mantenimiento de los registros y alertas en la nube, e investigación y respuesta a incidentes de seguridad en la nube.
- **Colaboración con ingeniería:** asesoría a los equipos de producto y plataforma sobre arquitectura segura en la nube.



Especialista en Seguridad de la Información

mar. 2025 - ago. 2026 (1 año y 6 meses) · Río de Janeiro, Brasil

Juntos Somos Mais

Marketplace B2B y plataforma de fidelización para el comercio minorista de materiales de construcción, creada por Votorantim Cimentos, Gerdau y Tigre.

Responsable de la ciberresiliencia y de la gobernanza de seguridad de la infraestructura, protegiendo activos críticos y difundiendo la cultura de seguridad con un enfoque consultivo y técnico.

- **Cloud Security y DevSecOps:** implementación de estrategias de CSPM y CWPP con Orca Security. SCA (Software Composition Analysis) y gestión de parches de código y servidores en la nube, con security gates integrados en el pipeline de CI/CD.
- **Seguridad perimetral y de aplicaciones:** administración y ajuste de las capas de protección de Akamai (WAF, Bot Manager y CDN). Implementación de ZTNA (Zero Trust Network Access) con Netskope.
- **Gestión de vulnerabilidades y endpoints:** ciclo de vida de vulnerabilidades en estaciones de trabajo con ManageEngine y monitoreo de amenazas avanzadas con Trend Micro Vision One (XDR).
- **Gobernanza, Riesgo y Cumplimiento (GRC):** sostenimiento del SGSI para la recertificación ISO 27001; redacción de normas de seguridad y políticas corporativas.
- **Monitoreo y respuesta a incidentes:** implementación y gestión de Elastic SIEM. Threat intelligence con Axur para protección de marca y mitigación de riesgos externos.
- **Cultura de seguridad:** programa de concienciación y simulaciones de phishing en KnowBe4.



Ingeniero de Seguridad

dic. 2020 - jun. 2024 (3 años y 7 meses) · Río de Janeiro, Brasil

Ame Digital

Billetera digital y fintech del grupo Americanas.

SOC, Blue Team, threat hunting e inteligencia de seguridad

- Implantación del Security Operations Center (SOC) desde cero: soluciones de seguridad, documentación de procesos y procedimientos base, recolectores de logs y alertas de seguridad, y posterior traspaso al equipo de operaciones.
- Apoyo directo al Blue Team en la mejora de las defensas y la implementación de soluciones de seguridad.
- Competencias desarrolladas: gestión y seguridad en la nube, CSPM, CWPP, antivirus de nueva generación (NGAV), SIEM/SOAR, seguridad perimetral, Zero Trust, threat intelligence de fuentes abiertas y threat hunting.

Seguridad de aplicaciones, DevSecOps y automatización

- Implementación de DevSecOps desde cero con un pipeline seguro en GitHub Actions.
- Desarrollo e implementación de pruebas de SCA, SAST, DAST, detección de secretos, IaC y seguridad de contenedores.
- Documentación de las herramientas de seguridad y formación de todos los desarrolladores en su uso y en la corrección de las vulnerabilidades encontradas.
- Competencias desarrolladas: seguridad en DevOps, arquitectura segura, desarrollo de automatizaciones y definición de estándares de seguridad.



Oi S.A.

nov. 2011 - nov. 2020 (9 años y 1 mes) · Río de Janeiro, Brasil

Uno de los mayores operadores de telecomunicaciones de Brasil: telefonía fija, móvil, banda ancha y datos corporativos.

Especialista en Ciberseguridad (líder de equipo) · mar. 2019 - nov. 2020

Analista de Seguridad de la Información, SOC y DFIR · jul. 2013 - feb. 2019

Becario de Seguridad de la Información · nov. 2011 - jun. 2013

Especialista en Ciberseguridad · mar. 2019 - nov. 2020

Líder del equipo de seguridad de la infraestructura de TI, coordinando proyectos de protección perimetral, seguridad de sistemas operativos, dispositivos de red, bases de datos e infraestructura web, y arquitectura segura de nube híbrida.

- Gestión de proyectos de seguridad e infraestructura.
- Hardening de Windows y Linux, dispositivos de red (routers y switches) y bases de datos (Oracle, SQL Server, MongoDB).
- Análisis y tratamiento de reglas de firewall con Tufin SecureTrack.
- Planificación de la gestión de políticas de seguridad de Cisco WSA y Cisco ESA (control de contenido).
- Planificación de la protección de DNS con Cisco Umbrella.
- Planificación de la solución anti-DDoS con NETSCOUT AED, antes Arbor Networks Pravail (APS).
- Evaluación de la seguridad de la infraestructura con Nessus y shodan.io.
- Definición de baselines de seguridad para activos de telecomunicaciones.
- Análisis y protección de la arquitectura de red y de la nube híbrida desde la perspectiva de seguridad.
- Gestión de amenazas y vulnerabilidades con RSA Archer.
- Servicios gestionados de seguridad en eventos patrocinados (protección perimetral con firewall L7, control de contenido, anti-DDoS, hardening, monitoreo y seguridad de DNS) para proteger la infraestructura de los eventos contra ciberataques.

Eventos patrocinados protegidos: Game XP (2017, 2018, 2019), Rio2C (2018, 2019), Comic Con Experience (2018, 2019), Rock in Rio 2019 y las Elecciones Generales de Brasil (2018, 2020).

Analista de Seguridad de la Información · jul. 2013 - feb. 2019

Actuación en los equipos internos de Security Operations Center (SOC) y de Digital Forensics and Incident Response (DFIR).

Security Operations Center (SOC)

- Creación y revisión de procedimientos operativos para el tratamiento de incidentes de seguridad (L1 y L2).
- Proyectos de mejora de la infraestructura de recolección de logs y de los sistemas de alarmas.
- Soporte operativo y creación de alarmas de seguridad.

- Detección y neutralización de amenazas de virus y ransomware.
- Facilitación de la adopción de nuevos procedimientos por el equipo de operaciones.
- Análisis de incidentes en NetIQ Sentinel SIEM y ArcSight SIEM y creación de alarmas de correlación.
- Control del cumplimiento de reglas de firewall con Tufin SecureTrack.
- Operación del antivirus Broadcom SEP contra virus, spyware y ransomware.
- Atención de tickets L2 y L3 de seguridad de la información (reglas de firewall, control de contenido).

Digital Forensics and Incident Response (DFIR)

- Análisis y resolución de incidentes de seguridad de la información L3.
- Tratamiento de casos de fraude tecnológico basados en la seguridad del negocio.
- Redacción de procedimientos operativos internos.
- Adquisición de imágenes de disco con Tableau TD3 e Image MASster Solo-5.
- Peritaje forense de dispositivos móviles con Cellebrite UFED.
- Peritaje forense de computadoras con EnCase y Autopsy.
- Monitoreo de actividades sospechosas de empleados con Veriato Investigator.
- Monitoreo de amenazas en el entorno con RSA NetWitness.
- Búsqueda de posibles nuevos incidentes en bases de datos, sistemas operativos, activos de red y sistemas críticos.
- Investigación de violaciones de seguridad y apoyo a la empresa en los asuntos disciplinarios y legales relacionados.
- Apertura de salas de crisis y creación de planes de acción ante amenazas graves.

Becario de Seguridad de la Información · nov. 2011 - jun. 2013

Becario en el equipo de seguridad de la información, en la prevención de seguridad de TI.

- Atención de tickets L1 (firewall, control de contenido, antivirus).
- Organización de las actividades del equipo y consolidación de presentaciones de resultados.
- Notificación a los responsables de activos cuando se detectaban nuevas vulnerabilidades.
- Gestión de pequeños proyectos de seguridad.



Asistente de Servicios Corporativos

may. 2008 - oct. 2011 (3 años y 6 meses) · Río de Janeiro, Brasil

Contax S.A.

Empresa de contact center y tercerización de atención al cliente.

Operador de atención al cliente de Oi S.A. en el equipo de atención personalizada a clientes de alto valor, atendiendo telefonía fija, móvil, banda ancha y enlaces de datos de alta velocidad, incluido el soporte remoto.

COMPETENCIAS

Operaciones defensivas

Blue Team Defensa perimetral Operaciones de seguridad (SOC) SIEM/SOAR Threat Hunting
Respuesta a incidentes Informática forense (DFIR) Mitigación de DDoS

Ingeniería de seguridad

Seguridad en la nube (CSPM, CWPP) Zero Trust DevSecOps AppSec Seguridad de redes Firewalls
Hardening

Gobernanza y liderazgo

Gestión de amenazas y vulnerabilidades ISO 27001 Concienciación en seguridad Liderazgo

Plataformas

Orca Security Snyk Netskope Akamai Elastic SIEM Trend Micro Vision One Cybereason
Microsoft Sentinel NetIQ Sentinel ArcSight RSA NetWitness GitHub Actions Nessus
Cellebrite UFED EnCase

LICENCIAS Y CERTIFICACIONES



GitLab Certified Associate - GitLab

Emitida abr. 2022 · de2e5529-edf0-44c0-8b92-17ec6a243b3a



Microsoft Certified: Azure Data Fundamentals - Microsoft

Emitida jun. 2021



Microsoft Certified: Azure AI Fundamentals - Microsoft

Emitida jun. 2021



Microsoft Certified: Azure Fundamentals - Microsoft

Emitida oct. 2020 · H551-3317



Scrum Foundation Professional Certificate (SFPC) - Certiprof

Emitida jun. 2020 · CLVSQDQFSS-SQGHZGJ-XHRHRHPTMH



ICSI | CNSS Certified Network Security Specialist - ICSI (International CyberSecurity Institute), Reino Unido

Emitida may. 2020 · 18218405



Autopsy 8-Hour Online Training - Basis Technology

Emitida abr. 2020 · 17209320



Firepower Threat Defense FTD NGFW & NGIPS - Cisco

Emitida ago. 2018



Huawei Certified Network Associate - LTE - Huawei

Emitida sep. 2017



RSA NetWitness Administration y RSA NetWitness Analysis - RSA Security

Emitidas oct. 2015 y jul. 2015



Cursos de Cisco Networking Academy - Cisco

CCNA R&S: Introduction to Networks y Routing and Switching Essentials (2016) · Cybersecurity Essentials, Introduction to IoT y Get Connected (2020)



Linux Unhatched - Network Development Group

Emitida may. 2020



Cybereason Threat Hunter y Cybereason Certified Threat Analyst - Cybereason

Emitidas jun. 2021 y mar. 2021 · Expiradas jun. 2023 y mar. 2023



AccessData Certified Investigator - AccessData (Exterro FTK)

Emitida may. 2020 · Expirada may. 2022



NSE 1 y NSE 2 Network Security Associate - Fortinet

Emitidas abr. 2020 · Expiradas abr. 2022 · VAr41N1hUD / 0x26FuSum8

FORMACIÓN ACADÉMICA



Universidade Federal do Rio de Janeiro

MBA (especialización), Gestión de la Seguridad de la Información
2018 - 2020



Centro Universitário Carioca (UniCarioca)

Tecnólogo, Análisis y Desarrollo de Sistemas
2010 - 2013

IDIOMAS

Portugués (nativo) · Inglés (nivel profesional) · Español (básico)