

Emerson Rodrigues

CPF: 04711622136

Rua Jaguaré, Várzea Grande, Mato Grosso, Brasil

Várzea Grande/MT - CEP: 78118-805

+5565992770403

emerson_rodrigues01@yahoo.com

Grau de instrução

UNIASSELVI - Análise e Desenvolvimento de Sistemas

Experiência profissional

Empresa: RedeFlex Comércio e Serviço de Telefonia Ltda

Cargo: Analista de Infraestrutura (5/2025 - Meu emprego atual)

Principais atividades desempenhadas: Na Redeflex, empresa do setor de telecomunicações e serviços com alta demanda operacional e necessidade de disponibilidade contínua, atuo presencialmente oferecendo suporte direto a servidores e apoio técnico às operações telefônica e administrativa. Atuo na administração de Windows Server e distribuições Linux básicas, realizando instalação, hardening inicial, criação e gestão de contas em Active Directory, aplicação de GPOs e manutenção de serviços críticos de infraestrutura, como DNS e DHCP. Acesso servidores Linux via SSH para manutenção remota e execução de tarefas administrativas.

Configuro e mantenho ambientes virtualizados em VMware e Hyper-V, criando e gerenciando máquinas virtuais para isolar serviços e permitir testes sem impactar a produção. Configurei o Unifi Dream Machine na matriz, centralizando a gestão de todos os Access Points Unifi nas filiais, garantindo padronização e conformidade de segurança, e ajusto regras de Firewall Fortinet para proteção da rede e controle de tráfego.

Utilizo Zabbix para monitorar servidores, links de internet e firewall, assegurando alta disponibilidade e proatividade na detecção de falhas. Realizo rotinas de backup e verificação de integridade de armazenamento, e participo da migração do storage local para SharePoint, promovendo maior segurança, acessibilidade e colaboração entre equipes.

Desenvolvo scripts em PowerShell, Bash e Python para automatizar tarefas repetitivas, como criação em lote de usuários, limpeza de logs e checagem de discos, reduzindo retrabalho e aumentando eficiência. Atendo chamados de primeiro nível, realizo diagnóstico inicial e escalono para times especializados quando necessário. Organizo atividades de infraestrutura no Jira, acompanhando demandas, prazos e entregas da equipe. Com Office 365, administro contas, permissões e serviços de e-mail corporativo.

Documentei procedimentos operacionais padrão (POPs) para garantir continuidade e padronização das rotinas, que receberam elogios da liderança por clareza e praticidade, tornando-se referência em treinamentos internos. Como resultados da minha atuação, a centralização do gerenciamento de APs Unifi reduz falhas de conectividade entre matriz e filiais, aumentando a estabilidade da rede; os ajustes no Firewall Fortinet reforçam a proteção perimetral e diminuem incidentes de segurança; o monitoramento via Zabbix permite identificar problemas antes que impactem os usuários, aumentando a disponibilidade de serviços em 20%; e a migração do storage para SharePoint aumenta a segurança dos dados e facilita o acesso remoto e colaboração.

Com essa experiência, aprofundo práticas de segurança operacional, ganho expertise em diagnóstico e resolução de problemas em ambientes mistos Windows/Linux, inclusive com acesso remoto via SSH, amadureço o uso de scripting para automação e ganho de eficiência, e desenvolvo habilidades em gestão de redes corporativas, centralização de APs Unifi, configuração de firewall Fortinet, monitoramento proativo via Zabbix, gestão de projetos no Jira e migração de storage para soluções em nuvem (SharePoint).

Empresa: Stefanini Group

Cargo: Analista de Suporte e Infraestrutura (3/2023 - 5/2025)

Principais atividades desempenhadas: Na Stefanini, empresa de serviços de TI, estava alocado na empresa de LogFintech Strada, atuei no suporte a usuários finais e à infraestrutura de redes locais e remotas, garantindo continuidade operacional e satisfação do usuário. Prestei administração de endpoints, troubleshooting de conectividade e configuração de políticas de acesso para usuários locais e remotos. Atendi chamados via ITIL Service Desk, utilizando Google Chat e ferramentas de service desk para abertura, acompanhamento e fechamento de chamados.

Apoiei a manutenção de servidores Windows, aplicação de políticas de segurança, controle de acesso e inventário de equipamentos. Participei de iniciativas de padronização do parque de estações e de pequenos projetos de infraestrutura, como substituição de switches gerenciáveis e reorganização de VLANs para separar tráfego e otimizar redes.

Melhorei a experiência do usuário final com atendimento claro, eficiente e orientado à resolução, sendo reconhecido pela liderança do cliente pela postura proativa e pela capacidade de comunicação entre equipes técnicas e não técnicas. As melhorias na padronização facilitaram o suporte remoto e reduziram o número de reaberturas de chamados por problemas recorrentes.

Durante esse período, consolidei conceitos ITIL aplicados ao dia a dia, aprimorei habilidades em suporte remoto, diagnóstico de problemas de rede e sistemas, e desenvolvi sensibilidade para priorização de incidentes e comunicação clara com usuários e equipes técnicas.

Empresa: Procuradoria Geral do Estado de Mato Grosso

Cargo: Analista de TI (11/2021 - 3/2023)

Principais atividades desempenhadas: Na Procuradoria Geral do Estado de Mato Grosso (PGE/MT), atuei no suporte a usuários e à infraestrutura interna, garantindo a continuidade operacional em um ambiente regulado e de alta sensibilidade. Realizei a instalação e configuração de estações de trabalho, acompanhei tecnicamente a implantação de redes e serviços, mantive servidores Windows, administrei Active Directory e apliquei GPOs para padronização de configurações, assegurando uniformidade e estabilidade nos sistemas. Participei de projetos de atualização de sistemas e substituição de equipamentos, contribuindo para a modernização incremental do parque de TI, o que aumentou a estabilidade das estações e reduziu incidentes recorrentes. Recebi feedback positivo de gestores pela disponibilidade, postura proativa e capacidade de adaptar soluções técnicas às restrições administrativas do órgão.

Durante a experiência, aprendi a importância de documentar cada etapa de mudanças em ambiente público, conciliando requisitos técnicos com regras de conformidade e processos de aquisição, fortalecendo minha compreensão sobre governança e continuidade operacional em ambientes regulados.

Como resultado, a modernização incremental do parque reduziu o número de incidentes repetitivos, aumentou a estabilidade da infraestrutura e melhorou a eficiência do suporte interno. E como aprendizado, desenvolvi habilidades em administração de Windows Server, Active Directory e GPOs, atendimento e solução de problemas dos usuários, cerca de 250 colaboradores, na compreensão de processos de governança e regras administrativas, além de aprimorar a capacidade de adaptação técnica.

Conquistas

Conquista: Curso

Título: Introduction to Cybersecurity – Cisco

Descrição: No curso, explorei conceitos fundamentais de cibersegurança, analisando práticas recomendadas de proteção de redes, identificação de vulnerabilidades e técnicas de detecção de ameaças. Realizei exercícios práticos de avaliação de riscos em redes corporativas simuladas, aplicação de medidas de proteção de dados e privacidade, e implementação de políticas de segurança da informação para garantir confidencialidade, integridade e disponibilidade dos sistemas.

Como resultado dos estudos nesse curso, aprimorei minha capacidade de identificar vulnerabilidades de rede e potenciais ameaças antes que impactassem os sistemas. Desenvolvi habilidades para aplicar melhores práticas de cibersegurança em ambientes corporativos, aumentando a resiliência da infraestrutura de TI. Ganhei experiência em proteção de dados e privacidade, reforçando controles de acesso e integridade das informações. e os aprendizados absorvidos nesse curso, melhorou a capacidade de aplicar boas práticas de cibersegurança no dia a dia de departamentos de TI. Compreensão de vulnerabilidades de rede, ameaças cibernéticas e estratégias de mitigação. Entendimento de privacidade e confidencialidade de dados, incluindo medidas para proteção de informações sensíveis. Habilidade em detecção de ameaças e análise de incidentes para reduzir impactos e riscos em redes corporativas.

Conquista: Curso

Título: Microsoft Security, Compliance, and Identity Fundamentals

Descrição: Durante o curso, explorei conceitos essenciais de segurança, conformidade e gerenciamento de identidade. Realizei atividades práticas sobre o modelo de responsabilidade compartilhada, estratégias de defesa em profundidade, aplicação do modelo Zero Trust e criptografia de dados para proteção de informações corporativas. Também estudei autenticação e autorização de usuários, implementação de políticas de identidade, administração de Active Directory e integração de sistemas via federação. E, como resultado e aprendizado temos: Desenvolvi capacidade de aplicar princípios de segurança e conformidade em ambientes corporativos, aumentando a proteção de dados e sistemas. Ganhei habilidade em planejar e gerenciar identidades digitais, garantindo acesso seguro e controlado a recursos críticos. Aprimorei o entendimento de modelos de segurança modernos, incluindo Zero Trust, fortalecendo a postura de segurança em ambientes corporativos e cloud. Também tive melhor compreensão de segurança da informação, compliance e proteção de dados, aplicável em infraestrutura de TI corporativa. Capacidade de gerenciar identidade e autenticação de usuários, incluindo Active Directory e federação entre sistemas. Entendimento de defesa em profundidade e Zero Trust, reforçando políticas de acesso seguro. Preparação para atuar em projetos de governança, gestão de riscos e segurança de TI.

Conquista: Certificado

Título: Introduction to Cybersecurity for Business – University of Colorado System

Descrição: Durante o curso, participei de exercícios voltados para gestão de riscos, avaliação de vulnerabilidades, segurança de redes e conscientização em cibersegurança. Analisei cenários de ameaças reais a empresas, simulando ataques e estudando métodos de autenticação segura, criptografia e proteção de dados corporativos. Realizei práticas de avaliação de vulnerabilidades e aplicação de controles de segurança em ambientes empresariais simulados, fortalecendo o conhecimento em enterprise security e segurança de TI para negócios. Como resultado obtive habilidade em identificar riscos e vulnerabilidades em ambientes corporativos, aplicando medidas preventivas e corretivas. Aprimorei a capacidade de planejar e implementar controles de segurança, autenticação e criptografia para proteger dados sensíveis. Ganhei experiência em treinamento de conscientização de usuários e práticas de segurança, reduzindo potenciais falhas humanas e fortalecendo a postura de segurança da empresa. E, como aprendizado obtive melhor capacidade de aplicar gestão de riscos, avaliação de vulnerabilidades e controles de segurança em empresas. Compreensão de segurança de rede, autenticação, criptografia e proteção de dados corporativos. Desenvolvimento de habilidades em segurança empresarial e treinamento de

conscientização em cibersegurança, promovendo práticas seguras entre usuários finais. Preparação para atuar em ambientes de TI corporativos com foco em prevenção, mitigação e governança de riscos cibernéticos.

Conquista: Certificado

Título: Cybersecurity for Everyone – University of Maryland, College Park

Descrição: Durante o curso, explorei os fundamentos da segurança cibernética, realizando exercícios sobre gestão de riscos, identificação de vulnerabilidades, ameaças cibernéticas e políticas de segurança. Analisei cenários de ataques reais e simulações de incidentes, aprendendo a aplicar estratégias de detecção de ameaças, governança de TI e segurança de dados em diferentes ambientes corporativos. Estudei a implementação de controles de segurança e boas práticas de gestão de incidentes para proteger redes e sistemas, considerando aspectos técnicos e organizacionais.

Resultados: Desenvolvi capacidade de identificar e gerenciar riscos cibernéticos em ambientes empresariais, priorizando ações de mitigação e prevenção. Ganhei habilidade em criar e implementar políticas de segurança, estratégias de cibersegurança e governança alinhadas aos objetivos do negócio. Aprimorei a capacidade de detectar e responder a ameaças e vulnerabilidades, aumentando a resiliência e a confiabilidade de sistemas e redes.

Aprendizado: Compreensão sólida de gerenciamento de segurança, gestão de riscos e ciberataques. Capacidade de aplicar políticas de segurança, governança de TI e estratégias de cibersegurança em diferentes contextos organizacionais. Conhecimento em proteção de dados, detecção de ameaças e segurança empresarial, incluindo fundamentos de redes e vulnerabilidades. Preparação para atuar de forma consciente e estratégica em projetos de segurança da informação e infraestrutura de TI, garantindo proteção e continuidade operacional.

Conquista: Curso

Título: Aprendendo Fortigate Firewall do Zero ao Avançado (NSE4)

Descrição: Durante o curso, configurei firewalls Fortigate em ambientes corporativos simulados, utilizando VirtualBox e GNS3 para criar topologias completas com múltiplos hosts (Fortigate, Windows, Kali Linux, Metasploitable). Executei a instalação e configuração de interfaces LAN e WAN, usuários administrativos, DHCP, DNS, NAT (dynamic, destination e central NAT), criação de políticas de firewall, objetos e autenticação via Captive Portal. Configurei DMZs, antivírus, filtros de web, DNS, aplicações, IPS e File Filter. Aprendi a implementar VDOMs, inter-VDOM links, SSL VPN (tunnel e web mode), inspeção SSL profunda e gerenciamento de certificados digitais. Também pratiquei backup e restauração de configurações e análise de logs locais e remotos para monitoramento e troubleshooting. Como resultado do curso desenvolvi a habilidade para projetar e gerenciar topologias complexas de firewall, garantindo conectividade segura em redes corporativas. Aprimorei a capacidade de prevenir e mitigar riscos de segurança com políticas avançadas de firewall, controle de aplicações, filtros e IPS. Ganhei experiência em implementação de SSL VPNs e segmentação de redes via VDOMs, permitindo acessos remotos seguros e gerenciamento isolado de ambientes. Melhorei a capacidade de troubleshooting e análise de logs, facilitando identificação de incidentes e garantindo disponibilidade dos serviços de rede.

E como aprendizado, Domínio do Fortigate: instalação, configuração e gerenciamento de interfaces, NAT, políticas, objetos, DMZs, filtros, IPS e SSL VPN. Capacidade de criar topologias complexas para testes e ambientes corporativos usando VirtualBox e GNS3. Compreensão de segurança de rede avançada, incluindo inspeção SSL profunda, certificação digital e políticas de autenticação. Habilidade em monitoramento, backup/restauração de configurações e análise de logs locais e remotos. Preparação para atuar em infraestrutura de TI corporativa, consultoria de segurança e administração de firewalls Fortigate, com foco em proteção, conectividade e continuidade operacional.

Conquista: Curso

Título: Ninja em pfSense

Descrição: Durante o curso, pratiquei a instalação e configuração completa do pfSense, incluindo interfaces de rede com IP estático, DHCP e PPPoE, criação de VLANs, configuração de IPs virtuais, hostname, DNS com ou sem Active Directory, timezone e horário. Configurei acesso web e SSH seguro, proteção de login, criação de usuários e grupos, atribuição de permissões e integração com LDAP seguro. Realizei backup e restauração manual e automática do firewall, inclusive em hardware diferente, além de testar reversão de configurações incorretas.

Como Resultado tive: Aumento de capacidade de gerenciar redes e segurança com pfSense, garantindo conectividade estável e proteção de dados em ambientes corporativos. Desenvolvi habilidade para implementar soluções robustas de firewall, incluindo Web Proxy, IDS/IPS e VPN de alta disponibilidade, proporcionando maior segurança e resiliência das redes. Gerei procedimentos de backup e restauração eficientes, reduzindo o tempo de recuperação de falhas e mantendo a continuidade operacional.

Aprendizado do curso: Domínio completo de pfSense, incluindo instalação, configuração de interfaces, VLANs, IPs virtuais, DNS, autenticação LDAP e gerenciamento de usuários/admins. Configuração de firewall, políticas de segurança, Web Proxy, VPNs e IDS/IPS, garantindo proteção avançada da rede. Desenvolvimento de boas práticas de backup, restauração e recuperação de configurações, aplicáveis em ambientes de produção. Capacidade de analisar e gerenciar tráfego de rede, processar pacotes e configurar notificações via e-mail ou Telegram. Preparação para atuar de forma prática e estratégica em consultorias, equipes de infraestrutura e ambientes corporativos de TI, aumentando segurança, disponibilidade e confiabilidade.

Conquista: Curso

Título: UniFi Expert: Redes Wi-Fi Profissionais na Prática

Descrição: Durante o curso, realizei configuração e gerenciamento de redes Wi-Fi corporativas utilizando equipamentos UniFi. Aprendi a explorar diferentes modelos de dispositivos e a acessar o controller local e em nuvem com segurança e eficiência. Configurei redes, VLANs, redes sem fio e controle de convidados, aplicando técnicas avançadas de planejamento de canais, largura de banda e gerenciamento de interferências. Também configurei nomes de dispositivos, adotei APs no controller, organizei grupos de administradores e realizei backups periódicos para garantir a segurança das configurações. Como Resultados temos: Aumento da eficiência e estabilidade das redes Wi-Fi, garantindo cobertura adequada, desempenho otimizado e redução de interferências. Ganhei capacidade de resolver problemas complexos de conectividade, utilizando análises detalhadas com ferramentas de varredura Wi-Fi e aplicando ajustes em tempo real. Melhorei a gestão de redes corporativas, incluindo planejamento de VLANs, administração de APs e organização de usuários, elevando a confiabilidade e segurança das operações de rede. Os aprendizados do curso foram: Domínio na configuração de Access Points UniFi, adoção de dispositivos e gerenciamento via controller local e em nuvem. Compreensão dos conceitos de cobertura, propagação de sinal e impactos de diferentes materiais no desempenho da rede. Planejamento de canais, largura de banda e mitigação de interferências para otimizar performance em ambientes corporativos. Habilidade em gerenciamento de usuários, grupos de administradores e políticas de controle de convidados, garantindo organização e segurança. Capacidade de realizar backups de configurações, mantendo integridade e continuidade operacional das redes Wi-Fi.

Conquista: Curso

Título: Administração de Servidores e Serviços de Rede

Descrição: Durante o curso, estudei e implementei principais serviços de rede, incluindo DNS, HTTP, servidores de e-mail (SMTP, POP e IMAP), DHCP, FTP, Proxy e soluções de firewall (UTM e NGFW). Realizei configurações e análise de logs em ambientes GNU/Linux (Debian, CentOS/Red Hat) e Windows Server, aplicando conceitos de interoperabilidade e segurança entre plataformas. Participei de simulações de problemas, utilizando os conceitos aprendidos para diagnóstico e resolução de incidentes de rede, aumentando a capacidade de troubleshooting de forma prática e assertiva. Como resultado, dominei a implementação e

administração de serviços de rede em diferentes plataformas, garantindo interoperabilidade e segurança. Aumentei a capacidade de resolução de problemas de rede, identificando rapidamente a origem de falhas a partir da análise de logs e da compreensão das camadas de transporte (TCP/UDP). Consolidei conhecimento em configuração de servidores e políticas de rede que poderiam ser aplicados em ambientes corporativos reais, aumentando confiabilidade e disponibilidade dos serviços. E Aprendizados, a compreensão aprofundada de conceitos e funcionamento de serviços de rede essenciais: DNS, HTTP, SMTP, POP, IMAP, DHCP, FTP, Proxy e firewalls (UTM/NGFW). A capacidade de implementar serviços de rede em ambientes GNU/Linux e Microsoft, considerando segurança, compatibilidade e melhores práticas. O desenvolvimento de habilidade de troubleshooting e análise de logs para identificar e corrigir falhas de forma assertiva. Entendimento da relação entre camadas de transporte, portas TCP/UDP e serviços de rede, essencial para diagnóstico avançado. A preparação para atuar de forma prática em ambientes corporativos com múltiplas plataformas e serviços de rede integrados.

Conquista: Curso

Título: Gerenciamento de Infraestrutura de TI

Descrição: Durante o curso, realizei estudos e exercícios práticos sobre infraestrutura de TI, compreendendo desde conceitos básicos até o gerenciamento completo de um parque de TI. Explorei o controle de ativos, incluindo inventário físico e de software, gestão de usuários e monitoramento de dados. Analisei ambientes de Data Center, servidores, redes e telecom, identificando pontos críticos e aprendendo a prevenir falhas. Simulei atividades de planejamento e condução de projetos de infraestrutura, aplicando boas práticas de monitoramento, manutenção e governança. Como Resultado destaco que desenvolvi uma visão holística da infraestrutura de TI, permitindo identificar áreas críticas e antecipar problemas que poderiam gerar paradas de sistemas ou serviços. Também aprimorei a proatividade na administração de TI, com foco em prevenção de incidentes e otimização de processos operacionais. Ganhei ferramentas para gerenciar e organizar toda a complexidade de um parque de TI, aumentando eficiência e confiabilidade dos serviços. Como Aprendizado cito a compreensão do que constitui infraestrutura e infraestrutura de TI, suas etapas, componentes e interdependências. A capacidade de realizar controle completo de ativos, inventário físico e de software, gerenciamento de usuários e dados críticos. Habilidade de monitorar ambientes complexos, incluindo Data Centers, servidores, redes e telecom, antecipando falhas e garantindo disponibilidade. O desenvolvimento de planejamento estratégico e operacional para condução de projetos de infraestrutura, aumentando previsibilidade e qualidade na entrega de serviços. Aplicação prática de conceitos de gerenciamento de infraestrutura de TI, integrando controle, monitoramento e planejamento para ambientes corporativos.

Conquista: Curso

Título: IT Support Management: Central de Serviços de TI

Descrição: Durante o curso, realizei exercícios práticos de identificação e análise de riscos em ambientes de TI, estudando casos reais de ameaças que impactam diretamente a infraestrutura e os serviços. Aprendi a mapear responsabilidades usando matrizes de RACI, aplicar conceitos de ITSM, GSTI e governança de TI em atividades simuladas e definir processos e procedimentos de controle de riscos para aumentar a eficiência operacional. Como resultado, consegui descrever com segurança a estrutura e os principais conceitos de análise e controle de riscos em TI, aplicar cada conceito em situações práticas simulando cenários reais de departamentos de TI, qualidade e governança, e desenvolver capacidade de realizar ações de ganhos rápidos por meio de boas práticas de ITSM e gestão de riscos, aumentando a previsibilidade e reduzindo potenciais falhas em serviços de TI.

Entre os principais aprendizados, destaco a identificação de ameaças que impactam diretamente o ambiente de TI. A aplicação de conceitos de governança, ITSM e GSTI em processos do dia a dia de um departamento de TI. A compreensão e utilização da terminologia técnica de gerenciamento de serviços e riscos de TI. Capacidade de

discutir e aplicar conceitos do ciclo de vida dos riscos de TI em uma perspectiva global. Planejamento e aplicação de matrizes de responsabilidades (RACI), priorização de processos e procedimentos, e seleção de boas práticas para ambientes reais de TI.

Idiomas

Idioma: Inglês
Nível: Intermediário

Idioma: Espanhol
Nível: Intermediário

Perfil em redes sociais

LinkedIn: <https://www.linkedin.com/in/emersonrodrigues10>