

20
26

WTR

WORKSHOP DE
TECNOLOGIAS
DE REDES
PoPBA

**O Inimigo Dentro de Casa: Falhas
Silenciosas, Convivência com Legados e
o Hardening da Rede Interna**

Prof. Dr. Rafael Freitas Reale

Ministério da Previdência Social

28 A 30
SETEMBRO

VOCÊ
FAZ
PARTE
DESSA
CONEXÃO

REALIZAÇÃO



PoPBA

RINP

MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO





RAFAEL FREITAS REALE



CISC
gov.br

DOUTOR UFBA (CAPES 6)

ENGENHEIRO MPS/MTE

CISCO NETACAD 9+ ANOS

Currículo e Atuação Profissional

Doutor em Ciência da Computação pela UFBA (Conceito CAPES 6).



ENAP: Criador do curso de primeiros passos em cibersegurança no serviço público da ENAP.



Governo: Atua como Engenheiro de Cibersegurança no MPS e MTE.



Cisco NetAcad: Instrutor da Academia Cisco (NETACAD) há mais de nove anos.



Docência e Gestão: Mais de 16 anos como professor, pesquisador e docente do Mestrado de Sistemas e Produtos no IFBA. Experiência em gestão educacional (Diretor de Ensino e Coordenador de Curso).



Projetos Federais: Participação ativa em projetos do Governo Federal (PRONATEC, GESAC, Telecentros e PROFROTA Pesqueira).



Network Security
Cisco

Issued May 23, 2021



CyberOps Associate
Cisco

Issued Dec 14, 2021



Network Security
Cisco

Issued May 23, 2021



Instructor 5 Years of Service
Cisco

Issued Feb 17, 2021



CCNA: Enterprise Networking,
Security, and Automation
Cisco

Issued Dec 30, 2020

+85%

Das invasões exploram configurações obsoletas, domínios planos, regras permissivas e falta de segmentação da rede.

SMBv1 & SMBv2 (TCP 445)

RCE Legado e Tráfego Não Cifrado

Execução remota crítica no v1 (vetor de ransomware) e ausência de cifragem nativa de dados no v2, suscetível a sniffing e relay.

NTLMv1 & NTLMv2

Quebra de Hash e Ataques de Relay

Criptografia obsoleta no v1 (quebra direta de senha) e vulnerabilidade intrínseca a repasse (relay) no v2 sem signing forçado.

LDAP Simples (TCP 389)

Credenciais em Claro

Senhas de bind e autenticação sem cifra no tráfego

LLMNR (UDP 5355)

Envenenamento Multicast de Nomes

Resolução local sem autenticação; atacantes forjam respostas via multicast para capturar credenciais NetNTLM em tempo real.

NetBIOS-NS (UDP 137)

Spoofing por Broadcast de Rede

Mecanismo legado de difusão (broadcast) em camada 2/3, facilmente explorado por ferramentas como Responder para interceptação e relay.

SNMPv1 & SNMPv2c (UDP 161)

Exfiltração e Strings em Claro

Senhas de comunidade (community strings) trafegam sem cifra, permitindo inventário não autorizado e manipulação de ativos de rede.

HTTP (TCP 80)

Intercepção e Manipulação de Sessões

Captura de credenciais e cookies de sessão, com exposição total a ataques de Man-in-the-Middle e injeção de tráfego.

TELNET (TCP 23)

Credenciais e Sessões em Claro

Envio de utilizador, palavra-passe e comandos sem qualquer cifra, permitindo a leitura direta de todo o tráfego administrativo.

FTP (TCP 20 / 21)

Exposição de Autenticação e Arquivos

Transmissão de comandos, credenciais de acesso e ficheiros confidenciais em texto simples através da rede.

Modelo Plano (Sem Isolamento)

ALTO RISCO / ROTA DE CRISE

Movimentação Lateral Irrestrita

Credenciais administrativas de Domain Admin utilizadas em estações de trabalho vulneráveis, expostas a ataques de LSASS e Pass-the-Hash.

Comprometimento Total do Domínio

A quebra de um único endpoint com sessão de admin possibilita o salto direto para o controle total dos Controladores de Domínio (DCs).

Ausência de Fronteiras de Autenticação

Não há restrição de logon cruzado entre ativos críticos, servidores de aplicação e estações comuns de usuários.

Modelo em Camadas (Tiering Model)

ARQUITETURA RECOMENDADA

Tier 0 — Ativos de Identidade Críticos

Controladores de Domínio, PKI e ADFS. Acesso exclusivo por contas T0 autenticadas apenas em dispositivos PAW (Privileged Access Workstations).

Tier 1 — Servidores e Aplicações

Gestão de servidores membros e serviços corporativos. Administradores T1 não possuem privilégios no Tier 0 nem logavam no Tier 2.

Tier 2 — Estações de Trabalho e Dispositivos

Dispositivos de usuários finais e helpdesk. O comprometimento desta camada é totalmente estancado, impedindo a elevação para T1 ou T0.

Administração Direta (Sem Jump Server)

ALTO RISCO / PONTO CEGO

Acesso Direto aos Ativos

Conexões diretas de estações de trabalho para servidores críticos sem intermediação, contornando controles de segurança e inspeção de rede.

Ausência de Diário de Bordo (Auditoria Zero)

Falta de registro centralizado das atividades executadas. Impossibilidade de rastrear comandos, alterações de configuração ou ações maliciosas.

Exposição Integrada de Credenciais

Credenciais privilegiadas são digitadas diretamente em endpoints vulneráveis, expostas a captura de sessão e roubo de credenciais.

Arquitetura Bastion Host / Jump Server

ARQUITETURA RECOMENDADA

Ponto Único de Inspeção e Controle

Todo o tráfego administrativo é forçado a passar por um servidor enrijecido (Bastion Host), isolando os ativos críticos da rede geral.

Diário de Bordo e Auditoria Completa

Gravação de sessões, gravação de comandos digitados e logs de acesso detalhados. Rastreabilidade total sobre quem fez o que e quando.

Isolamento e Autenticação Forte

Exigência de MFA e controle de acesso estrito. As credenciais do servidor final nunca são expostas no endpoint do administrador.

Práticas Inseguras (Servidor Exposto)

ALTO RISCO / SUPERFÍCIE
AMPLIADA

Conexões Ativas e Iniciadas pelo Servidor

Servidores realizando conexões ativas de saída para a rede ou internet, facilitando canais de comando e controle (C2) e exfiltração.

Serviços Desnecessários Ativos

Execução de serviços secundários não essenciais (ex: Spooler de Impressão), expandindo a superfície para exploração de vulnerabilidades.

Rede Plana (VLAN Única)

Todos os servidores concentrados no mesmo segmento de rede, eliminando a proteção e permitindo movimentação lateral livre (Leste-Oeste).

Arquitetura Segura e Enrijecida

ARQUITETURA RECOMENDADA

Comportamento Passivo e Regras Estritas

Servidores respondem apenas a requisições. Controle rigoroso de tráfego de entrada e saída estritamente necessário.

Desativação de Serviços não Essenciais

Hardening contínuo com desativação de recursos supérfluos (como serviços de impressão) para reduzir vetores de ataque.

Microsegmentação e Fronteiras Leste-Oeste

Divisão de ambientes em múltiplas VLANs/zonas com firewalls para criar barreiras efetivas contra a movimentação lateral.

Riscos de Sistemas Legados (EOL)

ALTO RISCO &
VULNERABILIDADE

Sistemas Operacionais Sem Suporte

Sistemas operacionais e aplicações legadas não recebem mais atualizações de segurança, tornando-se alvos fáceis para exploração contínua.

Autenticação Insegura no AD

Aplicações legadas autenticam diretamente no AD principal sem protocolos modernos, sem proteção contra força bruta e sem suporte a MFA.

Exposição e Movimentação Lateral

A falta de controles modernos permite que o comprometimento de um sistema legado sirva de ponte para invadir toda a rede corporativa.

Mitigação e Controles de Segurança

ARQUITETURA DE
COMPENSAÇÃO

Quarentena de Rede e VLAN Dedicada

Isolamento estrito dos sistemas legados em VLAN específica sem acesso direto à internet, contendo eventuais ameaças e vazamentos.

Acesso Seguro via RemoteApp / Jump Server

Intermediação do acesso do usuário através de RemoteApp ou Bastion/Jump Server, impedindo conexões diretas aos hosts vulneráveis.

Uso de WAF (Web Application Firewall)

Implementação de WAF para inspecionar o tráfego de aplicação e mitigar vulnerabilidades conhecidas em sistemas sem patch.

Redes Wi-Fi e Visitantes (Wi-Fi Guest)

ISOLAMENTO E VISITANTES

VLAN Exclusiva para Visitantes

Rede Wi-Fi de convidados isolada da infraestrutura acadêmica interna, garantindo apenas acesso direto à internet sem comunicação entre dispositivos (Client Isolation).

Captive Portal e Autenticação

Controle de acesso via portal de cadastro para convidados e integração 802.1X/eduroam para alunos, professores e pesquisadores de instituições de ensino.

Inspeção e Qualidade de Serviço (QoS)

Limitação de largura de banda e bloqueio de protocolos abusivos no Wi-Fi de visitantes para evitar sobrecarga da banda e mitigar riscos de uso indevido da rede.

Laboratórios e Acesso Público

PROTEÇÃO E INTEGRIDADE

Proteção por Reboot-to-Restore (Deep Freeze)

Computadores de laboratórios acadêmicos e bibliotecas restauram o estado original a cada reinicialização, descartando softwares maliciosos e alterações indesejadas.

Segmentação de VLANs por Laboratório

Isolamento em zonas distintas entre laboratórios de ensino, máquinas da biblioteca e redes administrativas, restringindo a propagação de malwares.

Restrições de Privilégio e Diretiva de Grupo

Uso de perfis de usuário não-administrador com bloqueio de instalação de softwares não autorizados e controle de portas USB em computadores públicos.

Vetores de Risco & Execução Indesejada

SUPERFÍCIE DE ATAQUE EXPOSTA

Execução Remota Não Autorizada (LOLBas)

Abuso de ferramentas legítimas de administração como PSEXec, WMI, RPC e PowerShell para movimentação lateral, execução de scripts maliciosos e evasão de defesas.

Softwares de Suporte & Acesso Remoto (RATs)

Uso de utilitários como AnyDesk, TeamViewer e RustDesk sem controle central, criando canais de acesso externo não monitorados e ignorando o firewall da organização.

Ferramentas de Desenvolvimento, Servidores Web e virtualizadores

Presença Virtualizadores (VM Ware, VirtualBox), interpretadores (Python, Node.js), e mini servidores web locais em estações de trabalho, permitindo execução de código arbitrário.

Controles de Segurança & Restrição

ARQUITETURA DE PROTEÇÃO

Bloqueio de Protocolos & Constrained Language

Restrição de RPC/WMI entre estações, desativação de PSEXec via firewall de host e configuração de PowerShell em Constrained Language Mode com Logging de Scriptblock.

Políticas de AppLocker & Bloqueio de RATs

Bloqueio executável por hash/assinatura de ferramentas de acesso remoto não corporativas, aliado ao bloqueio de portas e conexões para servidores dessas ferramentas no EDR/NGFW.

Controle de Aplicações & Princípio do Menor Privilégio

Whitelisting rigoroso de binários permitidos, remoção de privilégios administrativos locais e isolamento de ambientes de desenvolvimento (Python) em containers ou sandboxes.

Baseline & Detecção de Anomalias

COMPORTAMENTO SUSPEITO

Conhecimento do Perfil de Tráfego (Baseline)

O entendimento prévio do padrão normal da rede possibilita a identificação rápida de desvios operacionais e alterações volumétricas atípicas.

Sinalização de Atividade Maliciosa

Mudanças repentinas no comportamento de comunicação costumam indicar varreduras, movimentação lateral ou presença de ameaças ativas na rede.

Prevenção e Identificação de Exfiltração

Transferências massivas para destinos não habituais ou picos de upload sinalizam potenciais vazamentos e roubo de dados corporativos sensíveis.

Métricas de Visibilidade ("Top Talkers")

AUDITORIA & TELEMETRIA

Mapeamento de Acessos & Hosts

Identificação contínua do consumo de banda e padrões de comunicação por ativos centrais:

Análise de Origem & Destino

Rastreabilidade ponta a ponta dos fluxos de conexão estabelecidos dentro e fora do perímetro:

Categorização de Aplicações & Serviços

Inspeção detalhada do tipo de tráfego trafegado para contenção de uso não autorizado:

O Perigo dos Zumbidos Negligenciados

CEGUEIRA OPERACIONAL & POLUIÇÃO

Acúmulo e Perda de Monitorabilidade

Alertas secundários não tratados se acumulam rapidamente até se tornarem imonitoráveis. Quando o volume de ruído é alto, indicadores cruciais de segurança são completamente ignorados.

Alto Volume de WebViolations

Pode parecer apenas navegação indevida ou falha de política, mas frequentemente oculta um processo automatizado malicioso rodando na máquina, como malware Adware ou comunicação C2/C&C.

Eventos Repetitivos de Autenticação (Erro 4625)

Geralmente descartado como uma senha errada salva em cache, mas pode representar uma força-bruta ativa ou tentativa oculta de quebra de credenciais na rede.

Ações de Mitigação & Higiene de Rede

RESPOSTA E CONTROLE IMEDIATO

Atuação Imediata na Redução de Ruído

Intervir imediatamente para baixar o nível de ruído base da rede. Manter os zumbidos baixos é o único meio de garantir que anomalias leves sinalizem ameaças reais.

Investigação de Processos e Infecções C2

Auditar e isolar máquinas gerando volume atípico de bloqueios web para identificar e eliminar scripts, adwares e canais de comando e controle ativos.

Tratamento de Credenciais e Bloqueio Preventivo

Corrigir mapeamentos com senhas expiradas salvas e aplicar bloqueios automáticos para diferenciar falhas legítimas de ataques de dicionário e password spraying.

Vulnerabilidades de Monitoramento & Firewall

PONTO CEGO & RISCO OPERACIONAL

Falhas em Sensores (Zabbix/ELK)

Não adianta ter uma estrutura robusta de monitoramento se um sensor parar e ninguém notar. Sem alertas de Heartbeat, a cegueira sobre a rede se torna total.

Regras Permissivas e Maliciosas

A alteração ou criação incorreta de regras no firewall pode expor serviços críticos. Alterações mal-intencionadas criam brechas diretas para invasão.

Evasão por Controle de Acesso

Se um atacante obtiver acesso às ferramentas de monitoramento ou firewall, ele pode silenciar os alarmes e derrubar as defesas sem ser detectado.

Controles & Notificação Rápida

ARQUITETURA DE RESILIÊNCIA

Aprovação Dual & Duplo Fator (Dual-Control)

Separação de credenciais: utilize uma senha dedicada para a criação da regra e outra senha distinta para a efetivação/commit das alterações.

Alertas em Canal Confiável

Envio imediato de alertas em canais corporativos (ex: Microsoft Teams, Signal) para qualquer mudança de configuração ou desativação de sensor.

Auditoria Integrada de Configuração

Rastreamento e auditoria contínua de diffs de configuração em firewalls e plataformas como Zabbix/ELK, garantindo pronta resposta a incidentes.

Auditoria Rígida & Rastreabilidade Tier 0

IDENTIFICAÇÃO & RESPOSTA RÁPIDA

Visibilidade Total de Sessões (Entrada, Ação e Saída)

Garantia de auditoria exata sobre quem acessou o Tier 0/Active Directory, quais ações executou e o horário exato do término da sessão.

Notificação Imediata em Canais Confiáveis

Alertas instantâneos em grupos seguros para ações críticas, garantindo janela hábil para contenção e mitigação caso haja roubo de credenciais.

Alertas de Desvio de Comportamento em AD

Deteção e sinalização em tempo real de alterações de privilégios, criação de contas privilegiadas e modificações não autorizadas.

Governança & Segregação de Funções

SEGREGAÇÃO DE RESPONSABILIDADES

Quem Autoriza, Não Executa

Aprovação de solicitações e mudanças de acesso gerida estritamente por perfis de gestão, prevenindo autorizações unilaterais no ambiente.

Quem Executa, Não Audita

Operadores e administradores de sistema não possuem privilégios para alterar ou apagar logs de auditoria e configurações de monitoramento.

Triangulação Independente de Logs Imutáveis

Coletores de telemetria isolados e imutáveis garantem a integridade das evidências e eliminam conflitos de interesse na infraestrutura.

Autorização & Decisão Estratégica

RESPONSABILIDADE INALIENÁVEL

Controle Absoluto de Acessos Críticos

Aprovação final de privilégios elevados, contas administrativas e acessos ao Tier 0/AD deve ser exclusiva da gestão interna, sem delegação integral.

Aprovação de Mudanças na Segurança

Alterações em regras de firewall, políticas de segurança e exceções operacionais exigem validação e aceite direto dos gestores da organização.

Gestão de Chaves e Credenciais MESTRE

A posse de certificados raiz, cofres de senhas do ambiente e chaves criptográficas vitais nunca deve ser transferida integralmente a terceiros.

Auditoria & Governança Directa

SUPERVISÃO NÃO TERCEIRIZÁVEL

Custódia Independente de Logs

Coletores de telemetria e registros de auditoria devem ser mantidos em infraestrutura sob domínio total da gestão para evitar adulterações.

Acompanhamento e Triangulação de Terceiros

Ações realizadas por empresas terceirizadas ou parceiras devem ser continuamente auditadas e validadas por um time de governança interno.

Tomada de Decisão em Incidentes Críticos

A contenção, isolamento de sistemas e comunicação de crises de segurança exigem autorização final e liderança da própria gestão.

1. Transparência & Sessões

NOTIFICAÇÕES & IDENTIDADE

Notificações e Transparência

- **Acessos:** E-mail automático a cada acesso (data, hora, IP, dispositivo, local).
- **Benefícios:** Alerta de alterações cadastrais/financeiras e histórico completo.
- **Relatórios:** Consolidado semanal/gerencial com volumetria e eventos sensíveis.

Proteção de Sessões e Identidade

- **Controle de Sessão:** Encerramento/revalidação por mudança de contexto (IP/local).
- **Correlação Geográfica:** Alerta/bloqueio para acessos incompatíveis com deslocamento físico.
- **Vinculação:** Sessão atrelada ao dispositivo autenticado.

Atendimento em Massa

- **Perfil Temporário:** Escopo mínimo e expiração automática pós-evento.
- **Controles:** Aprovação prévia, auditoria integral e relatório consolidado.
- **Monitoramento:** Alertas de desvio e revisão pela auditoria.

2. Governança & Operações

OBSERVABILIDADE & AUTOMAÇÃO

Observabilidade & Volumetria

- **Dashboards:** Acompanhamento diário/semanal e detecção de anomalias.
- **Limites Operacionais:** Teto configurável para consultas, relatórios e aprovações.
- **Janelas Agendadas:** Obrigatoriedade para auditorias massivas e mineração.

Governança de Operações Sensíveis

- **Workflows:** Aprovação multinível para concessões, extrações e acessos temporários.
- **Revisão Periódica:** Certificação e revogação automática por inatividade.
- **Trilhas de Auditoria:** Registros imutáveis com solicitante, justificativa e IP.

Gestão de Robôs e Automações

- **Internalização:** Redução da dependência de robôs externos.
- **Segregação:** Ambiente isolado, cofre de senhas (PAM) e MFA.
- **Controle:** Inventário centralizado, rastreabilidade total e uso de ambientes confiáveis para execução.

3. Segurança de APIs

PROTEÇÃO & CONSUMO

Autenticação & Volumetria

- **Acesso Autenticado:** Exigência de autenticação mesmo para dados públicos.
- **Limites Padrão:** Teto de consultas e tráfego por perfil.
- **Consumo Elevado:** Exige justificativa formal e chave especial.

Proteção contra Abusos

- **Anti-Scraping:** Bloqueio de mineração massiva e enumeração.
- **Detecção Automática:** Identificação de anomalias e comportamentos incompatíveis.
- **Minimização:** Retorno exclusivo de dados estritamente necessários.

Auditoria & Revisão Contínua

- **Trilha Completa:** Registro de consumidor, IP, horário e volume.
- **Revisão Periódica:** Avaliação de consumidores de alta volumetria.
- **Perfis Especiais:** Liberação condicional para pesquisas e integrações legítimas.

Frameworks de Segurança & PPSI 2.0

GOVERNANÇA & SETOR PÚBLICO

Adoção de Frameworks Estruturados

Garante maturidade, padronização global e alinhamento das melhores práticas de segurança da informação (NIST, ISO 27001, CIS Controls) para a proteção do ambiente corporativo e público.

Diretrizes do PPSI 2.0 da SGD/MGI

O Programa de Privacidade e Segurança da Informação estabelece requisitos obrigatórios de governança, gestão de riscos, controles essenciais e maturidade digital para órgãos do Poder Executivo Federal.

Acompanhamento e Nível de Maturidade

Uso de indicadores continuados e avaliações periódicas para assegurar a conformidade legal, auditoria governamental e contínua evolução da postura de cibersegurança pública.

Notificação & Comunicação de Incidentes

RESPOSTA COORDENADA & ECOSISTEMA

CTIR.gov (Centro de Prevenção e Resposta)

Notificação obrigatória de incidentes cibernéticos na Administração Pública Federal para coordenação centralizada, mitigações nacionais e contenção de ameaças à infraestrutura crítica.

CISC & Articulação Setorial

Integração com o Comitê de Gestão de Incidentes Cibernéticos para alinhamento estratégico, compartilhamento seguro de inteligência de ameaças e respostas rápidas interórgãos.

CERT.br & Cooperação com a Internet

Reporte e apoio técnico para tratamento de incidentes no ecossistema da Internet do Brasil, atuando na análise de tendências, estatísticas nacionais e correlação global de ataques.

1. Memória RAM & Volatilidade

NÃO DESLIGUE A MÁQUINA!

Coleta de RAM em 1º Lugar

- **Ordem de Volatilidade:** A memória RAM possui altíssima volatilidade e deve ser capturada imediatamente antes de qualquer desligamento.
- **Ameaças Fileless:** Malwares modernos executam exclusivamente em memória. Desligar a máquina destrói totalmente as evidências vitais.

Ambientes Virtuais (VMs)

- **Snapshot com Memória:** Em hipervisores, realize o snapshot incluindo explicitamente o estado da memória RAM.
- **Preservação do Estado:** Garanta o snapshot adequado antes de qualquer alteração na infraestrutura virtualizada.

Artefatos e Processos

- **Injeção de Código:** Mapeamento de DLLs injetadas, payloads ocultos e conexões de rede ativas em tempo de execução.
- **Adulteração:** Evite rodar ferramentas locais não confiáveis que possam alterar o espaço de endereçamento da RAM.

2. Logs & Rastreabilidade de Rede

REGISTROS DE CONEXÃO

Portas de Origem

- **Essencial para NAT:** A exportação de logs deve conter obrigatoriamente a porta de origem (Source Port).
- **Identificação Precisa:** Sem a porta de origem, é impossível correlacionar conexões em ambientes com tradução de NAT/CGNAT.

Exportação Centralizada de Logs

- **Isolamento de Trilha:** Exporte imediatamente os logs de firewalls, proxies, VPNs e servidores para repositórios seguros.
- **Prevenção contra Limpeza:** Atacantes frequentemente tentam apagar rastros locais (Event Logs / syslog) durante a intrusão.

Sincronização Temporal (NTP)

- **Correlação de Eventos:** Valide a precisão de timestamps em todos os ativos envolvidos no incidente.
- **Linha do Tempo (Timeline):** Crucial para reconstrução exata da cadeia de eventos e movimentação lateral.

3. Custódia & Integridade

CADEIA DE CUSTÓDIA

Geração e Guarda de Hashes

- **Integridade Criptográfica:** Calcule e registre imediatamente os hashes (SHA-256) de todas as imagens de memória e arquivos coletados.
- **Não Repúdio:** O hash garante que a evidência não sofreu alterações desde o momento de sua extração.

Documentação da Coleta

- **Registro de Custódia:** Formalize quem coletou, data, hora, ferramentas utilizadas e local de armazenamento seguro.
- **Armazenamento Imutável:** Guarde as evidências em mídias de leitura única ou repositórios protegidos contra gravação.

Validade Legal e Pericial

- **Conformidade:** Alinhamento com padrões ISO/IEC 27037 para tratamento de evidências digitais.
- **Suporte a Auditoria:** Assegura que o material seja aceito em investigações internas, governamentais ou judiciais.

Prof. Dr. Rafael Freitas Reale

rafael.reale@previdencia.gov.br
linkedin.com/in/rafaelreale/

OLRO

nic.br

Q13

Webfoco
TECH

XSITE
kaspersky

PRATA

InforTel

PRONTE

DISTRITO
engenharia

PARANÁ ROBERT

KALAXI
SISTEMAS

IMTECH

infor
barra

PROBAHIA
Proteção Patrimônio & Acesso à Informação

SOFTDADOS

OPRO

cais

ESCOLA
SUPERIOR
DE REDES

nic.br

UFBA
Universidade Federal da Bahia

REMESSA

REALIZAÇÃO

PopBA

RNP

MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

AGÊNCIA, TECNOLOGIA
E INOVAÇÃO

