PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Instituto de Ciências Exatas e de Informática

Infraestrutura de TI como Pilar Estratégico para a Expansão Cooperativa

Gabriel Freitas de Oliveira

Helberth Alencar Diniz Martins

Ian Benevides de Abreu

Nathan de Mesquita dos Santos

Rafael Moreira Arantes de Castro

Vitoria Lorrayne dos Santos Soares

Orientador: Alexandre Teixeira

Resumo

O presente trabalho detalha o projeto de infraestrutura de redes para a cooperativa bancária COOPGO em seu processo de expansão geográfica. Aborda-se o problema da instabilidade da rede, da segurança de dados e do baixo desempenho na comunicação entre a matriz e as filiais, cuja justificativa reside na necessidade crítica de garantir a continuidade e a eficiência das operações por meio de uma rede robusta. Buscou-se, como objetivo, desenvolver uma infraestrutura de redes escalável e de alta disponibilidade. Para isso, desenvolveu-se uma arquitetura híbrida com a configuração de um servidor local Windows Server, uma Virtual Private Cloud (VPC) na AWS e a implementação da ferramenta Zabbix para monitoramento. Como resultado, obteve-se uma infraestrutura estável, cujos indicadores de desempenho dos servidores foram validados pelo monitoramento contínuo. Conclui-se que a solução implementada atende aos requisitos de estabilidade, segurança e escalabilidade, fornecendo uma base sólida para o crescimento futuro da cooperativa.

Palavras-chave: infraestrutura de redes; computação em nuvem; aws; windows server; segurança da informação; zabbix.

Abstract

This work details the network infrastructure project for the COOPGO banking cooperative during its geographical expansion process. It addresses the problem of network instability, data security, and low performance in communication between the headquarters and branches, justified by the critical need to ensure the continuity and efficiency of operations through a robust network. The objective was to develop a scalable and high-availability network infrastructure. To achieve this, a hybrid architecture was developed by configuring a local Windows Server, a Virtual Private Cloud (VPC) on AWS, and implementing the Zabbix tool for monitoring. As a result, a stable infrastructure was obtained, with server performance indicators validated by continuous monitoring. It is concluded that the implemented solution meets the requirements for stability, security, and scalability, providing a solid foundation for the cooperative's future growth.

Keywords: network infrastructure; cloud computing; aws; windows server; information security; zabbix.

---

*Artigo apresentado ao Instituto de Ciências Exatas e Informática da Pontifícia Universidade Católica de Minas Gerais, campus Contagem, como pré-requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

[1]Ian Benevides de Abreu - Aluno do Programa de Graduação em Sistemas de Informação – ian.abreu.1449254@sga.pucminas.br
Gabriel Freitas de Oliveira - Aluno do Programa de Graduação em Sistemas de Informação - gabriel.oliveira.1265286@sga.pucminas.br
Helberth Alencar Diniz Martins - Aluno do Programa de Graduação em Sistemas de Informação - helberth.martins@sga.pucminas.br
Vitoria Lorrayne dos Santos Soares - Aluna do Programa de Graduação em Sistemas de Informação - vitoria.lorrayne@sga.pucminas.br
Nathan de Mesquita dos Santos - Aluno do Programa de Graduação em Sistemas de Informação - nathan.mesquita@sga.pucminas.br
Rafael Moreira Arantes de Castro - Aluno do Programa de Graduação em Sistemas de Informação - rafael.arantes@sga.pucminas.br

[2]Alexandre Teixeira - Professor(a) do Programa de Graduação em Sistemas de Informação – teixeira@sga.pucminas.br

1. INTRODUÇÃO

O presente artigo descreve o projeto e a implementação de uma infraestrutura de redes de computadores para uma organização fictícia, denominada Cooperativa Bancária COOPGO, criada exclusivamente para fins acadêmicos. A COOPGO representa uma instituição financeira cooperativa em fase de expansão estratégica. No contexto proposto, foi fundada em Uberaba, no ano de 2022, com o objetivo de aliar justiça social e prosperidade econômica, princípios que contribuíram para um crescimento expressivo e a decisão de inaugurar três novas filiais.. Este cenário, contudo, impõe desafios tecnológicos significativos, pois a sustentabilidade deste crescimento depende de uma comunicação de dados eficiente, segura e resiliente entre a matriz e as novas unidades. A infraestrutura de TI atual, concebida para uma única localidade, mostra-se inadequada para o novo modelo multibranch, apresentando problemas como alta latência, ausência de redundância efetiva e múltiplos pontos únicos de falha. A questão que este projeto busca responder, portanto, é: qual a arquitetura de rede mais adequada para interligar a matriz e as filiais, solucionando os problemas atuais e fornecendo uma plataforma escalável para o futuro?

A resolução desta questão é crítica e urgente, justificando-se como um investimento estratégico para a cooperativa. Uma infraestrutura instável representa um risco direto à eficiência operacional, à conformidade regulatória (LGPD e normativas do Banco Central) e à reputação da COOPGO. A implementação de uma rede robusta, por outro lado, mitiga esses riscos, otimiza processos internos e habilita a inovação, fortalecendo a governança corporativa. Diante disso, o objetivo geral deste projeto é desenvolver e implementar uma infraestrutura de redes que seja robusta, segura, escalável e de alto desempenho. Para alcançar este propósito, foram estabelecidos os seguintes objetivos específicos:

Garantir Alta Disponibilidade, implementando mecanismos de redundância para evitar pontos únicos de falha.

Otimizar o Desempenho, utilizando técnicas de balanceamento de carga e otimização de tráfego de rede (QoS).

Assegurar a Escalabilidade, projetando uma arquitetura modular que permita a fácil adição de novas filiais ou serviços.

Centralizar o Gerenciamento e Monitoramento, implementando ferramentas como o Zabbix para visibilidade completa da rede.

Fortalecer a Segurança da Informação, aplicando uma Política de Segurança robusta, firewalls e gestão de acessos baseada no princípio do menor privilégio.

Para apresentar de forma clara o desenvolvimento e os resultados deste projeto, este relatório foi organizado em seções sequenciais. Após esta introdução, a seção de Metodologia e Desenvolvimento descreve os procedimentos técnicos adotados. Em seguida, a seção de Gerência e Monitoramento apresenta os resultados práticos da implementação. A seção sobre Mecanismos de Segurança detalha a política e a governança criadas, e, por fim, a Conclusão sintetiza os achados e aponta os próximos passos.

2. METODOLOGIA E DESENVOLVIMENTO

Esta seção descreve os procedimentos técnicos e as etapas de implementação da infraestrutura. A abordagem adotada foi a de um estudo de caso, aplicando conceitos de virtualização e computação em nuvem para construir uma solução funcional e adaptada às necessidades da COOPGO.

2.1 Visão Geral do Projeto de Rede

O projeto de rede da COOPGO foi estruturado no simulador Cisco Packet Tracer para atender às necessidades de conectividade, desempenho e segurança das operações entre a matriz (em Uberaba) e suas três filiais localizadas em Ituiutaba, Monte Carmelo e Frutal. A topologia contempla a segmentação lógica da rede em VLANs, para isolar diferentes tipos de tráfego, e a utilização de conexões ponto-a-ponto entre as unidades, garantindo uma comunicação direta e segura. Além disso, a arquitetura foi organizada por departamentos e serviços críticos, como servidores de autenticação, sistemas internos e a infraestrutura de rede, estabelecendo uma base sólida para a implementação física e em nuvem.

2.2 Ambiente de Virtualização Local

O ambiente local foi configurado utilizando o Windows Server 2012. O servidor, nomeado Server01, foi promovido a Controlador de Domínio com o domínio coopgo.net. Dentro do Active Directory, foram criadas Unidades Organizacionais (OUs) para a Matriz e cada uma das filiais, permitindo a organização de usuários e computadores. Foi estabelecida uma Política de Grupo (GPO) para restringir o acesso dos usuários ao Painel de Controle e às configurações do sistema, aumentando a segurança e a padronização dos ambientes de trabalho.

2.3 Infraestrutura em Nuvem (Cloud)

A plataforma Amazon Web Services (AWS) foi utilizada para a implementação dos serviços em nuvem.

2.3.1 Virtual Private Cloud (VPC)

Foi configurada uma VPC (ID: vpc-0820bbeceee8b032b) na região us-east-1 (Norte da Virgínia) com o bloco de endereçamento CIDR 10.0.0.0/16. Dentro desta VPC, foi criada uma sub-rede pública (Matriz-subnet-public1-us-east-1a) com o CIDR 10.0.0.0/20. Um Internet Gateway (Matriz-igw) foi associado à VPC e uma tabela de rotas foi configurada para direcionar o tráfego externo, permitindo que os recursos na sub-rede pública acessem a internet.

2.3.2 Segurança da VPC

Um Grupo de Segurança (Security Group) denominado Matriz foi criado e associado à VPC. Foram configuradas regras de entrada (inbound rules) para permitir o tráfego nos protocolos HTTP (porta 80) e RDP (porta 3389) a partir de qualquer endereço IPv4 (0.0.0.0/0), viabilizando o acesso web e remoto ao servidor.

2.3.3 Instância EC2

Um servidor virtual foi provisionado por meio de uma instância EC2, denominada MatrizServer. A imagem utilizada foi o Windows Server 2016 com o tipo de instância t2.large. O servidor foi alocado na VPC e associado ao grupo de segurança previamente criado, recebendo o endereço IP público 44.195.41.154 para acesso externo.

3. GERÊNCIA E MONITORAMENTO (RESULTADOS)

Para monitorar continuamente a saúde e o desempenho dos servidores local e em nuvem, foi implementada a ferramenta Zabbix. Esta seção apresenta os resultados obtidos por meio do monitoramento.

3.1 Monitoramento do Servidor na Nuvem (MatrizServer)

Os dados coletados do servidor EC2 na AWS indicam uma operação estável. Os gráficos demonstram que o uso de espaço em disco, a utilização da CPU e as métricas de conectividade estão dentro dos parâmetros esperados, sem apresentar anomalias ou sobrecargas.

Gráfico de uso de disco do servidor na nuvem

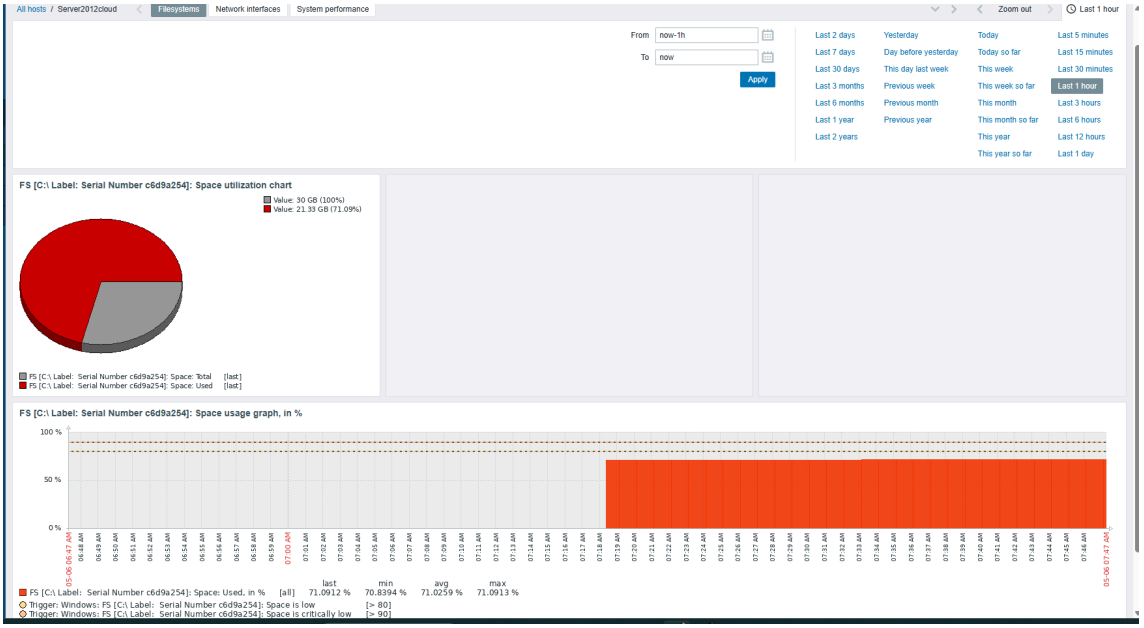

Gráfico de uso de CPU do servidor na nuvem

Gráfico de conectividade do servidor na nuvem

3.2 Monitoramento do Servidor Local (Server01)

O servidor local também apresentou desempenho estável, com o uso de disco e de CPU mantendo-se em níveis baixos, indicando que o hardware atual é suficiente para a carga de trabalho. As métricas de conectividade confirmam que a rede local opera sem interrupções.

Gráfico de uso de disco do servidor Local

Gráfico de uso de CPU do servidor Local

Gráfico de conectividade do servidor Local

4. MECANISMOS DE SEGURANÇA DA INFORMAÇÃO

Para fortalecer a cultura de segurança e formalizar as práticas na cooperativa, foram desenvolvidos dois documentos essenciais.

4.1 Política de Segurança da Informação (PSI)

OBJETIVO

Estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, protegendo as informações da instituição, dos clientes e do público em geral, observando as melhores práticas de mercado e regulamentações aplicáveis.

PÚBLICO-ALVO

Todos aqueles que interagem com a informação da COOPGO, seja internamente ou externamente. Isso engloba todos os colaboradores, prestadores de serviço, clientes, parceiros, acionistas e até visitantes que possam ter acesso aos sistemas e dados da empresa.

A informação é o principal ativo da COOPGO. Assim, ficou definida a estratégia de segurança da Informação para proteção da integridade, disponibilidade e confidencialidade da informação. Esta estratégia é baseada na detecção, prevenção, monitoramento e resposta a incidentes e busca fortalecer a gestão do risco de segurança cibernética e a construção de uma base sólida para o melhor ambiente digital.

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Na COOPGO, temos o compromisso com o tratamento adequado das informações dos nossos clientes e público em geral, sendo fundamentado nos seguintes princípios:

Confidencialidade: garantir que o acesso à informação seja obtido somente por pessoas autorizadas;

Disponibilidade: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;

Integridade: garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

DIRETRIZES

Todos os documentos de segurança da informação (política, regras e procedimentos) devem estar disponíveis em local acessível aos colaboradores e protegidos contra alterações.

A Política Corporativa de Segurança da Informação é revisada anualmente pela COOPGO com aplicação para todos colaboradores e protegidos contra alterações.

A inclusão de diretrizes ou eventuais alterações serão identificadas e realizadas pelo responsável pela segurança da informação da COOPGO, que deverá formalizar e submeter de forma prévia a proposta de diretrizes ou exceções para aprovação pela Diretoria de Segurança Corporativa da COOPGO.

A adesão a essa Política e eventuais falhas são reportados periodicamente pela Diretoria de Segurança Corporativa aos comitê gestor da COOPGO.

A informação deve ser utilizada de forma transparente, para as finalidades informadas ao cliente e de acordo com a legislação vigente, conforme descrito em políticas internas.

As diretrizes e eventuais exceções são complementadas em procedimentos com regras específicas que devem ser observadas.

PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

As violações a esta política estão sujeitas às sanções disciplinares previstas em documento interno, bem como nas normas internas da COOPGO.

a) Gestão de Ativos: Entende-se por ativo, tudo aquilo que a instituição considerar como relevante para o negócio. Os ativos tecnológicos devem ser identificados, inventariados, atualizados, possuir um proprietário, descartados de forma segura e protegidos contra acessos indevidos.

b) Classificação da Informação: As informações devem ser classificadas de acordo com a confidencialidade, considerando as necessidades do negócio e os impactos de seu uso indevido durante todo o seu ciclo de vida (Geração, Manuseio, Armazenamento, Transporte e Descarte).

c) Gestão de Acessos: Os acessos devem ser rastreáveis, obedecer ao critério de menor privilégio e garantir a segregação de funções. A identificação do colaborador é única e intransferível, e as senhas são confidenciais. As revisões de acesso devem ser contínuas.

d) Segurança Física do Ambiente: O acesso físico aos ambientes é controlado de acordo com a criticidade das informações, utilizando recursos como crachás, senhas e biometria, além do controle de entrada e saída de equipamentos e pessoas.

e) Conscientização em Segurança da Informação: A COOPGO promove a disseminação dos princípios de segurança por meio de programas contínuos de conscientização e capacitação.

f) Identificação: O acesso aos sistemas corporativos exige que o usuário seja identificado, autenticado e autorizado, com todas as ações passíveis de auditoria.

g) Uso de dispositivos: É proibida a conexão de dispositivos particulares não homologados pela COOPGO à rede corporativa.

h) Correio eletrônico: Os recursos de e-mail corporativo são monitorados e devem ser utilizados para fins profissionais.

i) Senhas: As senhas são individuais, intransferíveis e devem seguir regras de complexidade.

j) Software: Todos os softwares devem ser licenciados e sua instalação autorizada pela COOPGO.

SEGURANÇA CORPORATIVA

Aprimorar a qualidade e efetividade de seus processos, buscando a integridade, disponibilidade e confidencialidade das informações.

Proteger a informação de ameaças buscando garantir a continuidade do negócio.

Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do Sistema de Gestão Integrado (SGI).

Definir e formalizar os objetivos, controles e a estratégia de governança de segurança.

Coordenar e disseminar uma cultura de segurança da informação.

Propor investimentos e definir políticas, padrões e controles mínimos de segurança.

PAPÉIS E RESPONSABILIDADES

Colaborador: Cumprir esta política e os demais instrumentos regulamentares.

Tecnologia da Informação: Propor soluções e manter o patrimônio tecnológico disponível e atualizado.

Área de Negócio: Proteger as informações sob sua responsabilidade.

Gerência de Tecnologia: Segregar funções, monitorar o ambiente, configurar equipamentos, coordenar incidentes e auxiliar o Encarregado pela Proteção de Dados.

Gerência (demais áreas): Zelar pelas informações produzidas por sua equipe e fazer cumprir as diretrizes desta política.

DECLARAÇÃO DE RESPONSABILIDADE

Periodicamente os colaboradores da COOPGO devem aderir formalmente a um termo de responsabilidade. Os contratos firmados com a COOPGO devem possuir cláusula de confidencialidade.

SANÇÕES DISCIPLINARES

As violações a esta política estão sujeitas às sanções disciplinares previstas em documento interno, bem como nas normas internas da COOPGO.

REGULAMENTAÇÕES

Resolução CD/ANPD n.º 20/2024;

Decreto nº 7.724, de 2012 (Regulamenta a Lei de Acesso à Informação - LAI);

Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018;

ABNT NBR ISO/IEC 27701:2019;

Resolução 4.893 do Banco Central;

Resolução nº 85 do Banco Central;

Resolução 4.752 do Banco Central.

4.3 Análise de Vulnerabilidades da Aplicação

Com o objetivo de mapear potenciais riscos que podem ocorrer na aplicação da cooperativa, foi realizada uma análise teórica de vulnerabilidades com base nas categorias do OWASP Top 10.

A07:2021 – Falhas de Identificação e Autenticação: Conhecida como Autenticação Quebrada, esta vulnerabilidade está relacionada a falhas nos mecanismos de confirmação de identidade do usuário. No contexto da aplicação da COOPGO, um risco potencial seria o armazenamento de senhas em texto simples ou com algoritmos de hash fracos, bem como a ausência de uma autenticação multifator (MFA) eficaz, o que poderia permitir que invasores contornem os processos de login.

A09:2021 – Falhas de Monitoramento e Registro de Segurança: Esta categoria visa auxiliar na detecção, escalonamento e resposta a violações ativas. A aplicação da COOPGO estaria vulnerável se não possuísse um sistema robusto de registro de eventos (logs) e monitoramento contínuo. Como consequência, ataques ou violações de segurança poderiam não ser detectados a tempo, impedindo uma resposta rápida ao incidente e a análise forense.

A02:2021 – Falhas Criptográficas: Esta categoria trata da proteção inadequada de dados sensíveis em repouso (armazenados) ou em trânsito (durante a comunicação). Um risco para a aplicação seria não utilizar criptografia para proteger dados sensíveis armazenados no banco de dados, como informações pessoais e financeiras, ou não adotar o protocolo HTTPS em todas as comunicações. Como consequência, esses dados poderiam ser interceptados ou acessados por terceiros mal-intencionados, comprometendo a confidencialidade e a integridade das informações.

5. CONCLUSÃO

Este trabalho apresentou o desenvolvimento de uma infraestrutura de redes híbrida, integrando recursos locais e em nuvem para atender às demandas de expansão da cooperativa COOPGO. A solução implementada demonstrou ser robusta, segura e escalável, alcançando os objetivos propostos de garantir alta disponibilidade e desempenho otimizado. A combinação do Active Directory local com os serviços da AWS, gerenciada e monitorada pelo Zabbix, oferece uma base tecnológica sólida para o futuro da cooperativa. Como trabalhos futuros, sugere-se a implementação de uma VPN Site-to-Site para aumentar a segurança na comunicação entre a matriz e a nuvem, bem como a realização de testes de penetração para validar as defesas implementadas.

6. REFERÊNCIAS

AMAZON WEB SERVICES. Documentação do Amazon EC2 para instâncias do Windows. Seattle: AWS, 2025. Disponível em: https://docs.aws.amazon.com/pt_br/AWSEC2/latest/WindowsGuide/Welcome.html. Acesso em: 17 jun. 2025.

AMAZON WEB SERVICES. O que é uma Amazon VPC?. Seattle: AWS, 2025. Disponível em: https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/what-is-amazon-vpc.html. Acesso em: 17 jun. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27701: Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

BANCO CENTRAL DO BRASIL. Resolução CMN nº 4.893, de 26 de fevereiro de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras. Brasília, DF: Diário Oficial da União, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Diário Oficial da União, 2018.

MICROSOFT. Documentação do Windows Server 2012. Redmond: Microsoft, 2025. Disponível em: https://learn.microsoft.com/pt-br/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831766(v=ws.11. Acesso em: 17 jun. 2025.

ZABBIX. Documentation Zabbix. Riga: Zabbix SIA, 2025. Disponível em: https://www.zabbix.com/documentation/current/en. Acesso em: 17 jun. 2025.