RELATÓRIO DE MELHORIAS EM CONEXÕES REMOTAS

Nome:	Inan Brunelli Brandão RA: 0040971521018
Disciplina:	Projeto de Trabalho de Graduação
Semestre:	6° Semestre Noturno

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

B817r BRANDÃO, Inan Brunelli

Relatório de melhorias em conexões remotas. / Inan Brunelli Brandão. – Americana, 2019.

25f.

Relatório técnico (Curso Superior de Tecnologia em Segurança da Informação) -- Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Esp. Juliane Borsato Beckedorf Pinto

1 Transmissão de dados 2. Auditoria em sistemas de informação I. PINTO, Juliane Borsato Beckedorf II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.519

681.518.3

Faculdade de Tecnologia de Americana

Inan Brunelli Brandão

Relatório de Melhorias em Conexões Remotas

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.
Área de concentração: Desenvolver e implementar política de segurança da informação.

Americana, 04 de dezembro de 2019.

Banca Examinadora:

Juliane Borsato Beckedorff Pinto
Especialista
FATEC Americana

Renato Kraide Soffner
Doutor
FATEC Americana

Vagner Ferreira
Mestre
FATEC Americana

SUMÁRIO

1 INTRODUÇÃO

Neste documento foi abordado etapas de segurança da informação visando a restruturação das políticas de segurança, colocando em prática o conhecimento aprendido durante o curso de segurança da informação.

1.1 METODOLOGIA

A realização dessa implementação foi feita em diferentes etapas, utilizando recursos profissionais, no qual foi iniciado com uma varredura em todas as formas de conexões e políticas de segurança relacionadas a elas, reconhecendo o cenário para criação de um escopo de necessidades deste estudo.

Dando início às validações, fazendo um inventário dos ativos e todas as políticas atuais de segurança da informação.

Após a realização da análise, foi desenvolvido um relatório com a criticidade de cada tópico e apresentado um plano de ação para que seja realizado, dando alternativas dependendo da gravidade de cada ponto relatado.

Foi sugerido ferramentas para aplicação das correções de cada tópico escolhido, levando em consideração o objetivo de cada um deles.

Como conclusão, foi sugerida uma nova política de utilização de conexões, baseada nas informações adquiridas dentro da empresa na qual foi aplicada para que possa ter um resultado maior e contínuo das aplicações de correção.

1.2 OBJETIVO

Este relatório tem como objetivo, dentro de um escritório de contabilidade, mostrar as possíveis melhorias que podem ser implementadas na estrutura, visando o aumento na segurança de conexões remotas, além de fácil utilização pelos usuários, para ter uma comunicação interna melhor, viabilizando a atualização de ferramentas de acessos obsoletas, das políticas de segurança da informação e todo o cenário atual no qual se relaciona com o acesso de redes internas e externas.

2 DESENVOLVIMENTO

Antes da realização das reais mudanças em todos os processos relacionados a conexões remotas dentro da empresa, foi realizado um processo de auditoria.

Uma auditoria nada mais é que a revisão e demonstração de todos os passos de algum processo específico, que em no caso deste trabalho é todos os meios de conexões remotas utilizadas.

Segundo Brunner (2017), auditoria em TI categoriza-se como:

> "Dentre as funções de uma auditoria, as principais consistem em avaliar os sistemas que a empresa adota a fim de proteger as informações da organização, preservar seus ativos e distribuir os dados, apontando eventuais desvios e vulnerabilidades. Oferecer alternativas de soluções para esses diversos problemas também é parte do processo".

Com a finalidade de entender como funcionavam as formas de acesso remoto, a auditoria trás consigo as deficiências que eventualmente podem aparecer em alguma parte do processo, deixando muito mais claros os pontos falhos a serem trabalhados.

2.1 REALIZAÇÃO DA AUDITORIA

A revisão das demonstrações dos passos que um usuário precisa seguir para fazer uma conexão foi feita com o objetivo de identificar todos os padrões de segurança que a empresa tem em relação as suas conexões, além de revisar se há documentos provando que suas atividades seguem um padrão pré-estabelecido.

Após a realização da auditoria, foi registrado um maior número de detalhes, com o objetivo de buscar alguma falha ou deficiência em alguma parte do processo.

Com esses padrões (ou a falta deles), foi identificado que a empresa não tinha sequer nenhum padrão de conexão, pois suas operações não eram bem definidas, levando muitas vezes a inconsistência na troca de informações, gerando a necessidade de reestruturação do ambiente lógico da empresa.

Um ambiente lógico categoriza-se por ser composto por aplicativos, dados, sistemas operacionais, senhas, e todos os dispositivos não palpáveis de um computador, sendo toda parte de *software* de uma máquina.

2.2 APRESENTAÇÃO DA EMPRESA

A empresa CRG Gestão foi fundada em 11 de Dezembro de 2014, na cidade de Piracicaba-SP, pelos senhores Israel Efraim Guimarães, Lucas Castro de Oliveira e a senhora Ana Paula Romano.

Atualmente contam com 14 funcionários, sendo seus principais clientes: Atacado Brasil, Supermercado Sete, Supermercado Guidolin, Supermercado Andrade, Supermercado Ideal, entre outros.

Em seus clientes, exercem o papel de auditar toda a parte de contabilidade, fiscal e recursos humanos que englobam seus processos. Além de prestar um grande papel na demonstração de resultados dos três pilares citados anteriormente, para que seus colaboradores entendam quais são seus pontos fortes e fracos.

Com um grande vínculo com a tecnologia da informação, fugindo dos padrões de escritórios contábeis, e partindo para a automação de tarefas manuais, com o desenvolvimento de um *software* próprio, evitando a sobrecarga de funcionários tanto na própria CRG, quanto em seus clientes.

Sua missão é mover-se e desenvolver-se sob as primícias de entender seus clientes e mensurar os resultados de forma confiável, ágil e em alta performance, além de viver conectado em todo tempo com as informações e atualidades, respeitando a ética profissional para proporcionar uma visão integrada com crescimento sustentável ao negócio.

2.3 AMBIENTE DA EMPRESA

Por meio da segurança da informação, serão os métodos aplicados, visando à proteção do ambiente lógico e físico, com foco maior em preservar a disponibilidade, integridade e confidencialidade (CID) de todos os processos envolvendo tecnologia.

A empresa CRG tinha um grande déficit em relação ao CID, pois quando a empresa surgiu, esta não foi projetada para suportar problemas relacionados à segurança da informação.

Para manter todo o ambiente da empresa estável e seguro, foi estabelecido que os três pilares da segurança da informação deveriam ser atingidos.

> Disponibilidade: a informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão.
>
> Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.
>
> Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia (FONTES, 2010, p. 26).

Com isso, após a estrutura tecnológica desta empresa aumentar gradativamente com o tempo, começaram a surgir problemas que não foram previstos anteriormente.

Levando em consideração que nenhum destes pilares estavam sendo cumpridos, para sanar os problemas básicos relacionados a segurança na informação, foi implementado o CID.

2.3.1 VISÃO DO PROJETO

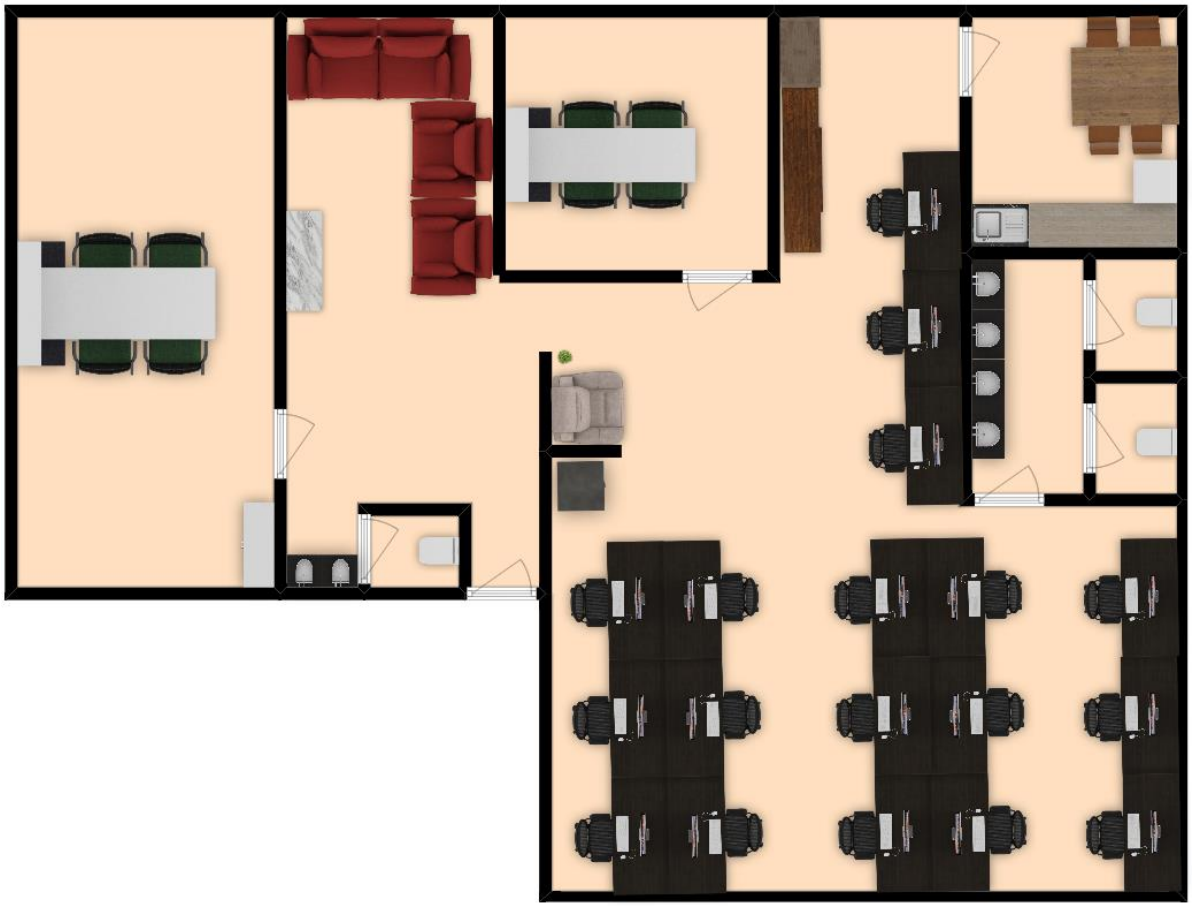
Pensando em integridade para o cenário deste projeto, a consistência da informação é extremamente importante, pois é necessário que os dados obtidos sejam consistentes e precisos, pois não pode haver percas de informações em qualquer parte das atividades.

Sendo a disponibilidade relacionada diretamente a garantia ao acesso das informações precisa ser mantida, a qualquer momento que o usuário precise, mantendo todas as conexões disponíveis em qualquer momento que o usuário deseje, podendo ser utilizada de qualquer lugar.

Levando em consideração a confidencialidade, as conexões devem se manter seguras, pois nenhum terceiro deve ter informações aos arquivos que estão sendo transferidos ou/e gerados através desses acessos.

2.3.2 PLANTA BAIXA

Figura 1: planta baixa da empresa.



Fonte: dados da empresa.

O ambiente da empresa é composto por cinco cômodos, sendo eles:

- Sala de Reunião;

- Recepção;
- Sala particular;
- Ambiente de escritório;
- Cozinha;

2.4 ANÁLISE

Antes da aplicação de qualquer mudança significativa, foi necessário analisar com cuidado todos os pontos fracos em relação às conexões, para que se possa aplicar as alterações de forma mais objetiva, focando nas atividades que estavam falhas na utilização da rede.

Para que possa ser realizada qualquer auditoria, é necessário possuir um ponto de direção a ser tomado, de forma que as avaliações de toda a rede da empresa e suas conexões sejam feitas corretamente.

2.4.1 CHECKLIST

Será seguido um *checklist* com objetivo de traçar os pontos importantes a serem feitos em todo o projeto, levando em consideração todos os dados obtidos anteriormente.

Assim, com os objetivos pré-definidos, deixa-se claro para todos os envolvidos, sendo eles colaboradores da empresa CRG ou/e funcionários dos clientes, no qual foi o intuito da reestruturação da segurança em conexões remotas.

Os critérios de segurança de conexões para este ambiente, foram os seguintes:

1) VPN

VPN ou Rede Privada Virtual nada mais é que um método para conectar dois computadores através de uma rede pública, como a internet. Levando em consideração que é necessário segurança lógica ao trocar informações na internet, uma das formas de segurança que a VPN disponibiliza é a criptografia, que apenas o emitente e destinatário tem acesso a informação, sem nenhuma perca de dados na comunicação entre dois pontos.

Outra definição que poderia ser dada, segundo Tanenbaum (2003):

> As VPNs (Virtual Private Networks) ou redes virtuais privadas são redes sobrepostas às redes públicas, tendo as mesmas características. São chamadas “virtuais” por que são uma ilusão, os circuitos virtuais não são circuitos reais e que a memória virtual não é memória real.

Este tipo de conexão utiliza um meio de comunicação chamado tunelamento, que tem o mesmo objetivo da criptografia: apenas o emitente e destinatário tem acesso à informação, quem não está em algum desses dois pontos, não tem permissão de acesso a esses dados.

Levando em consideração que todo o projeto ganha um maior nível de segurança com a utilização de VPN, pois quando a conexão é estabelecida, todas as informações que estão sendo trocados entre esses dois pontos estão seguras por meio de uma criptografia altamente confiável.

Com isso, a VPN, neste cenário, é o melhor meio de conexão atual para esta empresa, pois como não haverá um grande número de usuários e sua velocidade depende da internet utilizada no momento da conexão, não terá problemas de usuários se desconectando frequentemente, além de ser uma ferramenta de baixo custo.

Ao comparar os meios de conexões remotas na empresa antes da implantação do projeto, foi identificado uma série de problemas que impactava na velocidade de trabalho de todos os colaboradores que utilizavam desses métodos de conexão.

Como nenhum método de conexão era adotado como padrão para estabelecer conexão remota sobre a área de trabalho do cliente, era utilizado qualquer ferramenta que fosse disponibilizada pelo mesmo, sem nenhum questionamento em relação à segurança, estabilidade e velocidade desse meio de conexão.

Não existia nenhum controle de atualização de *software*, o que acarretava a necessidade de *download* de várias versões da ferramenta de conexão utilizada, até as duas estações estarem com a mesma versão entre elas, possibilitando a compatibilidade, e assim, a conexão remota.

Todas as ferramentas eram utilizadas de suas versões gratuitas, o que disponibilizava uma ferramenta mais ‘básica’ em relação a um pacote de usuários deste mesmo *software*, que vinha com uma série de limitações em suas conexões, como por exemplo:

- Tempo limitado de conexão remota;
- Não há nenhum controle de log de conexões estabelecidas;
- Apenas uma conexão simultânea;
- Não há suporte a ferramenta de conexão remota.

Algumas destas ferramentas possibilitam escolher a opção de modo ‘uso particular’, ou ‘uso empresarial’, porém a utilização destes *softwares* era feita de forma particular, mesmo sendo uma empresa, podendo acarretar em problemas judiciais.

Em relação às conexões remotas estabelecidas para acessar a rede da empresa CRG, o maior problema identificado foi à falta de segurança em suas conexões, pois os *softwares* de conexões remotas ficavam sendo executadas 24 horas por dia no próprio servidor de aplicação da empresa, mantendo uma senha fixa nessas ferramentas.

Essas conexões não tinham nenhum tipo confirmação de identidade necessária ao acessar a rede da empresa, além de não manter nenhum registro de qual usuário acessou a rede e o que fez nela.

2) Cadastro de usuário

Um problema que a empresa enfrentava era a queda frequente de conexão remota, pois a quantidade de usuários para se conectar a uma rede era menor que a quantidade de funcionários.

Como havia uma grande carência no controle de usuários para acesso a conexões remotas, estas eram estabelecidas de forma aleatória, sem nenhuma requisição pré-definida ou agendada.

Quando algum usuário se conectava a uma estação de trabalho e outro usuário perdia a conexão pois estava conectado a esta mesma estação, estes dois colaboradores ficavam cortando a conexão um do outro, não deixando fluir o trabalho de nenhum dos dois.

3) Controle de acesso

Controle de acesso se define como o que cada usuário tem direito de acesso na rede, incluindo as permissões de leitura, modificação, adição e exclusão de arquivos.

Como várias pessoas utilizavam um mesmo usuário para fazer conexão remota a um determinado computador, não havia nenhum controle de permissão pré-estabelecido.

Qualquer usuário poderia excluir um arquivo importante do cliente ou instalar algum tipo de *malware*, sem que ninguém saiba exatamente quem foi a pessoa que executou esta ação.

Quando havia uma conexão remota que era estabelecida em algum computador do cliente, seu banco de dados estava totalmente aberto para

fazer qualquer alteração que o usuário queira, e isto poderia ter como consequência um grande número de informações em risco.

4) Segurança

RDP (Remote Desktop Protocol) é um protocolo que possibilita o usuário acessar remotamente outro computador através de um terminal service, interligados entre si por uma rede, que no caso deste projeto, a VPN daria acesso a mesma rede.

Tendo isto em vista, um terminal service é uma ferramenta Microsoft que possibilita um meio de conexão entre dois computadores que estão em uma mesma rede, possibilitando a troca de informações entre eles.

5) Segurança

Levando em consideração que um grande número de ataques a redes privadas atualmente é causado pela falta de conhecimento básico dos utilizadores desta infraestrutura, foi adotada uma política de treinamento mensal para todos os usuários da empresa, como forma de conscientização.

Dando conhecimento básico e estes, a tendência de roubo de informações é muito menor, porque a maior parte de trocas de dados é feita através destes usuários.

No cenário antigo, não havia nenhum conhecimento por parte dos usuários sobre os prováveis perigos que uma má utilização de uma conexão remota poderia causar tanto para o cliente quanto para a empresa.

Como exemplo disso, é a forma que os usuários mantinham controle dos acessos: era feito uma planilha excel na máquina local do usuário, sem nenhum tipo de senha ou criptografia, com os logins e senhas contendo as conexões de todos os clientes.

Caso está planilha fosse acessada por usuários maus intencionados, poderia causar um impacto gigantesco nas informações de todos os clientes.

6) Antivírus e *Firewall*

Com a utilização de antivírus e *firewall*, há um filtro de pacotes que está entrando e saindo da rede da empresa, agindo como uma ‘peneira’, tratando as informações que tem um potencial de serem nocivas para a infraestrura.

Como estes recursos era utilizados sem nenhum controle e até mesmo não utilizados (como em algumas máquinas de funcionários não havia antivírus), a maioria dos ganhos que estas ferramentas proporcionam não estavam sendo aplicadas a rede lógica da empresa.

Os antivírus utilizados eram *softwares* gratuitos, que não atendiam todas as necessidades da empresa, pois estas versões tendem ser mais básicas que suas versões pagas.

Com isso, as consequências do uso de um antivírus ineficiente era o aumento de risco, como ataques, contaminação de vírus ou roubo de dados.

Já o *firewall* não era atualizado constantemente nos computadores que acessavam a rede interna da empresa, causando assim uma abertura no tráfego de saída de dados, o que pode gerar em uma contaminação de um vírus em toda a rede, mesmo com a utilização de um antivírus.

7) Senhas criptografadas

Para não ter problemas de algum funcionário utilizando usuário de outro colaborador, todos os utilizadores da rede da empresa têm acesso a um usuário, evitando o conflito, além da segurança em suas senhas, evitando o roubo delas.

Como não eram utilizados estes recursos para salvar as informações dos usuários, como resultado havia uma falta de segurança das informações, onde vários usuários utilizavam as mesmas credenciais, perdendo total controle de ações de cada indivíduo.

2.4.2 EXECUÇÃO DO CHECKLIST

Será aplicado um *checklist* com base na infraestrutura computacional da empresa, além da quantidade de conexões simultâneas, onde será selecionado apenas os tópicos cabíveis a este ambiente. Por se tratar de uma empresa com uma rede computacional de pequeno porte, onde o ramo de contabilidade não é voltado à área de TI, a adaptação trará agilidade no momento da realização da auditoria, contendo somente os tópicos aplicáveis as suas formas de conexões e sua política de segurança. Com isso a clareza dos resultados trará agilidade e foco na implementação do projeto.

Utilizando o relatório contendo o escopo da empresa e suas necessidades, iniciou-se o processo de aplicação do *checklist* no ambiente do cliente, visando analisar as formas de conexões e políticas de segurança da informação.

2.5 RELATÓRIO DE CRITICIDADE

A criticidade de ativos nada mais é que uma maneira de organizar os ativos nos quais tem papéis mais importantes no negócio. Sendo um atributo que expressa o quanto um equipamento é indispensável para todos os recursos funcionarem entre si.

Entre todas as ferramentas disponíveis para fazer toda a identificação da prioridade dos ativos existentes na empresa, foi escolhido a ‘Curva ABC’.

A Curva ABC é um método de classificação de importância a qualquer coisa, não servindo apenas para a área de TI, mas muitas vezes utilizados para está, pois atende todos os requisitos para uma avaliação completa.

Sua classificação feita da seguinte forma:

Coloca-se um nível de criticidade para cada item, sendo A para maior importância (correspondendo a 20% do total), B para importância mediana (50% do total) e C para menor importância (80% do total).

Essa classificação é feita de maneira óbvia, mas de extrema importância. Como por exemplo, um servidor é considerado como prioridade máxima, por se tratar de algo de extrema importância, e que causaria danos profundos na empresa caso este venha a dar algum problema técnico. Já um computador da recepção seria uma prioridade baixa, pois caso este venha a apresentar algum problema, pode ser substituído facilmente por qualquer outra máquina, levando em consideração que as informações contidas nele são de baixo valor para a empresa.

3 CENÁRIO PASSADO

O antigo cenário de conexão era composto por dez funcionários, sendo sete utilizando conexões remotas para acessar o banco de dados e informações dos seus clientes, e três funcionários, que ficam fisicamente em clientes, acessando a rede interna da empresa.

Todos os funcionários, tanto os que estão na empresa ou não, precisam acessar, de forma rápida e simultânea, informações que estão tanto na base de dados do cliente, quanto na da própria empresa.

Para acessar todos os dados necessários, levando em consideração que são cerca de quinze clientes, as conexões não eram muito bem definidas. Apenas três clientes possuíam serviços de VPN para ser utilizado pelos funcionários da empresa CRG, porém não era disponibilizado a quantidade de usuários suficientes para o número de funcionários que a empresa tem, sendo assim, mais de um funcionário utiliza o mesmo usuário de VPN, tornando a conexão de ambos muito instável.

Softwares que permite que os usuários tenham controle sobre outro computador eram comuns na antiga forma de conexão remota utilizada pelos funcionários da empresa. Com eles, é possível fazer compartilhamento de dados entre dois dispositivos, além de prestar suporte direto na máquina desejada.

Com a utilização destes programas para estabelecer as conexões, como por exemplo, Anny Desk, Team Viewer ou Ammy, resultava em uma lentidão na execução de todos os processos, pois para utilizar esta conexão, o funcionário precisaria entrar em contato com alguém que esteja no cliente para liberar acesso. O que muitas vezes acontecia é de uma pessoa acessar a mesma conexão que já está sendo utilizada, levando assim em perdas de conexões em ambas as partes.

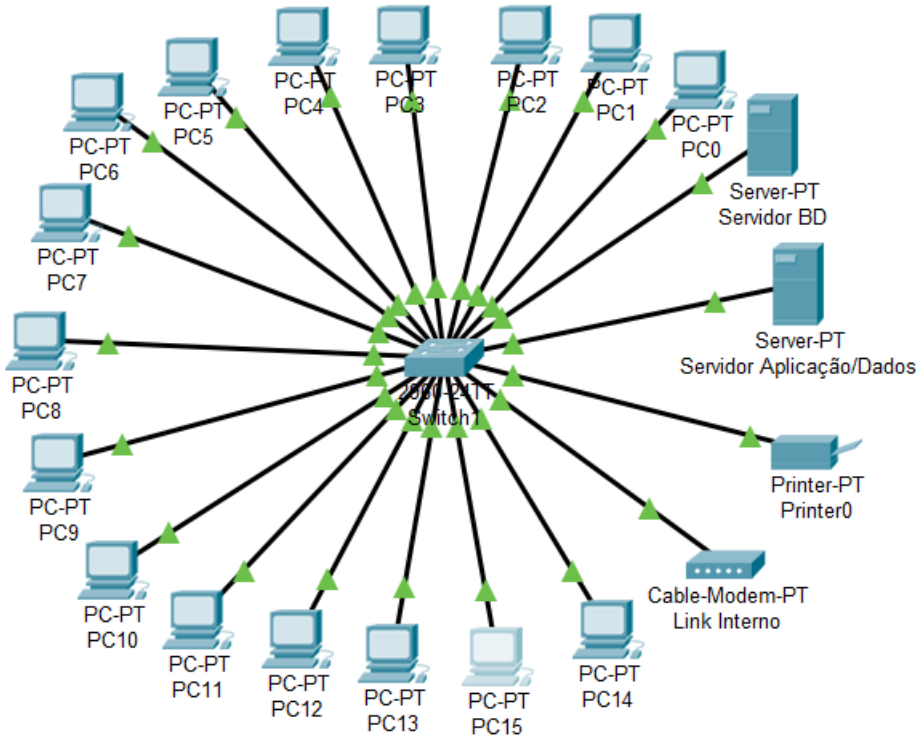
3.1 ESTRUTURA DE REDE

Uma estrutura de rede pode ser categorizada, de forma resumida, como a conexão de vários dispositivos conectados entre si, através de uma forma de conexão, para compartilhar informações entre eles.

Sendo assim, abaixo é detalhado como se encontrava a estrutura de computadores da empresa, antes de qualquer mudança ser executada.

A figura 2 mostra uma simulação da antiga estrutura de rede da empresa.

Figura 2: diagrama de rede.



Fonte: dados da empresa.

Com cerca de dezesseis computadores conectados simultaneamente a rede, a imagem mostra que há dois servidores, um para guardar todas as informações relevantes da empresa e para execução de uma aplicação web. Já o outro servidor tem a função de armazenamento do banco de dados.

Apenas um link de internet é disponibilizado ao Switch, que tem por seu objetivo ser uma extensão de pontos de rede, interligando todos os dispositivos.

Este Switch é composto por 24 portas, e destas portas, eram utilizadas 20, causando uma grande sobrecarga neste dispositivo, pois se houvesse uma queda de internet, a rede inteira perderia conexão.

É possível observar que nenhum tipo de *firewall* era utilizado nesta rede, deixando todos os equipamentos mais vulneráveis a qualquer tipo de ataque, já que nenhuma proteção básica sobre a rede era feita.

4 PLANO DE CONTINUIDADE DE NEGÓCIO

Como o principal objetivo é solucionar o máximo possível dos problemas e transtornos que as conexões estavam gerando a todos seus utilizadores, não pode-se deixar aberto a oportunidade de novas conexões remotas causarem problemas que já foram solucionados em situações anteriores com as conexões, pois deve-se deixar toda a estrutura de conexão de forma fácil para receber novos usuários, além de evitar qualquer futuro problema.

4.1 ESTRUTURA DE REDE

Sendo assim, foi definido que, caso algum novo cliente deseje contratar a empresa, há algumas perguntas necessárias para serem feitas antes de prestar qualquer serviço:

- Como as conexões estão preparadas para receber qualquer tipo de solicitação, de forma rápida e segura?
- Qual o impacto de uma possível queda de conexão?
- Os métodos de conexões atuais deste possível cliente estão de acordo com as políticas de segurança estabelecidas pela empresa CRG?
- Esta empresa está disposta a fazer modificações na sua atual estrutura de conexão para atender os requisitos de segurança?

Para isso, é extremamente relevante observar a importância de um Plano de Continuidade de Negócios.

> Plano de Continuidade de Negócios (PCN) é o processo de gestão da capacidade de uma organização de conseguir manter um nível de funcionamento adequado até o retorno à situação normal, após a ocorrência de incidentes e interrupções de negócios críticos (LEOBONS, 2012, p. 8).

Desta forma, terá o conhecimento dos processos mais cruciais do negócio, com normas e padrões em mãos, para que em situações adversas, a empresa possa se recuperar, retomar e dar prosseguimento a esses processos, evitando lentidão ou queda de conexões.

Após o contato de alguma empresa desejando contratar os serviços da CRG, o próximo passo seria a análise de atual forma de conexão que a empresa utiliza, para observar se a empresa tem todos os requisitos necessários para fazer uma implementação de toda a política de conexão.

4.1.1 POLÍTICA DE CONEXÃO REMOTA

Para manter todos os processos protocolados e para que os usuários tenham documentos para serem seguidos, abaixo são listados os requisitos para orientar e estabelecer os padrões de conexões remotas:

- As autenticações de identidade dos utilizadores devem ser verificadas sempre que possível.
- O acesso remoto deve ter controle de acesso para cada usuário, contendo o que cada usuário pode ou não acessar, controlados previamente antes da criação de cada usuário, podendo modificar-se a qualquer momento.
- O acesso remoto a rede corporativa da empresa deve ser estabelecida por meio de um canal criptografado.
- Todas as conexões remotas estabelecidas devem ser gravadas em logs, para manter o controle de modificação, exclusão, edição e adição de alguma informação, de acordo com qual usuário executou a ação.
- A permissão ao acesso remoto deve ser concedida previamente pelo departamento de TI (Tecnologia da Informação), com definição estabelecida de horários para executar tal conexão.
- Todas as permissões devem ser revisadas a cada quinze dias, confirmando com todos os usuários e necessidades de cada permissão.
- Os usuários que enfrentarem qualquer problema relacionado à conexão remota, deverão reportar e abrir um *ticket* para o departamento de TI, podendo ter acesso ao acompanhamento do *status* desta requisição.
- RDP é a ferramenta homologada para estabelecer conexão.
- Atualização de senhas de usuários de VPN a cada 120 (cento e vinte) dias.
- Manter sigilo das informações encontradas/obtidas através de uma conexão remota na rede corporativa da empresa, sendo de responsabilidade qualquer ação feita utilizando alguma credencial.
- Quando identificado que há permissões desnecessárias vinculadas a conta de usuário, avisar o mais breve possível o departamento de TI para efetuar a correção.

5 CENÁRIO ATUAL

Com todas as mudanças feitas dentro da empresa, tanto em seu ambiente lógico quanto em seu ambiente físico, as alterações resultaram em objetivos que não poderiam ser alcançados utilizando a estrutura anterior.

Podemos classificar as mudanças executadas em duas categorias: *software* e *hardware*.

5.1 *SOFTWARE*

Sendo uma parte fundamental para a melhoria de estabilidade e velocidade de uma conexão remota, a mudança dos *softwares* de conexão e de sua forma de utilização causa grande impacto em todo o projeto, além da segurança do mesmo.

Para levantar todas as mudanças estabelecidas e suas melhorias relatadas, podemos classificar as alterações feitas nos tópicos citados abaixo.

5.1.1 CONEXÃO REMOTA

Após a remoção de *softwares* de conexão remota que não atendiam completamente as necessidades da empresa em relação a segurança e estabilidade das conexões remotas, foi identificado maior produtividade por parte dos colaboradores da empresa.

- Resultado da implantação da política de conexão remota:

Todas as alterações feitas em relação à política de conexões remotas com o objetivo de aumentar o controle e segurança das conexões remotas causaram um grande transtorno dos primeiros dias de aplicação.

Como todos os utilizadores das conexões remotas já tinham se acostumado em utilizar as conexões da forma antiga, mesmo que elas não tivessem o mínimo de segurança, estabilidade ou velocidade, ainda assim era uma forma ‘padrão’ de conexão remota.

Como qualquer mudança drástica em algo que é utilizado com certa frequência, mesmo que seja mudanças com o objetivo de melhorias, causa transtorno para os usuários, pois para alterar qualquer estrutura, é necessário a parada de todo o processo, além da necessidade de novas instruções para utilização do novo método.

Com isso, houve reclamações por parte dos usuários com as alterações no primeiro mês da implantação da política de conexões remotas, principalmente em relação ao controle de usuários e senhas.

Porém, ao ver que todos os novos métodos e processos que estavam sendo implementados resultavam em uma maior velocidade nas conexões, que por sua vez, tinha como consequência uma maior produtividade em seus trabalhos, as reclamações diminuíam gradativamente com o tempo.

Na primeira semana da após a implementação do controle de usuários de VPN’s, as quedas de conexões remotas por motivo de um usuário encerrar a conexão de outro, diminuíram gradativamente ao passar da semana.

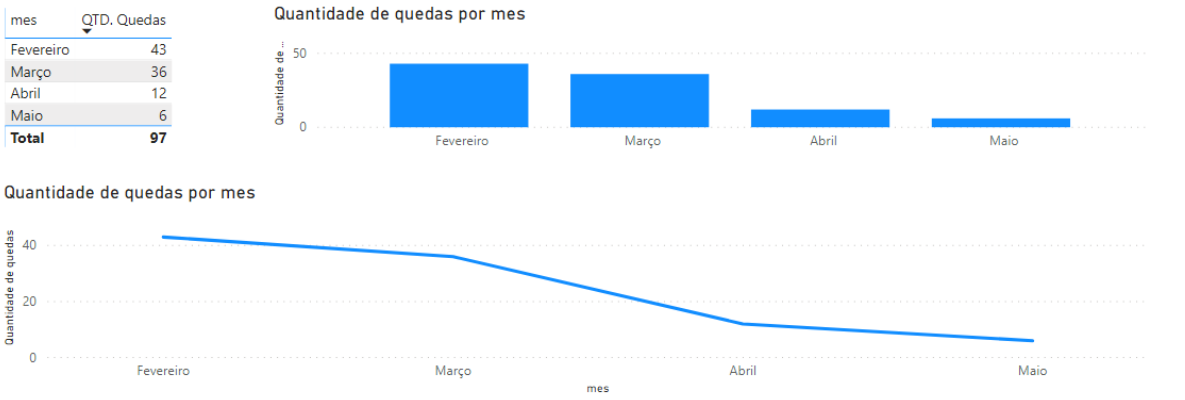
A implementação dessa política de usuários causou pequenos transtornos para seus utilizadores, pois houve a necessidade de uma pausa coletiva para a troca e configuração de todos os usuários.

Após toda a manutenção feita completamente entre os usuários, a média de queda de conexão na primeira semana foi de três a quatro quedas diárias, por conta e confusão de arquivos para efetuar login em uma VPN entre os usuários.

Porém, após os sete primeiros dias, a taxa queda de conexão caiu para uma média de uma a duas quedas. E após trinta dias da implantação, a taxa era menor que um, chegando à uma média mensal de 0,2 quedas diárias no segundo mês após a implantação, tanto as conexões remotas feitas de dentro da empresa para computadores de clientes, quanto os colaboradores que se conectam remotamente para acessar a rede da empresa.

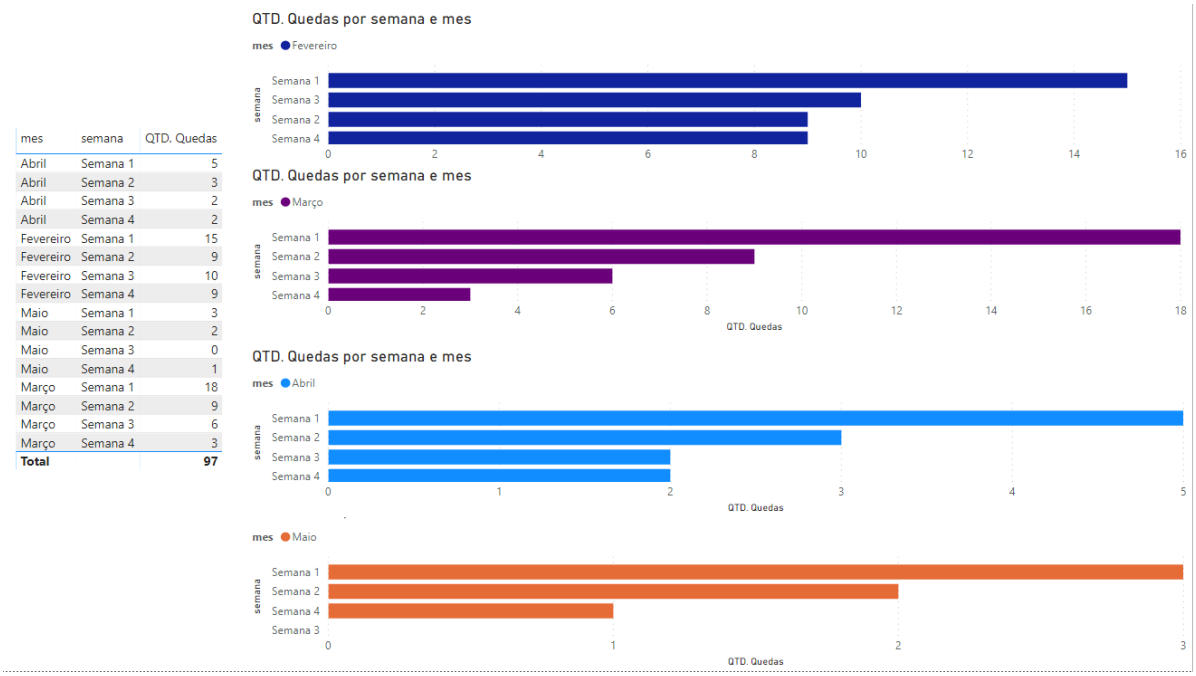
Os dados acima citados podem ser visualizados de uma forma mais clara como mostra a figura 2 e 3.

Figura 3: gráficos sobre quantidade de quedas de conexões por mês.



Fonte: dados da empresa.

Figura 4: gráfico sobre quedas de conexões por semana.



mes	semana	QTD. Quedas
Abril	Semana 1	5
Abril	Semana 2	3
Abril	Semana 3	2
Abril	Semana 4	2
Fevereiro	Semana 1	15
Fevereiro	Semana 2	9
Fevereiro	Semana 3	10
Fevereiro	Semana 4	9
Maio	Semana 1	3
Maio	Semana 2	2
Maio	Semana 3	0
Maio	Semana 4	1
Março	Semana 1	18
Março	Semana 2	9
Março	Semana 3	6
Março	Semana 4	3
Total		**97**

Fonte: dados da empresa.

5.1.2 *FIREWALL* E ANTÍVIRUS

A empresa possuía todos os módulos de *firewall* desatualizados ou até desativados em grande parte das máquinas, incluindo os servidores, possibilitando um enorme montante de riscos e possíveis vírus. Esse cenário permitia que *softwares* mal-intencionados pudessem provocar lentidão nos computadores, além de eventuais roubos de senha dos bancos. Todo esse atraso no rendimento da máquina emplacaria diretamente na produção da empresa, além de futuramente promover a perda de credibilidade com clientes e colaboradores. Portanto, todas as atualizações disponíveis nas máquinas foram realizadas, incluindo as do *firewall* nativo do Windows.

Com relação a antivírus, era utilizado um *software* gratuito, que não atendia todos os requisitos que está infraestrutura necessitava de fato. Para resolver este problema, foi implementado o *software* ‘Kaspersky’ em todas as máquinas dos colaboradores, com a atualização automática assim que disponível.

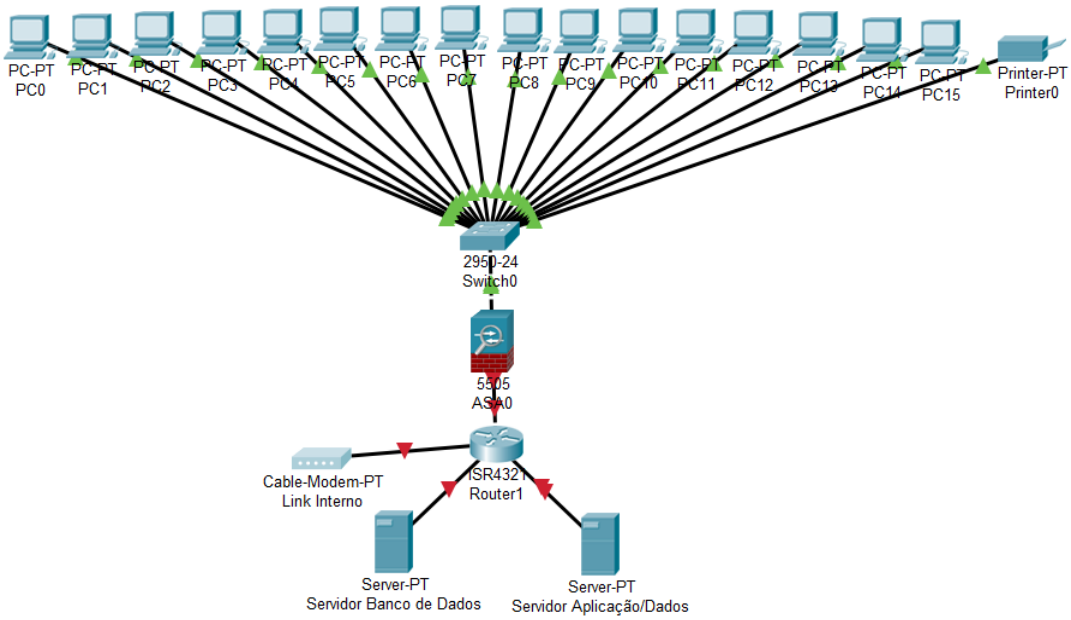
5.2 HARDWARE

As operações feitas em um computador dependem de seu *hardware*, onde são processadas todas as informações que entram e saem de uma determinada máquina. Com isso em mente, qualquer requisição de processo feito tem seu tempo de resposta ligado diretamente ao *hardware*, que por sua vez, tem como objetivo executar todas as transferências de dados que são feitas dentro de uma conexão remota.

5.2.1 ESTRUTURA DE REDE ATUAL

Como a antiga estrutura de rede da empresa pecava seriamente na segurança, foi necessária uma reestruturação dos equipamentos para amplificar na eficiência/velocidade de utilização da rede, além de garantir muito mais segurança aos dados que trafegam.

Figura 5: estrutura de rede atual.



Fonte: dados da empresa.

Com a adição de um *firewall* para proteger os dados internos da rede, todos os dados que trafegam são validados pelo *firewall*, servindo como uma peneira, deixando apenas os dados válidos entrarem/saírem.

Assim, a rede fica muito mais estruturada e organizada, de fácil manutenção e com uma segurança a altura da estrutura de rede da empresa.

Como a empresa nunca sofreu nenhum ataque malicioso, não é possível afirmar que houve alguma mudança em relação à diminuição de vírus ou/e ataques contra a rede da empresa, porém foi notado que a frequência de queda de link de internet diminuiu, pois a distribuição da rede fez com que não sobrecarregasse o switch.

5.2.2 COMPUTADORES DA EMPRESA

Cerca de 16 máquinas eram utilizadas ativamente dentro da empresa, e dentro deste número, 13 computadores foram trocados completamente, sendo feito a venda das máquinas antigas, e comprando novos computadores para atender todas as necessidades de processamento que as máquinas requisitavam.

A figura abaixo mostra com detalhes quais as configurações dos novos computadores:

Figura 6: *Hardware* dos novos computadores.

Dispositivo	Especificações
Notebook DELL Inspiron 15 3000 Quantidade: 10	Windows 10 Professional Processador: Intel Core i5-8265U - 3.9 GHz Memória instalada (RAM): 4GB, DDR4, 2666MHz Tipo de sistema: Sistema Operacional de 64 Bits Unidade de estado sólido (SSD): 128GB
Computador Optiplex 3070 Micro Quantidade: 3	Windows 10 Professional Processador: Intel Core i3-9100T - 2.5 GHz Memória instalada (RAM): 4GB, DDR4, 2666MHz Tipo de sistema: Sistema Operacional de 64 Bits Unidade de estado sólido (SSD): 128GB

Fonte: dados da empresa.

O motivo pelo qual os outros 3 computadores não tiveram seus equipamentos atualizados, é porque eles já atendiam os requisitos suficientes de um computador mediano/avançado em relação ao seu *hardware*, levando a não necessidade de mudanças físicas nestes computadores, assim como mostra a relação destes na figura abaixo:

Figura 7: Computadores mantidos.

Dispositivo	Especificações
Notebook DELL Vostro 14 5000 Quantidade: 3	Windows 10 Professional Processador: Intel Core i5-8265U - 3.9 GHz Memória instalada (RAM): 8GB, DDR4, 2666MHz Tipo de sistema: Sistema Operacional de 64 Bits Unidade de estado sólido (SSD): 260GB Placa de vídeo NVIDIA® GeForce® MX130 com 2GB de GDDR5

Fonte: dados da empresa.

Posteriormente a mudança das peças dos computadores dos colaboradores da empresa, observou-se que não houve mais problemas em relação a *softwares* modernos não serem executados de forma correta nas estações de trabalho, pois os computadores antigos não suportavam sistemas

de grande porte, garantindo assim uma maior velocidade no decorrer das tarefas diárias e na compatibilidade de todos os *softwares* utilizados no dia a dia.

5.2.3 SERVIDOR DE BORDA

Após a compra do segundo servidor voltado exclusivamente para o banco de dados, o primeiro servidor de aplicação não ficou sobrecarregado, sobrando memória volátil para as conexões serem validadas e executadas de forma mais ágil.

A implementação do servidor de borda teve como resultado principal a aceleração do fluxo de dados entre dois pontos conectados na rede, que neste caso é a conexão remota.

Levando em consideração que a empresa CRG tem um grande volume de dados entrando e saindo o tempo todo de seus servidores, o método de computação na borda levou a diminuição de consumo de banda de internet, o que deixou todos os passos de processo de conexão remoto com menor tempo de resposta de informações.

5.2.4 CUSTO

O projeto para implantar toda a parte de *software* e *hardware* não teve seu foco em custo, pois todos os problemas relacionados às conexões remotas que estavam prejudicando o escritório de contabilidade tinham um custo monetário mensal bem maior que o gasto total da implantação do projeto.

Sendo assim, os dados abaixo tem apenas valor demonstrativo, pois não produziu nenhuma mudança significativa no projeto.

Abaixo, podemos ver os equipamentos adquiridos para a nova estrutura de rede da empresa:

Figura 8: Resumo dos *hardwares* adquiridos.

Equipamento	Quantidade	Custo Total
Notebook DELL Inspiron 15 3000	10	R$28.590,00
Computador Optiplex 3070 Micro	3	R$8.853,00
SSD Kingston 240GB	13	R$2.273,70
Total		**R$39.716,70**

Fonte: dados da empresa.

Assim como os serviços relacionados a *software*:

Figura 9: Serviços/*softwares* contratados.

Serviço	Custo anual
NOIP	R$124,29
VPN	RS$6,22
Antivírus Kaspersky	R$419,60
Total	**R$550,11**

Fonte: dados da empresa.

6 CONCLUSÃO

O projeto foi pensado e estudado para a melhoria de alguns pontos negativos que a empresa em questão enfrentava, como: desorganização na forma padrão de estabelecer conexões remotas, nenhum controle de usuários sobre as conexões, falta de segurança nas conexões estabelecidas de forma interna e externa, pouco conhecimento técnico dos colaboradores diante as políticas necessárias para se utilizar uma conexão remota, entre outros. Em virtude a esses pontos, o serviço de melhoria de conexões remotas foi requerido.

Após o estudo do ambiente as ações foram tomadas, avaliando sempre o que era necessário para melhorar as atividades relacionadas as conexões remotas, pensando na atualização da parte lógica e física da empresa.

A padronização de uma forma de conexão remota possibilitou o melhor rendimento operacional dos colaboradores, uma vez que as dúvidas e problemas relacionados às conexões remotas que eram utilizadas pelos funcionários, tiveram grande melhorias de performance, além da divisão e organização individual de cada usuário.

O *upgrade* das máquinas que eram utilizadas para estabelecer conexões remotas trouxe um maior rendimento e velocidade aos colaboradores desta empresa, sendo este um problema recorrente entre os funcionários.

A segurança dos dados da empresa foi reestruturada, deixando claro aos utilizadores da rede interna quais as etapas obrigatórias para acessar qualquer informação da empresa. Além disso, com a utilização de um *firewall*, antivírus e senhas criptografadas, essas ferramentas trouxeram uma confiabilidade muito maior por parte dos clientes que utilizam os serviços da CRG Gestão, levando em consideração que houve um grande investimento em relação a segurança das informações contidas nesta empresa.

O projeto se mostrou eficaz e conseguiu atender o que a empresa desejava: uma notável melhora na estabilidade das conexões remotas, produtividade de seus funcionários e segurança para armazenar seus dados.

REFERÊNCIAS BIBLIOGRÁFICAS

BRUNNER, Marcelo. **A importância da auditoria de TI para a sua empresa**, [s. l.], 2017. Disponível em: <http://www.cloverit.com.br/auditoria-de-ti-empresa/>. Acesso em: 20 out. de 2019.

FONTES, Edison. **Segurança da informação: o usuário faz a diferença**. [s. l.], 2010. Disponível em: <https://books.google.com.br/books?id=FyprDwAAQBAJ&printsec=frontcover&dq=edison+fontes+seguran%C3%A7a+da+informa%C3%A7%C3%A3o&hl=pt-BR&sa=X&ved=0ahUKEwiJlrPEz-DkAhW-ILkGHfavCpgQ6AEILzAB#v=onepage&q=edison%20fontes%20seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o&f=false>. Acesso em: 20 de set. de 2019.

LEOBONS, Milton Luis. **Guia de boas práticas para planos de continuidade de negócios.** [*s. l.*], 2012. Disponível em: <http://www.abrapp.org.br/GuiasManuais/guia_continuidade_negocios.pdf>. Acesso em: 30 de set. de 2019.

TANENBAUM, Andrew S. **Computer Networks: Fourth Edition**. Upper Saddle River, Nova Jersey. Prentice Hall, 2003.