REVISTA Interdisciplinar da Meta

LGPD - PROPOSTA DE IMPLEMENTAÇÃO DE MELHORIAS EM ESCRITÓRIO DE CONTABILIDADE: ESTUDO DE CASO

LGPD - PROPOSAL FOR IMPLEMENTATION OF IMPROVEMENTS IN ACCOUNTING OFFICE: CASE STUDY

Arlline Conceição Favacho de Oliveira[1]
Beatriz de Amorim Campos[2]
Alex Sanches Macedo[3]
Amerson Riley Cabral Chagas[4]

RESUMO: A Lei Geral de Proteção de Dados – LGPD, foi criada com o intuito de estabelecer um padrão de regras e procedimentos que compreendem a forma como são armazenados, tratados e compartilhados os dados pessoais dentro de uma instituição, deixando evidente que, as empresas que descumprirem seus preceitos poderão sofrer sanções, haja vista que seu principal objetivo consiste em garantir a segurança, privacidade e transparência no tratamento dos dados. Este trabalho apresenta-se como uma proposta de implementação da LGPD em um escritório de contabilidade, visando contribuir com melhorias tanto na infraestrutura de rede do local, quanto no desempenho dos funcionários. Dessa forma, garantir a confiabilidade e segurança aos clientes e colaboradores acerca da proteção de seus dados pessoais. Sua metodologia baseia-se em um estudo de caso, caracterizado como bibliográfico e exploratório descritivo, se deu através de um mapeamento da infraestrutura da rede do escritório, bem como na aplicação de questionários e entrevistas. Através dos resultados, observou-se como ocorre o tratamento das informações que estão sob sua competência. E observou-se a necessidade de entendimento e treinamento da equipe quanto às novas regras exigidas pela lei. Desse modo, a pesquisa conclui-se com a proposição de melhorias - em concordância com os fundamentos que norteiam a LGPD - na infraestrutura de rede do escritório, mantendo um foco especial na capacitação dos funcionários, na contratação de um *Data Professional Officer* – DPO e na implementação de ferramentas e equipamentos que irão agregar valor à segurança da rede, de modo a atender suas necessidades.

Palavras-chave: DADOS PESSOAIS; LGPD; INFRAESTRUTURA DE REDE; ESCRITÓRIO DE CONTABILIDADE; ESTUDO DE CASO.

ABSTRACT: The General Data Law - was created with the aim of establishing a standard of rules and procedures that were designed to protect people, treated and shared with LGPD data, an organization that, of course, its precepts must comply with the main efforts, given that your privacy consists of ensuring security and transparency in. This work presents itself as a proposal for the implementation of LGPD in an accounting office, complementing the network infrastructure of the place, regarding the performance of employees. In this way, guarantee your personal trust and security to data protection customers and employees. The methodology was based, as a bibliography and it was done through a mapping of the office network infrastructure, as well as the application of its case study and interviews. Through the results, it was verified how the treatment of the information that is under its competence occurs. The need for treatment and new tools by the team was observed. Thus, the proposal for improvements - in research based on LGPD - in the office's network infrastructure, is concluded, keeping a special focus on employee training, on hiring a Data Professional - DPO and on the implementation of tools and equipment that will add value to network security to meet your needs.

[1] Acadêmica do Curso de Redes de Computadores da Faculdade de Tecnologia do Amapá – META; E-mail: arllinecfavacho@gmail.com
[2] Acadêmica do Curso de Redes de Computadores da Faculdade de Tecnologia do Amapá – META; E-mail: beatrizamorimcampos@gmail.com
[3] Mestre em Engenharia Elétrica na área de Telecomunicações (UFPA), docente do curso de Redes de Computadores; e-mail: alex.macedo@meta.edu.br
[4] Mestre em Engenharia de Software pelo Centro de Estudos e Sistemas Avançados do Recife (CESAR). Docente do curso de Redes de Computadores da Faculdade de Tecnologia do Amapá – META. E-mail: amersonchagas@meta.edu.br

Keywords: PERSONAL DATA; LGPD; NETWORK INFRASTRUCTURE; ACCOUNTING OFFICE; CASE STUDY.

INTRODUÇÃO

É notável que nos dias atuais o avanço da tecnologia e seus recursos trouxeram inúmeras facilidades para a vida dos usuários em suas atividades residenciais, como também para as empresas que utilizam dessas funcionalidades para se manterem atuantes no mercado. Contudo, juntamente com esses benefícios, são crescentes os riscos que andam atrelados a esta evolução. Para isso, torna-se de fundamental importância tomar medidas preventivas que busquem garantir a proteção das informações.

No cenário contábil, é evidente que há uma necessidade de unificar a utilização das tecnologias entre os aspectos físicos e digitais, visando uma maior segurança para dentro do ambiente profissional, como também passar mais confiança para seus colaboradores. Com isso, tornou-se elevado o nível de preocupação de empresas contábeis em se adequarem às políticas de segurança de informações. E neste contexto de insegurança informacional, a Lei Geral de Proteção de Dados – LGPD surge com o intuito de estabelecer normas e regras que amparam à segurança dos dados em seus diversos aspectos.

Esta pesquisa tem como foco um estudo de caso em um escritório de contabilidade localizado no bairro do Trem, na cidade de Macapá-AP, ao qual foram realizados levantamentos técnicos e foi possível observar as vulnerabilidades apresentadas no ambiente físico, bem como em sua estrutura virtual, ficando evidente a necessidade de estruturar o ambiente a estar de acordo com os preceitos da LGPD, suas regras e procedimentos para o uso, armazenamento, tratamento e compartilhamento de dados pessoais.

Desta forma, dadas as insuficiências encontradas, este estudo surge com a proposta de uma implementação de recursos físicos e virtuais, baseados na LGPD, visando levar uma série de melhorias para o ambiente, tanto em termos de infraestrutura, como também na capacitação dos funcionários.

A pesquisa busca relatar para as empresas em geral, sobre a necessidade de se estar de acordo com a lei, através da implementação de meios que contribuam para tornar seu ambiente mais seguro e confiável, assim como, estimular outros profissionais acerca da importância de estudos relacionados ao ambiente profissional e a segurança das informações.

LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

A Lei Geral de Proteção de Dados foi criada com o intuito de estabelecer regras e procedimentos que compreendam a utilização, o armazenamento, o tratamento e o compartilhamento dos dados pessoais, bem como, aplicar sanções aqueles que não se enquadrarem às normas que devem ser seguidas.

Marques (2020) complementa que, a implementação da lei consiste em uma tarefa complexa, pois parte da necessidade de uma mudança de pensamento associada a boas práticas de gestão destes dados pessoais, investimentos na área de segurança por parte da instituição, e até mesmo na capacitação dos profissionais ali presentes.

O ideal é que todas as empresas, independentemente de seu porte, invistam em segurança tecnológica, visando impedir a invasão e a violação dos dados pessoais, assim, todas as organizações brasileiras devem se adequar a LGPD.

Os principais papéis dentro da LGPD são: o titular dos dados, controlador, operador, encarregado e a Autoridade Nacional de Proteção de Dados – ANPD.

TITULAR

O titular dos dados é uma pessoa singular referida pelos dados, reconhecida ou identificável, sendo assim possível de se obter a identificação de forma direta ou indireta. Maciel (2019) define o titular dos dados como sendo pessoas naturais, excluindo-se deste conceito as pessoas jurídicas.

De acordo com Brasil (2018), a LGPD cria direitos que amparam os titulares dos dados, estes que vão desde a confirmação da existência do tratamento, acesso, correção, anonimização, bloqueio, exclusão ou compartilhamento dos dados, informações sobre a possibilidade de negar ou revogar seu consentimento.

CONTROLADOR, OPERADOR E ENCARREGADO

A LGPD traz as definições de encarregado dos dados e dos agentes de tratamento, Donda (2020) complementa que os agentes de tratamento são os controladores e os operadores.

O autor ressalta ainda, que os agentes de tratamento são os responsáveis pela segurança e pela privacidade dos dados, e são juridicamente responsáveis por indicar o encarregado, este que consiste em ser o canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

O controlador consiste na pessoa física ou jurídica (de direito público ou privado), que está à frente das decisões relativas ao tratamento dos dados pessoais. Para Lima (2020) o controlador é o responsável pelas decisões relacionadas ao tratamento dos dados, bem como registros sobre o seu tratamento, trabalhando como um canal de comunicação com a ANPD. Este agente possui relação direta com o titular, e deve adotar medidas de boas práticas de segurança e governança para que o tratamento dos dados esteja em conformidade com as diretrizes da lei.

Donda (2020) define operador como sendo a pessoa que realiza o tratamento de dados pessoais em nome do controlador, este que consiste em uma pessoa natural ou jurídica, de direito público ou privado, responsável pelo tratamento dos dados pessoais, devendo sempre documentar todos os registros das operações de tratamento.

A lei define o encarregado de dados como, pessoa designada pelo controlador e operador para atuar como um canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. (LIMA, 2020, pág. 19)

O autor ressalta que o encarregado tem por função intermediar as ações entre os envolvidos no tratamento dos dados, possuindo plena liberdade para tratar sobre as informações, realizar denúncias em casos de irregularidades e fiscalizar se as políticas adotadas estão sendo cumpridas.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD NA LGPD

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional. (GARCIA *et al.*, pág. 18, 2020)

Ainda nas palavras de Garcia *et al.* (2020) cabe a ANPD fiscalizar os eventuais abusos ou desvios do Poder Público com relação ao uso dos dados, sendo a figura central para a aplicação da LGPD, em um contexto em que os agentes de tratamento, tanto o setor público como do privado, estarão sujeitos a sua atividade regulatória, especialmente no campo sancionatório, com a possibilidade da exigência de penalidades.

DADOS PESSOAIS NA LGPD

Os dados em si, são informações as quais devem ser tratadas com extrema importância dentro das organizações atuais pois, segundo Botelho e Camargo (2021) se tratam de um ativo extremamente relevante para as atividades econômicas, seu tratamento e seu uso são fatores determinantes para as atividades dentro da instituição.

Um dado pessoal consiste em toda informação que possa identificar um indivíduo, de forma direta ou indireta. Lima (2020) classifica os dados pessoais em informações como nome, RG, CPF, endereço residencial, data e local de nascimento, telefone, ou qualquer outro dado que o possa identificá-lo.

TRATAMENTO DE DADOS

Leite, Lamboy e Lapolla (2019) discorrem que o dado protegido encontra na LGPD regras que vão desde a coleta das informações, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência e compartilhamento – seja entre entes ou países –, além da difusão e da extração destes dados.

Dando continuidade ao seu pensamento, expõem que a LGPD protege os dados pessoais que possuem como finalidade a oferta ou o fornecimento de bens ou serviços individuais, localizados em todo território nacional, e não apenas aos negócios realizados no país, independentemente de onde tenham sido coletados.

PRINCÍPIOS GERAIS DA LGPD

A LGPD se baseia em seus princípios gerais que são fundamentais para o tratamento adequado dos dados. Para Lima (2020), são estes:

- **Princípio da finalidade:** se faz necessário que exista um motivo para que o dado seja tratado.

- **Princípio da adequação:** o tratamento tem que ter uma relação com a finalidade informada

- **Princípio da necessidade:** garante que o dado coletado seja limitado à sua finalidade.

- **Princípio do livre acesso e transparência:** toda utilização, compartilhamento, comunicação ou duração do tempo de uso dos dados fornecidos devem ser informados ao titular.

- **Princípio da qualidade dos dados:** consiste na manutenção dos dados pessoais completos, claros, atualizados e monitorados pelo controlador.

- **Princípio da segurança e prevenção:** onde os dados devem estar protegidos de danos ou de tratamentos não autorizados.

- **Princípio da não discriminação:** os dados pessoais não poderão ser utilizados de forma discriminatória, ilícita ou abusiva.

- **Princípio da responsabilização e prestação de contas:** os agentes de tratamento demonstrem, formalmente, a adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção dos dados e da eficácia das medidas.

PROFISSIONAIS DA CONTABILIDADE E A SEGURANÇA DOS DADOS

Os avanços tecnológicos abrem portas para o acesso e compartilhamento mais ágil de dados pessoais, exigindo uma segurança ainda maior e uma mudança de atitudes nos mais diversos campos profissionais.

Para Krüger *et al.* (2021) os profissionais da contabilidade se destacam por serem responsáveis por dados de clientes, fornecedores, ou seja, todos os seus colaboradores. Ainda, explana que os riscos a que estes dados estão expostos devem exigir atitudes conscientes e proativas, especialmente em se tratando da segurança de informações.

A LGPD surge para orientar as mais diversas áreas profissionais, mas especialmente os profissionais da contabilidade.

MATERIAL E MÉTODO

Esta pesquisa caracterizou-se como um estudo de caso de caráter exploratório descritivo concentrada em um público específico - um escritório de contabilidade, localizado no bairro do Trem, na cidade de Macapá, estado do Amapá - cuja identidade foi mantida em sigilo, a pedido da administração, por se tratar de uma pesquisa que explicitamente expõe as vulnerabilidades apresentadas pela organização. Neste sentido, no decurso do trabalho, será mencionada apenas como Escritório de Contabilidade.

Realizou-se um levantamento bibliográfico, constituído de conceitos relacionados ao objeto deste estudo, sendo eles, conceitos da LGPD e questões sobre a importância de se garantir a segurança de informações em espaços contábeis.

Foram elaborados 02 (dois) questionários parcialmente semelhantes, definidos como **Questionário I**, que apresentou 17 (dezessete) perguntas, respondido unicamente pela responsável administrativa e financeira da organização, por se tratar de uma pesquisa geral, que visou coletar informações da organização de um modo geral.

O **Questionário II**, apresentou 12 (doze) perguntas, onde todos os funcionários puderam responder questões relacionadas às políticas adotadas pela organização, como também suas práticas pessoais referentes à segurança dos dados. Ambos os questionários foram baseados em estudos realizados por Câmara (2020).

Juntamente com a coleta das informações por meio dos questionários, realizou-se uma visita técnica no escritório de contabilidade para mapear a infraestrutura da rede de computadores, e presencialmente, foi possível conversar com cada um dos funcionários, para uma melhor compreensão do ambiente profissional e suas práticas pessoais.

ANÁLISE E DISCUSSÃO DOS RESULTADOS

1. OBTENÇÃO DOS DADOS COLETADOS

O **Questionário I** foi respondido objetivando coletar informações acerca da situação que a organização se encontra atualmente, em termos de segurança de seus dados.

O escritório é composto por 10 (dez) funcionários no total. Destes, 08 (oito) mulheres e 02 (dois) homens, com faixa etária entre 32 e 61 anos. E atendem a 21 (vinte e um) clientes e 03 (três) fornecedores externos.

A empresa dispõe de acesso aos dados de todos os seus colaboradores. Diante dessa informação, questionou-se a respeito de políticas de segurança da informação. A responsável esclareceu que acredita possuir, pois na organização há uma *"padronização das informações que são usadas e confidencialidade dos dados que são recebidos, ainda que de forma implícita"*.

As informações são acessadas por todos dentro da organização (gerência e funcionários), e os mesmos são utilizados com o propósito de: *"garantir a qualidade do serviço, bem como o próprio funcionamento do escritório"*.

Os dados que a organização solicita e utiliza em sua rotina diária se classificam entre dados pessoais (nome, sobrenome, CPF, RG, gênero, data e local de nascimento, telefone, endereço) e dados financeiros (faturamento, lucratividade).

A organização se preocupa em estar de acordo com as normas atuais que asseguram ainda mais a integridade e a confidencialidade dos dados que são tratados diariamente por eles, com isso, concluíram ser de grande importância a implementação de uma política de segurança de informações, assegurando que trabalham *"com informações de diversas empresas e pessoas em variados setores de prestação de serviços".*

2. APRESENTAÇÃO DOS DADOS COLETADOS

Diante do que foi respondido pelo funcionários no **Questionário II**, a pesquisa apresentou os seguintes resultados:

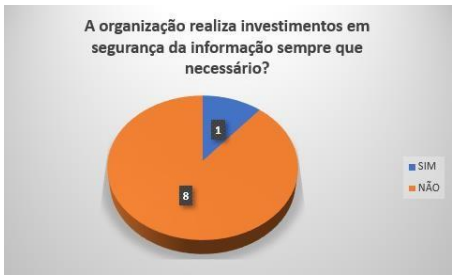
Quando questionados sobre a existência de uma política de segurançade informações dentro da organização, apenas 01 (uma) funcionária respondeu que existe uma política de segurança de informações. Em contrapartida, os demais responderam não existir uma política que atenda aos requisitos dentro da organização, conforme gráfico abaixo:

Gráfico 1: Questão 1

Fonte: Autoras, 2022

De acordo com o **Gráfico 2** abaixo, apenas 01 (uma) funcionária respondeu que a organização realiza investimentos em segurança da informação sempre que necessário. E os demais responderam não existir investimentos.

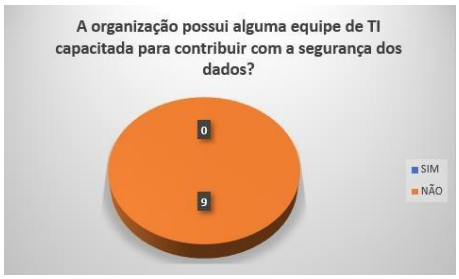
Gráfico 2: Questão 2



Fonte: Autoras, 2022

No **Gráfico 3**, quando questionados sobre a existência de equipe capacitada na área de tecnologia da informação para atender às necessidades da empresa nessa área, todos os funcionários responderam que não existe nenhuma equipe ou profissional que atenda à esta necessidade.

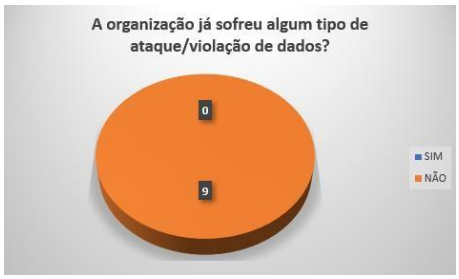
Gráfico 3: Questão 3



Fonte: Autoras, 2022

Não é de conhecimento de nenhum funcionário que a organização tenha sofrido algum tipo de ataque ou tentativa de violação de dados, conforme mostra o **Gráfico 4**.

Gráfico 4: Questão 4



Fonte: Autoras, 2022

De acordo com o **Gráfico 5**, apenas 01 (um) funcionário desconhece sobre a existência

de algum sistema ou *software* que funcione como antivírus. Os demais informaram que o Sistema Operacional – SO utilizado nos computadores é o *Windows*, portanto, informaram que o próprio SO disponibiliza o *Windows Defender*.

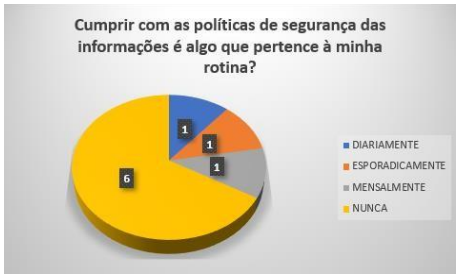
Gráfico 5: Questão 5

Fonte: Autoras, 2022

A partir do **Gráfico 6**, as perguntas passaram a ser de cunho pessoal, onde as informações se basearam em conhecimentos e práticas dos funcionários em suas atividades diárias.

Neste sentido, a maior parte dos funcionários – 06 (seis) – responderam que não costumam cumprir com as políticas de segurança das informações em sua rotina diária. Quanto aos demais, 01 (uma) funcionária respondeu cumprir de forma diária, 01 (um) funcionário respondeu cumprir de forma esporádica (01 ou 02 vezes na semana) e 01 (uma) funcionária respondeu cumprir mensalmente.

Gráfico 6: Questão 6



Fonte: Autoras, 2022

Segundo o **Gráfico 7**, apenas 03 (três) dos funcionários não lidam com o tratamentode dados de clientes da organização diariamente e os 06 (seis) demais informaram lidar diariamente com os dados.

Gráfico 7: Questão 7

Fonte: Autoras, 2022

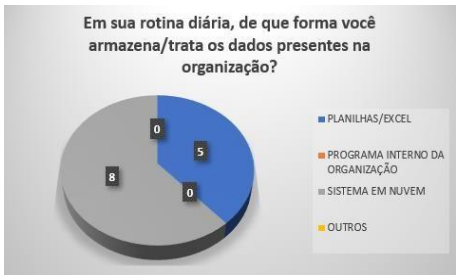
Foi questionada a forma como os funcionários armazenam ou tratam, diariamente os dados dos clientes na organização.

- 06 (seis) deles informaram utilizar somente os serviços de armazenamento em nuvem, através do sistema utilizado no escritório – Alterdata.

- 01 (uma) funcionária respondeu utilizar apenas os dados através de planilhas no Excel.

- 02 (dois) dos funcionários informaram utilizar ambos os serviços de nuvem e armazenamento em planilhas no Excel, conforme exibe o **Gráfico 8** abaixo.

Gráfico 8: Questão 8



Fonte: Autoras, 2022

A respeito de como solicitam os dados dos clientes da organização, e de acordo com o **Gráfico 9**, os mesmos responderam da seguinte forma:

- 02 (dois) funcionários utilizam somente os serviços de e-mail para solicitação e tratamento das informações.

- 02 (dois) funcionários responderam utilizar os serviços de telefone, e-mail, de forma presencial e para isso solicitam somente os dados que serão utilizados naquele momento.

- 01 (uma) funcionária utiliza somente os serviços de telefone, e-mail e solicita somente os dados que serão utilizados naquele momento.

- 01 (uma) funcionária informou já possuir somente os dados necessários das empresas que faz a contabilidade.

- 01 (uma) funcionária utiliza somente osserviços de telefone, e-mail e solicita apenas os dados que serão utilizados.

- 01 (uma) funcionária utiliza somente os serviços de e-mail e solicita somente os dados que serãoutilizados

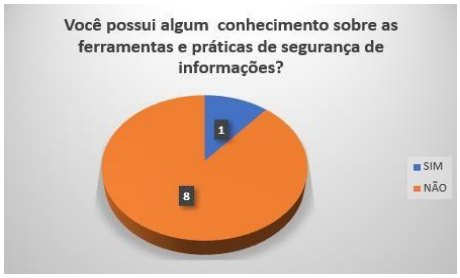
- 01 (um) funcionário utiliza apenas os serviços de telefone e e-mail.

Gráfico 9: Questão 9

Fonte: Autoras, 2022

Segundo o **Gráfico 10**, apenas 01 (um) funcionário disse ter conhecimento sobre ferramentas e práticas de segurança da informação, e informou saber o básico sobre antivírus e controles de acesso. Já os demais informaram não possuir conhecimento.

Gráfico 10: Questão 10



Fonte: Autoras, 2022

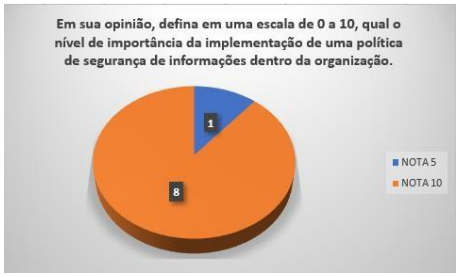
Sobre a LGPD, o **Gráfico 11** mostra que apenas 03 (três) dos funcionários informaram possuir conhecimento sobre a lei. Os demais informaram desconhecer ou já ter ouvido falar, mas sem aprofundamentos.

Gráfico 11: Questão 11

Fonte: Autoras, 2022

Em relação à implementação de uma política de proteção de dados dentro da organização, 08 (oito) dos funcionários avaliaram com nota 10 acerca da importância de implementação da mesma. Apenas 01 (um) funcionário avaliou com nota 5 sobre a questão, porém optou por não se justificar.

Gráfico 12: Questão 12



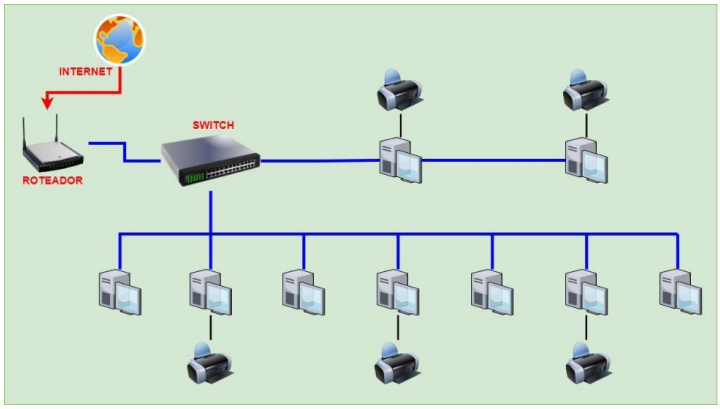
Fonte: Autoras, 2022

4.3 VULNERABILIDADES ENCONTRADAS NO ESCRITÓRIO DE CONTABILIDADE

A vulnerabilidade a que as empresas estão expostas e a proteção de seus dados pessoais nas relações com seus clientes e colaboradores passaram a se tornar foco de muitos estudos.

Detectou-se no escritório que, em termos físicos e lógicos, o mesmo possui uma rede cabeada, toda estruturada para atender suficientemente o escritório como um todo, cada funcionário dispõe de 01 (um) computador para suas atividades diárias. As impressoras são distribuídas de forma a atender a todos. Conforme construído na **Figura 1**, abaixo:

Figura 1: Infraestrutura de rede atual do Escritório de Contabilidade.



Fonte: Autoras, 2022

Quando questionados acerca da utilização de um *software* que funcione como antivírus, os mesmos informaram possuir em seus computadores o próprio recurso disponibilizado pela *Microsoft* – o *Windows Defender* – que funciona como antivírus e *firewall*.

Porém, há de se observar que, ainda que o mesmo possua os serviços básicos de proteção contra infecções externas por *malwares* dos mais variados tipos, dispensando assim a instalação de outros programas, o *software* mencionado acaba sendo insuficiente para alguns usuários, tais como empresas que trabalham com grande fluxo de dados, além do quê, este recurso não detecta *malwares* de baixo risco, como por exemplo, *adwares*, que apesar de não ser tão prejudicial, o ideal é evitar que os computadores obtenham qualquer tipo de ameaça.

Notou-se ainda, que a organização utiliza o programa Alterdata Nuvem para emissão e lançamento de notas das empresas que trabalha, porém, armazena algumasinformações em planilhas do Excel nos computadores.

Apesar destas formas de armazenamento que o escritório utiliza, até os dias atuais, não terem apresentado nenhum tipo de problema para a organização, ainda assim apresenta grande risco, visto que a organização não está segura,caso ocorra algum problema nos dispositivos de armazenamento simples, ou até mesmo um roubo.

Outro ponto vulnerável dentro da organização consiste no despreparo dos funcionários em relação à preocupação com a segurança das informações pois, em sua maioria desconhecem os riscos a que expõem as informações das empresas que trabalham diariamente.

PROPOSTA DE MELHORIAS PARA O ESCRITÓRIO DE CONTABILIDADE

A implementação da LGPD em qualquer ambiente que seja, é uma tarefa complexa, o

que de acordo com Marques (2020), consiste em uma série de recursos que devem partir desde uma mudança na mentalidade relacionada às boas práticas no tratamento dos dados, investimentos em segurança da informação, e até mesmo, na capacitação de profissionais que irão atuar na área.

Câmara (2020) explana que muitas mudanças devem ocorrer dentro de uma instituição para que possa estar adequada aos preceitos da LGPD.

A presente pesquisa traz uma proposta de implementação de melhorias no escritório de contabilidade, baseada na seguinte propositura:

- **Capacitação dos Funcionários de acordo com a LGPD**

Como os funcionários do escritório em sua maioria desconhecem questões relativas à LGPD, o ideal é que inicialmente sejam realizados treinamentos e apresentação de cursos e palestras, para que estes possam capacitar-se adequadamente.

Krüger *et al.* (2021) expõe em seus estudos que a realização de treinamentos contínuos, apresentação de cursos e palestras facilitam grandemente a conscientização dos funcionários sobre questões de segurança de dados, bem como a promoção de campanhas de conscientização da equipe, objetivando alcançar uma capacitação interna, por meio de cursos e eventos em conformidade com a LGPD.

- **Designação de um *Data Protection Officer* – DPO**

O DPO consiste na pessoa responsável pela elaboração de estratégias que visam verificar como funciona a coleta dos dados pessoais e auxiliar na proteção destes dentro de uma instituição, é o que expõe Aguiar (2021).

Para Garcia et. al. (2020) este será o profissional que atuará como um canal de comunicação e atenderá aos pedidos dos titulares dos dados, bem como, será responsável por receber informações da ANPD, orientando os colaboradores a respeitos das boas práticas relacionadas à segurança dos dados pessoais.

O DPO consistirá no encarregado dentro do escritório de contabilidade, será a figura que irá estruturar a LGPD dentro do ambiente, neste caso, irá iniciar o processo de adequação.

- **Ferramentas utilizadas para adequação à LGPD**

Antivírus

Considerada uma ferramenta de grande utilidade dentro de qualquer ambiente profissional, o antivírus, tem por objetivo principal proteger os dispositivos utilizados na rede, o que, para Tristão *et. al.* (2021) é extremamente relevante possuir este recurso em um ambiente de trabalho, pois estes trabalham de forma a prevenir, detectar e a eliminar os vírus encontrados nos mais diversos dispositivos.

A administração do escritório de contabilidade estará ciente quanto a existência de uma variedade de programas antivírus, dentre os gratuitos e os pagos. Porém, será recomendável que eles utilizem uma licença paga, esta que melhor atender as necessidades do ambiente. Este tipo de *software* pode oferecer soluções de segurança para e-mail, acesso à internet e acesso à rede, funções estas que são pouco encontradas em versões gratuitas.

Firewall

Esta ferramenta tem função fundamental dentro de uma rede de computadores, pois realiza a filtragem das informações, ou seja, se trata da primeira proteção entre os dispositivos internos da rede com a internet.

Para Tristão *et. al.* (2021), é através desta ferramenta que se torna possível manter o controle do que entra e do que sai de uma rede, e ainda, realizar bloqueios relacionados a sites considerados periculosos, aumentando assim a segurança ao evitar os ataques remotos de *hackers.*

Nos dias atuais, a maioria dos sistema operacionais já possuem instalados em sua configuração o *firewall*, tal qual possuem no escritório objeto deste estudo, porém, conforme ressaltado pelos autores acima, um *firewall* de *hardware* é um equipamento com vantagens relevantes a serem levadas em conta, pois consiste em um equipamento especificamente para este fim, ou seja, pode trabalhar tranquilamente com uma quantidade considerável de entrada e saída de dados, e ainda assim não estar sujeito a incidentes que possam vir a ocorrer, como por exemplo, uma falha em outro *software*, haja vista que este equipamento se dedicará unicamente à segurança com suas funções específicas, ao invés de compartilhar recursos com outros aplicativos.

Data Loss Prevention – DLP

O Data Loss Prevention – DLP, consiste em uma solução tecnológica que surgiu com o intuito de trazer aos ambientes mais segurança e atenuar possíveis roubos ou furtos de dados. Para Ricci, Luz e Ferreira (2020), o DLP é definido como uma prática de detecção e prevenção de vazamento de dados confidenciais para uso não autorizado, logo, neste cenário estão incluídos todos os tipos de dados, sejam eles físicos ou digitais.

Nas palavras de Tristão *et. al.* (2021), a ferramenta DLP trabalha na identificação, monitoração e proteção da perda de dados, monitorando em tempo real, registros de logs e demais políticas definidas para impedir que acessos não autorizados ocorram ou sejam roubados.

Esta ferramenta será de grande relevância dentro do escritório, pois este modelo de *software* virá a oferecer à empresa, recursos adicionais de proteção e segurança, evitando assim, extravios de informações e até impedir acessos indevidos aos dados.

Intrusion Prevention System – IPS

O IPS consiste em um sistema que protege e monitora uma rede de forma contínua e ativa, isto é, executam uma análise do tráfego da rede, e quando encontram um tráfego suspeito, bloqueiam a ação. Para Tristão *et. al.* (2021), esta ferramenta impede ataques que possam ter ultrapassado as barreiras do *firewall.*

Rangel (2020) define o IPS:

> "O IPS geralmente fica diretamente atrás do *firewall* e fornece uma camada complementar de análise que seleciona negativamente o conteúdo perigoso. Quando colocado em linha, isto é, no caminho de comunicação direta entre fonte e destino, o software analisa ativamente e toma decisões automatizadas e todos os fluxos de tráfego." (RANGEL, pág. 1, 2020)

O IPS irá trabalhar de forma a monitorar a rede do escritório em busca de atividades suspeitas, implementando medidas de prevenção e até mesmo restringindo a atividade suspeita, bloqueando o acesso da pessoa responsável pela ação. Para mais, esta ferramenta agregará enorme valor dentro da organização devido sua grande autonomia, trará mais eficiência para dentro do ambiente.

Backup

Tristão *et. al.* (2021) conceitua backups como sendo cópias de segurança de arquivos e sistemas, processos que garantem a proteção dos dados contra danos ou perdas, sejam estas por meios naturais ou intencionais.

O escritório de contabilidade possui seus dados salvos em nuvem, através do software utilizado por eles – Alterdata Nuvem, porém, é de suma importância que haja a implementação de um serviço de backup extra, para as informações que também são armazenadas em dispositivos físicos, garantindo assim redundância dos dados, podendo ser armazenadas tanto em nuvem, como em forma física e segura, como exemplo, o backup em fitas.

A implementação de um sistema de backup em fitas seria ideal para a estrutura atual do escritório, visto que é um dos meios físicos de armazenamento que possui ótimo custo benefício e grande confiabilidade

Virtual Private Network – VPN

Tristão *et. al.* (2021) define a Rede Virtual Privada – VPN como uma ferramenta que permite que seja realizado um acesso remoto de qualquer lugar com acesso à internet.

Leal e Pereira Filho (2021) expõem que a VPN possibilita que o tráfego pela internet seja realizado de forma privada, onde todos os dados serão enviados e recebidos criptografados, de modo que não será possível que terceiros possam acessá-los. Atuando como um *firewall,* a rede privada protege o computador criando uma espécie de "túnel" próprio para que os dados possam trafegar de forma segura.

A VPN é um elemento necessário dentro de qualquer ambiente profissional e trará uma série de benefícios para o escritório de contabilidade uma vez que possibilitará aos funcionários acessarem os serviços de rede e as informações da empresa e dos clientes em qualquer lugar, necessitando apenas de um dispositivo próprio e de conexão com internet.

Servidor de Rede

Um servidor pode ser conceituado como uma espécie de computador que possui uma configuração mais robusta e com processadores mais potentes. Noleto (2020) ressalta que apesar de operar como as máquinas comuns, um servidor possui uma potência muito superior do que dispositivos como desktops e notebooks.

Devido o escritório de contabilidade ser localizado em um espaço com estrutura pequena, recomenda-se a implementação e utilização de um servidor virtualizado, pois será possível implementar vários servidores virtuais dentro de um único equipamento.

Nas palavras de Mourão (2021), a implementação da virtualização pode ser benéfica para o escritório, pois em se tratando de um *software*, permitirá que a rede de computadores não seja tão dependente da infraestrutura física da organização.

Switch

Os *switches* são os principais componentes de qualquer rede. Eles conectam vários dispositivos, como computadores, *access points* sem fio, impressoras e servidores na mesma rede, seja em um prédio ou no campus. (CISCO, pág. 1. 2022)

Em sua estrutura, o escritório de contabilidade possui um *switch* gerenciado, conforme mostrado na **Figura 1**, porém, há de se ressaltar que se esse equipamento vier a danificar por causas naturais, irá prejudicar toda uma estrutura que está ligada a ele. Logo, é essencial que seja implementado mais um equipamento *switch*, o que, em caso de dano em algum dos equipamentos, a rede não será prejudicada visto que o outro poderá continuar operando normalmente.

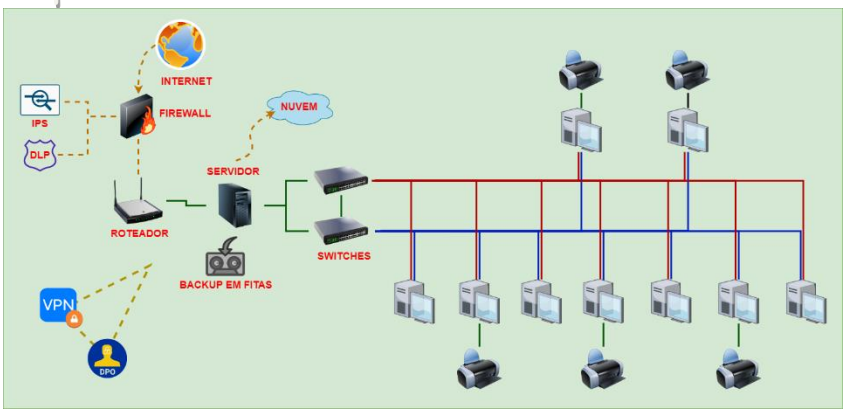
Para Cisco (2022) a utilização de *switches* gerenciados possibilita um ambiente de maior segurança, pois através de seus recursos de flexibilidade podem ser configurados de acordo com as necessidades da rede, permitindo um maior controle e aprimoramento da qualidade dos serviços para os funcionários que utilizarão a rede.

4.4.4 Escritório de Contabilidade com a Implementação das Melhorias

O uso da internet requer muita segurança, visto que por ali passa todos os dados que pode comprometer o futuro de uma empresa. (LEAL, PEREIRA FILHO, pág. 328, 2021)

A infraesturuta da rede do escritório de contabilidade com a implementação das melhorias, em acordo com as políticas da LGPD se dará conforme a **Figura 2**, abaixo:

Figura 2: Infraestrutura de rede do Escritório de Contabilidade com as melhorias.



Fonte: Autoras, 2022

CONSIDERAÇÕES FINAIS

A ascensão da tecnologia nos últimos anos, possibilitou para muitos o acesso e o compartilhamento rápido de dados. Essa evolução requereu uma maior atenção às questões referentes à segurança de informações, solicitando de forma insistente a atenção quanto ao comportamento de muitos profissionais que lidam com este tipo de informação.

Neste contexto, este estudo de caso, buscou observar de que forma ocorria a coleta, o armazenamento e o tratamento das informações em um escritório de contabilidade. Esta investigação se deu por meio de análise em pesquisa qualitativa e quantitativa com auxílio de questionários como ferramenta. E dadas as vulnerabilidades encontradas, tanto em infraestrutura computacional como em humanas, motivou-se a necessidade de propor um modelo adequado para que o ambiente possa se reestruturar de acordo com as novas políticas e diretrizes tratadas na LGPD.

Este trabalho propõe a implementação de melhorias em termos físicos e virtuais no ambiente, com o intuito de tornar os procedimentos quanto ao uso dos dados de forma geral mais seguro e confiável. Pode-se concluir que por meio da implementação desta proposta, com base nas regras e princípios da LGPD, o escritório de contabilidade sofrerá uma série de impactos positivos, já que passarão a trabalhar com mais segurança e um maior comprometimento em se tratando de segurança de dados.

REFERÊNCIAS

AGUIAR, A. C. **A Proteção de Dados no Contrato de Trabalho.** Ano X. n. 97. PUC/SP. Mar. 2021. Disponível em <https://juslaboris-hml.tst.jus.br/bitstream/handle/20.500.12178/142831/2021_aguiar_antonio_protecao_dados.pdf?sequence=1&isAllowed=y> Acesso em 23 de mai. de 2022.

BOTELHO, M. C.; CAMARGO, E. P. A. C.. **A Aplicação da Lei Geral de Proteção de Dados na Saúde**. R. Dir. sanit., São Paulo v.21, e-0021, 2021. Disponível em <https://www.revistas.usp.br/rdisan/article/view/168023/178494> Acesso em 24 de mar de 2022.

BRASIL. Lei 13.709 de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Diário Oficial da República Federativa do Brasil, 15 agosto de 2018. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 20 de mar de 2022

CÂMARA, F. S.. **Lei Geral de Proteção de Dados (LGPD) - Aplicada às Empresas de Contabilidade.** Natal, RN. 2020. Disponível em <https://repositorio.ufrn.br/bitstream/123456789/41227/1/LeiGeraldeProtecao_Camara_2020.pdf>. Acesso em 20 de abr de 2022.

COMO FUNCIONA UM SWITCH. **CISCO**, 2022. Disponível em: <https://www.cisco.com/c/pt_br/solutions/small-business/resource-center/networking/network-switch-how.html> Acesso em: 02 de jun. de 2022.

DONDA, D. **Guia Prático de Implementação da LGPD: tudo o que sua empresa precisa saber para estar em conformidade.** – São Paulo: Labrador, 2020.

GARCIA, L. R. et al. **Lei Geral de Proteção de Dados Pessoais (LGPD): Guia de Implantação.** São Paulo: Bleucher, 2020.

KRÜGER, C. et al. **Lei Geral de Proteção de Dados Pessoais: Uma Análise dos Determinantes Junto aos Profissionais de Contabilidade.** Revista Catarinense da Ciência Contábil, ISSN 2237-7662, Florianópolis, SC, v. 20, 1-19, e3220, 2021. Disponível em: < https://revista.crcsc.org.br/index.php/CRCSC/article/view/3220/2323>. Acesso em: 19 de março de 2022.

LEAL, M. C.; PEREIRA FILHO, M. R. C.. **A Importancia da Vpn (Virtual Private Network) Durante a Pandemia Covid-19: Uma Revisão de Literatura**. Facit Business And Technology Journal. QUALIS B1. ISSN: 2526-4281. Out/Nov - 2021. Ed. 31; V. 1. Págs. 314-332. Disponível em <http://revistas.faculdadefacit.edu.br/index.php/JNT> Acesso em 02 de jun. de 2022.

LEITE, L. V.; LAMBOY, C.; LAPOLLA, M.. **Manual de Implementação da Lei Geral de Proteção de Dados.** São Paulo: Via Ética, 2019.

LIMA, V. H. P.. **LGPD Análise dos Impactos da Implementação em Ambientes Corporativos: Estudo de Caso.** Trabalho de Conclusão de Curso, Pontifícia Universidade Católica de Goiás - Escola de Ciências Exatas e da Computação, Goiânia, 2020. Disponível em <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/108/1/LGPD%20-%20ANALISE%20DOS%20IMPACTOS%20DA%20IMPLEMENTAC%cc%a7A%cc%83O%20-%2003-12%20-%20final.pdf> Acesso em 19 de mar de 2022.

MACIEL, R. F. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. 1. ed. Goiânia: RM Digital Education, 2019.

MARQUES, L. N. (2020). **O mapeamento do modelo data management maturity (dmm) à Lei Geral de Proteção de Dados (LGPD).** Trabalho de Conclusão de Curso, Pontifícia Universidade Católica de Goiás, Goiás, Goiânia, GO, Brasil. Disponível em < https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1289>. Acesso em 20 de mar de 2022.

MOURÃO, Rafael de Melo. **Benefícios na utilização de servidores virtualizados: Economia financeira e facilidade na manutenção e migração.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 06, Ed. 02, Vol. 12, pp. 05-32. Fevereiro de 2021. ISSN: 2448-

0959. Disponível em <https://www.nucleodoconhecimento.com.br/tecnologia/servidores-virtualizados> Acesso em 02 de jun. de 2022.

NOLETO, C. **O que é um servidor e como funciona? TRYBE**, 2020. Disponível em: <https://blog.betrybe.com/tecnologia/o-que-e-servidor/> Acesso em 02 de jun. de 2022.

RANGEL, R. **O que é um IPS (Intrusion Prevention System).** X-Tech Blog, 2020. Disponível em < https://xtech.com.br/Blog/O-Que-E-Um-Ipsintrusion-Prevention-System/b/51/#:~:text=Um%20Sistema%20de%20Preven%C3%A7%C3%A3o%20de,para%20detectar%20e%20prevenir%20vulnerabilidades.> Acesso em 01 de jun. 2022.

RICCI, G. C.; LUZ, G. S.; FERREIRA, L. S. **BYOD E DLP: IMPLEMENTANDO SOLUÇÕES DE SEGURANÇA PARA PREVENÇÃO DE PERDA DE DADOS.** Fatec. São Caetano do Sul, São Paulo, 2020. Disponível em < http://ric.cps.sp.gov.br/bitstream/123456789/5256/1/19_Edna_20200630.pdf> Acesso em 25 de mai. de 2022.

TRISTÃO, G. R. et al. **Lei Geral de Proteção de Dados: Desafios Técnicos enfrentados por microempresas e empresas de pequeno porte.** Congresso de Segurança da Informação das Fatec – Fatec Seg. São Caetano do Sul – São Paulo, 2021.

ANEXO A – QUESTIONÁRIO I

Sobre a organização

1) **A organização possui quantos clientes ao todo?**

27 CLIENTES

2) **A organização possui quantos funcionários ao todo?**

09 FUNCIONÁRIOS

3) **A organização possui algum tipo de fornecedor de produtos (material de escritório, limpeza, etc) ou de serviços (limpeza, serviços de TI, etc)?**

(X) Sim. Quantos? 03 FORNECEDORES
( ) Não

4) **Ao todo, a organização possui quantos ativos ligados à rede? (computadores, servidores, impressoras, etc)**

09 COMPUTADORES ; 05 IMPRESSORAS

5) **A organização tem acesso aos dados de todos os colaboradores, internos e externos à empresa? (clientes, funcionários, fornecedores)**

(X) Sim
( ) Não

Sobre a segurança das informações dentro da organização

6) **Existe uma política de segurança da informação na organização?**

(X) Sim. Qual? _____
( ) Não

7) **A segurança das informações está de acordo com os requisitos legais vigentes?**

( ) Sim
(X) Não

8) **Quem pode acessar os dados dentro da organização?**

( ) Ninguém
( ) Somente a gerência
( ) Somente os funcionários
(X) Todos (gerência e funcionários)
( ) Outros _____

9) Todos os dados coletados são realmente necessários para o propósito de seu processamento? (envio de e-mail, serviços de rotina, etc)

(X) Sim
( ) Não

Qual(is) o(s) propósito(s)? GARANTIR A QUALIDADE DO SERVIÇO, BEM COMO O PRÓPRIO FUNCIONAMENTO DO ESCRITÓRIO.

10) Quais os tipos de dados que a organização solicita a seus clientes? (Pode marcar mais de uma opção).

[X] Dados Pessoais (nome, sobrenome; CPF, RG, gênero, data e local de nascimento, telefone, endereço residencial, renda, cartão bancário)

[ ] Dados Pessoais Sensíveis (posicionamento religioso, orientação sexual, posicionamento político, biometria, filiação sindical, dados relativos à saúde)

[X] Dados Financeiros (faturamento, lucro, lucratividade)

[ ] Outros. Quais? _____

11) A organização possui recursos de segurança da informação adequados contra ameaças internas e externas? (boas práticas por parte da gerência e dos funcionários)

( ) Sim. Quais? _____
(X) Não

12) A organização possui recursos tecnológicos adequados para apoiar a segurança dos dados? (antivírus, firewall, etc)

(X) Sim. Quais? ANTIVÍRUS; DADOS EM NUVEM
( ) Não

13) A organização dispõe de procedimentos para detectar e punir violações de segurança de informações?

( ) Sim. Quais? _____
(X) Não

14) A organização se preocupa com a proteção dos seus dados e de seus clientes?

(X) Sim

( ) Não

15) Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?

10. POIS TRABALHAMOS COM INFORMAÇÕES DE DIVERSAS EMPRESAS E PESSOAS EM VARIADOS SETORES DE PRESTAÇÃO DE SERVIÇOS.

16) A organização tem conhecimento da Lei Geral de Proteção de Dados - LGPD?

(X) Sim
( ) Não

17) A organização tem conhecimento sobre as sanções que pode sofrer se estiver em desacordo com a LGPD?

(X) Sim
( ) Não

ANEXO B – QUESTIONÁRIO II

Nome: [redacted]

Idade: 46 anos

Função: Auxiliar de escritório

Sobre a organização

1) **Existe uma política de segurança da informação dentro da organização?**

( ) Sim
(X) Não

2) **A organização realiza investimentos em segurança da informação sempre que necessário?**

( ) Sim
(X) Não

3) **A organização possui alguma equipe de TI capacitada para contribuir com a segurança dos dados?**

( ) Sim
(X) Não

4) **A organização já sofreu algum tipo de ataque/violação de dados? (vazamento de dados, ataques de hackers, etc)**

( ) Sim. Qual? _____
(X) Não

5) **Os computadores possuem algum sistema/software antivírus ou firewall?**

(X) Sim
( ) Não

Sobre sua rotina diária

6) **Cumprir com as políticas de segurança das informações é algo que pertence à minha rotina...**

( ) Sim. Com que frequência? _____
(X) Não

7) Você lida diariamente com o tratamento de dados dos clientes?

(X) Sim
( ) Não

8) Em sua rotina diária, de que forma você armazena/trata os dados presentes na organização? (Pode marcar mais de uma opção).

[X] Planilhas/Excel

[ ] Programa interno da organização. Qual? _____

[X] Sistema em nuvem. Qual? ALTERDATA

[ ] Outros. Quais? _____

9) De que forma você solicita os dados dos clientes da organização?

[X] Telefone
[X] E-mail
[X] Presencialmente
[X] São solicitados somente os dados que serão utilizados
[ ] São solicitados todas os dados, ainda que para utilização posterior

10) Você possui conhecimento sobre as ferramentas e práticas de segurança de informações?

( ) Sim
(X) Não

Quais: _____

11) Você conhece a Lei Geral de Proteção de Dados - LGPD?

( ) Sim
(X) Não

12) Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?

10

ANEXO C – QUESTIONÁRIO II

Nome: [redacted]

Idade: 54

Função: Auxiliar de portabilidade

Sobre a organização

1) **Existe uma política de segurança da informação dentro da organização?**

( ) Sim
(X) Não

2) **A organização realiza investimentos em segurança da informação sempre que necessário?**

( ) Sim
(X) Não

3) **A organização possui alguma equipe de TI capacitada para contribuir com a segurança dos dados?**

( ) Sim
(X) Não

4) **A organização já sofreu algum tipo de ataque/violação de dados? (vazamento de dados, ataques de hackers, etc)**

( ) Sim. Qual? _____
(X) Não

5) **Os computadores possuem algum sistema/software antivírus ou firewall?**

(X) Sim
( ) Não

Sobre sua rotina diária

6) **Cumprir com as políticas de segurança das informações é algo que pertence à minha rotina...**

( ) Sim. Com que frequência? _____
(X) Não

7) **Você lida diariamente com o tratamento de dados dos clientes?**

(X) Sim
( ) Não

8) **Em sua rotina diária, de que forma você armazena/trata os dados presentes na organização? (Pode marcar mais de uma opção).**

[ ] Planilhas/Excel

[ ] Programa interno da organização. Qual? _____

[X] Sistema em nuvem. Qual? Alterdata

[ ] Outros. Quais? _____

9) **De que forma você solicita os dados dos clientes da organização?**

[X] Telefone
[X] E-mail
[ ] Presencialmente
[ ] São solicitados somente os dados que serão utilizados
[ ] São solicitados todas os dados, ainda que para utilização posterior

10) **Você possui conhecimento sobre as ferramentas e práticas de segurança de informações?**

( ) Sim
(X) Não

Quais: _____

11) **Você conhece a Lei Geral de Proteção de Dados - LGPD?**

( ) Sim
(X) Não

12) **Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?**

10

ANEXO D – QUESTIONÁRIO II

Nome: [redacted]

Idade: 32 ANOS

Função: SETOR ADMINISTRATIVO E FINANCEIRO

Sobre a organização

1) **Existe uma política de segurança da informação dentro da organização?**

(X) Sim, IMPLICITAMENTE
( ) Não

2) **A organização realiza investimentos em segurança da informação sempre que necessário?**

(X) Sim
( ) Não

3) **A organização possui alguma equipe de TI capacitada para contribuir com a segurança dos dados?**

( ) Sim
(X) Não

4) **A organização já sofreu algum tipo de ataque/violação de dados? (vazamento de dados, ataques de hackers, etc)**

( ) Sim. Qual? _____
(X) Não

5) **Os computadores possuem algum sistema/software antivírus ou firewall?**

(X) Sim
( ) Não

Sobre sua rotina diária

6) **Cumprir com as políticas de segurança das informações é algo que pertence à minha rotina...**

(X) Sim. Com que frequência? MENSALMENTE (1 OU 2 VEZES)
( ) Não

7) **Você lida diariamente com o tratamento de dados dos clientes?**

( ) Sim
(X) Não

8) **Em sua rotina diária, de que forma você armazena/trata os dados presentes na organização? (Pode marcar mais de uma opção).**

[X] Planilhas/Excel

[ ] Programa interno da organização. Qual? _____

[X] Sistema em nuvem. Qual? ALTER.DATA

[ ] Outros. Quais? _____

9) **De que forma você solicita os dados dos clientes da organização?**

[X] Telefone
[X] E-mail
[ ] Presencialmente
[X] São solicitados somente os dados que serão utilizados
[ ] São solicitados todas os dados, ainda que para utilização posterior

10) **Você possui conhecimento sobre as ferramentas e práticas de segurança de informações?**

( ) Sim
(X) Não

Quais: _____

11) **Você conhece a Lei Geral de Proteção de Dados - LGPD?**

(X) Sim
( ) Não

12) **Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?**

10. POIS TRABALHAMOS COM INFORMAÇÕES DE DIVERSAS EMPRESAS E PESSOAS EM VARIADOS SETORES DE PRESTAÇÃO DE SERVIÇOS.

ANEXO E – QUESTIONÁRIO II

Nome: [redacted]

Idade: 61

Função: Auxiliar contábil

Sobre a organização

1) **Existe uma política de segurança da informação dentro da organização?**

( ) Sim
(X) Não

2) **A organização realiza investimentos em segurança da informação sempre que necessário?**

( ) Sim
(X) Não

3) **A organização possui alguma equipe de TI capacitada para contribuir com a segurança dos dados?**

( ) Sim
(X) Não

4) **A organização já sofreu algum tipo de ataque/violação de dados? (vazamento de dados, ataques de hackers, etc)**

( ) Sim. Qual? _____
(X) Não

5) **Os computadores possuem algum sistema/software antivírus ou firewall?**

( ) Sim
(X) Não

Sobre sua rotina diária

6) **Cumprir com as políticas de segurança das informações é algo que pertence à minha rotina...**

( ) Sim. Com que frequência? _____
(X) Não

7) Você lida diariamente com o tratamento de dados dos clientes?

( ) Sim
(X) Não

8) Em sua rotina diária, de que forma você armazena/trata os dados presentes na organização? (Pode marcar mais de uma opção).

[X] Planilhas/Excel

[ ] Programa interno da organização. Qual? _____

[ ] Sistema em nuvem. Qual? _____

[ ] Outros. Quais? _____

9) De que forma você solicita os dados dos clientes da organização?

[ ] Telefone
[ ] E-mail
[ ] Presencialmente
[X] São solicitados somente os dados que serão utilizados
[ ] São solicitados todas os dados, ainda que para utilização posterior

10) Você possui conhecimento sobre as ferramentas e práticas de segurança de informações?

( ) Sim
(X) Não

Quais: _____

11) Você conhece a Lei Geral de Proteção de Dados - LGPD?

( ) Sim
(X) Não

12) Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?

10

ANEXO F – QUESTIONÁRIO II

Nome: [redacted]

Idade: 48

Função: Técnico Informática

Sobre a organização

1) **Existe uma política de segurança da informação dentro da organização?**

( ) Sim
(X) Não

2) **A organização realiza investimentos em segurança da informação sempre que necessário?**

( ) Sim
(X) Não

3) **A organização possui alguma equipe de TI capacitada para contribuir com a segurança dos dados?**

( ) Sim
(X) Não

4) **A organização já sofreu algum tipo de ataque/violação de dados? (vazamento de dados, ataques de hackers, etc)**

( ) Sim. Qual? _____
(X) Não

5) **Os computadores possuem algum sistema/software antivírus ou firewall?**

(X) Sim
( ) Não

Sobre sua rotina diária

6) **Cumprir com as políticas de segurança das informações é algo que pertence à minha rotina...**

(X) Sim. Com que frequência? na medida do possível
( ) Não

7) Você lida diariamente com o tratamento de dados dos clientes?

(X) Sim
( ) Não

8) Em sua rotina diária, de que forma você armazena/trata os dados presentes na organização? (Pode marcar mais de uma opção).

[ ] Planilhas/Excel

[ ] Programa interno da organização. Qual? _____

[X] Sistema em nuvem. Qual? Agendata

[ ] Outros. Quais? _____

9) De que forma você solicita os dados dos clientes da organização?

[X] Telefone
[X] E-mail
[X] Presencialmente
[ ] São solicitados somente os dados que serão utilizados
[ ] São solicitados todas os dados, ainda que para utilização posterior

10) Você possui conhecimento sobre as ferramentas e práticas de segurança de informações?

(X) Sim
( ) Não

Quais: antivirus, controlar acesso, (pouco conhecimento)

11) Você conhece a Lei Geral de Proteção de Dados - LGPD?

( ) Sim
(X) Não

12) Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?

5

ANEXO G – QUESTIONÁRIO II

Nome: [redacted]

Idade: 39 anos

Função: Contadora

Sobre a organização

1) **Existe uma política de segurança da informação dentro da organização?**

( ) Sim
(X) Não

2) **A organização realiza investimentos em segurança da informação sempre que necessário?**

( ) Sim
(X) Não

3) **A organização possui alguma equipe de TI capacitada para contribuir com a segurança dos dados?**

( ) Sim
(X) Não

4) **A organização já sofreu algum tipo de ataque/violação de dados? (vazamento de dados, ataques de hackers, etc)**

( ) Sim. Qual? _____
(X) Não

5) **Os computadores possuem algum sistema/software antivírus ou firewall?**

(X) Sim
( ) Não

Sobre sua rotina diária

6) **Cumprir com as políticas de segurança das informações é algo que pertence à minha rotina...**

( ) Sim. Com que frequência? _____
(X) Não

7) **Você lida diariamente com o tratamento de dados dos clientes?**

(X) Sim
( ) Não

8) **Em sua rotina diária, de que forma você armazena/trata os dados presentes na organização? (Pode marcar mais de uma opção).**

[ ] Planilhas/Excel

[ ] Programa interno da organização. Qual? _____

[x] Sistema em nuvem. Qual? Alterdata

[ ] Outros. Quais? _____

9) **De que forma você solicita os dados dos clientes da organização?**

[ ] Telefone
[x] E-mail
[ ] Presencialmente
[ ] São solicitados somente os dados que serão utilizados
[ ] São solicitados todas os dados, ainda que para utilização posterior

10) **Você possui conhecimento sobre as ferramentas e práticas de segurança de informações?**

( ) Sim
(x) Não

Quais: _____

11) **Você conhece a Lei Geral de Proteção de Dados - LGPD?**

( ) Sim
(X) Não

12) **Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?**

10

ANEXO H – QUESTIONÁRIO II

Nome: [redacted]

Idade: 40

Função: Auxiliar de Escritório.

Sobre a organização

1) **Existe uma política de segurança da informação dentro da organização?**

( ) Sim
(X) Não

2) **A organização realiza investimentos em segurança da informação sempre que necessário?**

( ) Sim
(X) Não

3) **A organização possui alguma equipe de TI capacitada para contribuir com a segurança dos dados?**

( ) Sim
(X) Não

4) **A organização já sofreu algum tipo de ataque/violação de dados? (vazamento de dados, ataques de hackers, etc)**

( ) Sim. Qual? _____
(X) Não

5) **Os computadores possuem algum sistema/software antivírus ou firewall?**

(X) Sim
( ) Não

Sobre sua rotina diária

6) **Cumprir com as políticas de segurança das informações é algo que pertence à minha rotina...**

(X) Sim. Com que frequência? diariamente
( ) Não

7) **Você lida diariamente com o tratamento de dados dos clientes?**

(X) Sim
( ) Não

8) **Em sua rotina diária, de que forma você armazena/trata os dados presentes na organização? (Pode marcar mais de uma opção).**

[ ] Planilhas/Excel

[ ] Programa interno da organização. Qual? _____

[X] Sistema em nuvem. Qual? Sefrosata / Windows

[ ] Outros. Quais? _____

9) **De que forma você solicita os dados dos clientes da organização?**

[ ] Telefone
[X] E-mail
[ ] Presencialmente
[ ] São solicitados somente os dados que serão utilizados
[ ] São solicitados todas os dados, ainda que para utilização posterior

10) **Você possui conhecimento sobre as ferramentas e práticas de segurança de informações?**

( ) Sim
(X) Não

Quais: _____

11) **Você conhece a Lei Geral de Proteção de Dados - LGPD?**

(X) Sim
( ) Não

12) **Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?**

10

ANEXO I – QUESTIONÁRIO II

Nome: [redacted]

Idade: 47

Função: Cozinha

Sobre a organização

1) **Existe uma política de segurança da informação dentro da organização?**

( ) Sim
(X) Não

2) **A organização realiza investimentos em segurança da informação sempre que necessário?**

( ) Sim
(X) Não

3) **A organização possui alguma equipe de TI capacitada para contribuir com a segurança dos dados?**

( ) Sim
(X) Não

4) **A organização já sofreu algum tipo de ataque/violação de dados? (vazamento de dados, ataques de hackers, etc)**

( ) Sim. Qual? _____
(X) Não

5) **Os computadores possuem algum sistema/software antivírus ou firewall?**

(X) Sim
( ) Não

Sobre sua rotina diária

6) **Cumprir com as políticas de segurança das informações é algo que pertence à minha rotina...**

( ) Sim. Com que frequência? _____
(X) Não

7) Você lida diariamente com o tratamento de dados dos clientes?

( ) Sim
(X) Não

8) Em sua rotina diária, de que forma você armazena/trata os dados presentes na organização? (Pode marcar mais de uma opção).

[ ] Planilhas/Excel

[ ] Programa interno da organização. Qual? _____

[X] Sistema em nuvem. Qual? DATABRICKS

[ ] Outros. Quais? _____

9) De que forma você solicita os dados dos clientes da organização?

[ ] Telefone
[X] E-mail
[ ] Presencialmente
[X] São solicitados somente os dados que serão utilizados
[ ] São solicitados todas os dados, ainda que para utilização posterior

10) Você possui conhecimento sobre as ferramentas e práticas de segurança de informações?

( ) Sim
(X) Não

Quais: _____

11) Você conhece a Lei Geral de Proteção de Dados - LGPD?

(X) Sim
( ) Não

12) Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?

10

ANEXO J – QUESTIONÁRIO II

Nome: [redacted]

Idade: 52 ANOS

Função: TEC. EM CONTABILIDADE

Sobre a organização

1) Existe uma política de segurança da informação dentro da organização?

( ) Sim
(X) Não

2) A organização realiza investimentos em segurança da informação sempre que necessário?

( ) Sim
(X) Não

3) A organização possui alguma equipe de TI capacitada para contribuir com a segurança dos dados?

( ) Sim
(X) Não

4) A organização já sofreu algum tipo de ataque/violação de dados? (vazamento de dados, ataques de hackers, etc)

( ) Sim. Qual? _____
(X) Não

5) Os computadores possuem algum sistema/software antivírus ou firewall?

(X) Sim
( ) Não

Sobre sua rotina diária

6) Cumprir com as políticas de segurança das informações é algo que pertence à minha rotina...

( ) Sim. Com que frequência? _____
(X) Não

7) Você lida diariamente com o tratamento de dados dos clientes?

(X) Sim
( ) Não

8) Em sua rotina diária, de que forma você armazena/trata os dados presentes na organização? (Pode marcar mais de uma opção).

[ ] Planilhas/Excel

[ ] Programa interno da organização. Qual? _____

[X] Sistema em nuvem. Qual? ALTERDATA

[ ] Outros. Quais? _____

9) De que forma você solicita os dados dos clientes da organização?

[X] Telefone
[X] E-mail
[X] Presencialmente
[X] São solicitados somente os dados que serão utilizados
[ ] São solicitados todas os dados, ainda que para utilização posterior

10) Você possui conhecimento sobre as ferramentas e práticas de segurança de informações?

( ) Sim
(X) Não

Quais: _____

11) Você conhece a Lei Geral de Proteção de Dados - LGPD?

( ) Sim
(X) Não

12) Em sua opinião, defina em uma escala de 0 a 10, qual o nível de importância da implementação de uma política de segurança de informações dentro da organização?

10