O PROCESSO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS: UM ESTUDO DE CASO EM UMA EMPRESA DO SEGMENTO DA SAÚDE

Recebido em: 24/08/2023
Aceito em: 22/09/2023
DOI: 10.25110/receu.v24i1-009

Fabiano Santos Quintanilha [1]
Vinicius Barcelos da Silva [2]

RESUMO: Após a criação em 2018 da Lei Geral de Proteção de Dados (LGPD), as organizações brasileiras iniciaram projetos de adequação à LGPD, visando melhorar a segurança da informação, evitando incidentes que possam comprometer a continuidade do negócio e gerar penalidades conforme a lei. O objetivo deste artigo é mostra na íntegra o processo de adequação à LGPD de uma empresa no seguimento da saúde localizada no estado do Rio de Janeiro, com levantamento dos problemas existentes e aplicação das melhores práticas de segurança da informação. Esta adequação ocorreu em um período conturbado de pandemia, onde os custos operacionais no seguimento da saúde foram elevados, o que tornou este trabalho ainda mais difícil. O estudo de caso foi a metodologia empregada neste trabalho, que permitiu uma investigação aprofundada das medidas adotadas pela empresa em seu processo de adequação a nova lei. Após diversas ações/mudanças organizacionais, culturais e tecnológicas, a empresa conseguiu alcançar o mínimo de adequação às boas práticas de segurança da informação. Como resultado, após o trabalho realizado, não foi identificado nenhum incidente grave relacionado à segurança dos dados na empresa em questão.
PALAVRAS-CHAVE: LGPD; Lei Geral de Proteção de Dados; Segurança da Informação.

THE PROCESS OF ADAPTATION TO THE GENERAL DATA PROTECTION LAW: A CASE STUDY IN A COMPANY IN THE HEALTH SEGMENT

ABSTRACT: After the creation of the General Data Protection Law (GDPL) in 2018, Brazilian organizations started adaptation projects to the GDPL, aiming to improve information security, avoiding incidents that could compromise the continuity of the business and generate penalties according to the law. The objective of this article is to show in full the process of adapting to the GDPL of a company in the health segment located in the state of Rio de Janeiro, with a survey of existing problems and application of best information security practices. This adjustment took place in a troubled period of the pandemic, where operating costs in the health segment were high, which made this work even more difficult. The case study was the methodology used in this work, which allowed an in-depth investigation of the measures adopted by the company in its adaptation process to the new law. After several organizational, cultural and technological actions/changes, the company managed to achieve the minimum adequacy to good information security practices. As a result, after the work carried out, no serious incident related to data security was identified in the company in question.

[1] Especialista em Redes de Computadores e Telecomunicações. Instituto Federal Fluminense (IFF).
E-mail: fabianoquintanilha@yahoo.com.br
[2] Mestre em Engenharia de Produção. Instituto Federal Fluminense (IFF).
E-mail: viniciusbs@iff.edu.br

KEYWORDS: GDPL; General Data Protection Law; Information Security.

EL PROCESO DE ADAPTACIÓN A LA LEY GENERAL DE PROTECCIÓN DE DATOS: UN ESTUDIO DE CASO EN UNA EMPRESA DEL SEGMENTO SALUD

RESUMEN: Luego de la creación de la Ley General de Protección de Datos (LGPD) en 2018, las organizaciones brasileñas iniciaron proyectos de adaptación a la LGPD, con el objetivo de mejorar la seguridad de la información, evitando incidentes que puedan comprometer la continuidad del negocio y generar sanciones conforme a la ley. El objetivo de este artículo es mostrar de manera integral el proceso de adaptación a la LGPD de una empresa del segmento de salud ubicada en el estado de Río de Janeiro, con un levantamiento de los problemas existentes y la aplicación de mejores prácticas de seguridad de la información. Este ajuste se produjo en un período convulso de la pandemia, donde los costos operativos en el segmento de salud eran elevados, lo que dificultó aún más este trabajo. El estudio de caso fue la metodología utilizada en este trabajo, el cual permitió investigar en profundidad las medidas adoptadas por la empresa en su proceso de adaptación a la nueva ley. Luego de varias acciones/cambios organizacionales, culturales y tecnológicos, la empresa logró alcanzar la mínima adecuación a las buenas prácticas de seguridad de la información. Como resultado, tras los trabajos realizados no se identificó ningún incidente grave relacionado con la seguridad de los datos en la empresa en cuestión.
PALABRAS CLAVE: LGPD; Ley General de Protección de Datos; Seguridad de la Información.

1. INTRODUÇÃO

Nos últimos anos, um importante acontecimento mundial na área de segurança da informação foi à introdução da General Protection Data Regulation (GPDR) na União Europeia (UE) em 24 de maio de 2016, idealizada após diversos escândalos de espionagem, divulgação e roubo de dados dos cidadãos europeus (CARVALHO et al., 2019). Uma das principais disposições consiste no fato de, para realizar negócios com a UE, o parceiro comercial necessita ter um programa interno de proteção de dados.

A partir deste momento, houve uma corrida mundial para criação de suas legislações, o que não foi diferente no Brasil com a criação da lei 13.709/18, a nossa Lei Geral de Proteção de Dados (LPGD), que dispõe sobre o tratamento dos dados pessoais.

A criação da LGPD ocorreu em um momento oportuno, uma vez que se observou um aumento significativo de vazamento de dados no país. Uma pesquisa realizada por Neto et al. (2021) verificou um aumento de 493% nos vazamentos de dados no Brasil entre os anos de 2018 e 2019, sendo vazados mais de 205 milhões de informações confidenciais de forma criminosa apenas em 2019. De acordo com o estudo, a quantidade

de grandes incidentes de segurança de dados no Brasil saltou de três no ano de 2018 para dezesseis grandes incidentes em 2019.

A LGPD de fato entrou em vigor em setembro de 2020, tendo como prazo limite de adequação a lei o dia 1º de agosto de 2021, sendo válido para todos os seguimentos, tanto público, privado e pessoas físicas com objetivos econômicos, dispondo sobre o tratamento de dados pessoais inseridos em meios físicos ou digitais. O modelo tem como foco principal a proteção dos dados pessoais dos indivíduos com o objetivo de proteger os direitos fundamentais de liberdade e privacidade, e qualquer ação com referência ao uso desses dados é necessário ter o consentimento legal do cidadão e cuidado em sua utilização (BRASIL, 2018).

Especificamente no segmento de saúde, os dados sensíveis estão em grande parte do ecossistema, no qual dados de pacientes são compartilhados entre diferentes profissionais, empresas e organizações. O prontuário de um paciente, por exemplo, contém informações sensíveis sobre a pessoa física e podem seguir um fluxo de compartilhamento entre diversos médicos na busca por diagnósticos mais precisos, envolvendo atendimentos em hospitais, clínicas, laboratórios, sendo alguns dados enviados até para a Agência Nacional de Saúde (ANS). Portanto, há uma forte demanda no processo de proteção dos dados manipulados por empresas do segmento de saúde.

O objetivo deste artigo é mostrar na íntegra o processo de adequação à LGPD em uma empresa no seguimento da saúde localizada no estado do Rio de Janeiro, com levantamento dos problemas existentes e aplicação das melhores práticas de segurança da informação. Esta adequação ocorreu durante a pandemia, um período conturbado com um forte desinvestimento no seguimento, tornando este trabalho ainda mais desafiador. Importante destacar que este artigo descreve o trabalho realizado por diversas equipes/setores, e registram-se aqui as melhores práticas ocorridas na empresa na busca da adequação à LGPD.

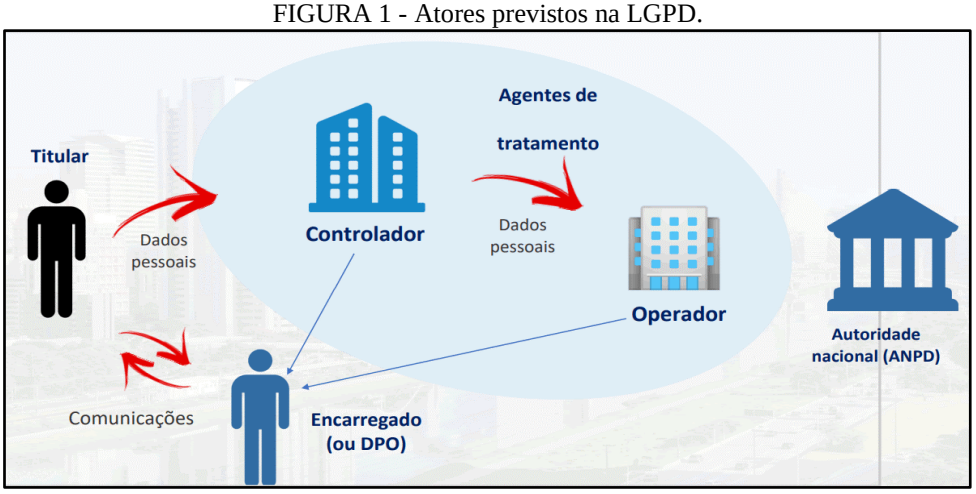
Embora existam na literatura diversos trabalhos analisando os impactos da LGPD nas empresas sob diversas óticas, trabalhos descrevendo o processo de adequação de uma organização à LGPD brasileira são escassos. Desta forma, este estudo se justifica, pois descreve minuciosamente todo o processo de adequação à LGPD em uma empresa do segmento de saúde, servindo como um referencial orientador para outras organizações que também necessitam se ajustar ao novo contexto regulatório de segurança da informação.

Este artigo está organizado da seguinte forma: na seção 2 é realizada uma análise sobre a lei geral de proteção de dados, identificando os atores responsáveis pela proteção de dados e suas responsabilidades; na seção 3 é realizada a descrição da empresa alvo deste trabalho; na seção 4 e em suas subseções é descrito todo o processo de adequação à LGPD ocorrido na empresa; na seção 5 são discutidos os resultados de todo o processo; por fim, são apresentadas as considerações finais deste trabalho.

2. LEI GERAL DE PROTEÇÃO DE DADOS

A publicação da Lei Geral de Proteção de Dados (LGPD) foi o marco de uma revolução tecnológica em nosso país. Esta lei dispõe sobre o tratamento de dados pessoais realizados por pessoas físicas e jurídicas, seja no ambiente público ou privado, visando proteger os direitos de liberdade e privacidade das pessoas. Os dados pessoais são informações relacionadas à pessoa natural identificada ou possível de ser identificada (BRASIL, 2018).

FIGURA 1 - Atores previstos na LGPD.



Fonte: Silva (2020).

Conforme figura 1, a LGPD define os atores envolvidos na organização dos dados pessoais, sendo estes: o titular do dado, composto por todas as pessoais físicas; o controlador do dado, em geral composto pela empresa que coleta o dado e pede o consentimento ao titular, podendo tratar este tipo de dado se o mesmo estiver na finalidade do negócio; o operador, composto por terceiros do controlador, tais como empresas de laboratórios, médicos externos, entre outros, que podem obter os dados pessoais via controlador e utilizar no seu negócio, ao qual competem as mesmas responsabilidades de proteção dos dados do controlador; o Data Protection Officer (DPO), sendo o encarregado

na organização pela proteção dos dados; e por fim a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela fiscalização e aplicação dos sansões (SILVA, 2020).

Dentre os atores supracitados, um dos principais é o DPO. O controlador deverá definir um profissional para ser seu DPO. De acordo com art. 41 da LGPD, as principais atividades do DPO são: aceitar reclamações e comunicações dos titulares; prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; e orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais (BRASIL, 2018).

Com a LGPD, pessoas físicas que possuem dados em algum controlador passaram a ter direitos, inclusive à possibilidade de questionamento sobre a utilização desses dados. A organização deve promover internamente a cultura de proteção dos dados, visando prevenir incidentes de segurança, através de ações pró-ativas a fim de evitar o acesso indevido e o vazamento de informações.

As penalidades também estão mais rígidas para as organizações em caso de vazamento de dados, sendo divididas nas seguintes categorias: eliminação de dados vazados; advertência e prazo; bloqueio do tratamento de dados, e consequentemente proibição no tratamento de dados; publicização do incidente, que consiste na compra de um espaço publicitário a fim de informar sobre o vazamento de dados; multa de até 2% do faturamento, limitado a 50 milhões; multa diária até o teto (BRASIL, 2018).

Embora existam na literatura diversos trabalhos analisando os impactos da LGPD nas empresas sob diversas ópticas, trabalhos descrevendo o processo de adequação de uma organização à Lei Geral de Proteção de Dados brasileira são escassos. Dentre os trabalhos encontrados, pode-se destacar:

- Rojas (2020), que verificou a aplicação da LGPD no Instituto Federal de Santa Catarina (IFSC), constatando que a Instituição se encontrava no estágio inicial de adequação à Lei, o que o autor considerou crítico em razão do volume trabalho que consiste em adequação dos processos e sistemas;
- Soares (2023), que analisou o modelo de adequação a LGPD em uma empresa que presta serviços de tecnologia corporativa no estado de Sergipe, realizado por uma empresa de consultoria em LGPD. Os resultados analisados comprovaram a eficiência do modelo de adequação à LGPD aplicado na empresa foco do estudo.
- Pereira (2023) descreveu o processo de adequação que iniciou em março de 2021 na Universidade Federal de Santa Catarina (UFSC), por meio de um grupo de trabalho instituído por portaria, mas que foi interrompido e encontra-se estagnado

devido a não renovação dessa portaria pela reitoria. Ele conclui que "o processo de adequação é muito mais complexo do que parece à primeira vista e exige dedicação e comprometimento de toda a hierarquia universitária, pois trata-se, no fundo, de uma mudança de cultura organizacional".

Desta forma, dado a escassa quantidade de trabalhos sobre o tema na literatura, este estudo é grande importância ao descrever minuciosamente todo o processo de adequação à LGPD em uma empresa do segmento de saúde.

3. DESCRIÇÃO DO CENÁRIO

Este artigo mostra o processo de adequação à LGPD em uma empresa do seguimento de saúde do interior do estado do Rio de Janeiro. Esta empresa possui aproximadamente 800 colaboradores, dois datacenters, aproximadamente 700 estações de trabalho, cerca de 50 servidores virtualizados e algumas dezenas de sistemas voltados para gestão hospitalar.

Um ponto importante a ser observar é que antes da LGPD a empresa não tinha um setor específico de segurança da informação, qualquer assunto relacionado à segurança era absorvido pela equipe de infraestrutura de TI, que de fato não tinha recursos humanos suficientes para gerir este item.

No aspecto tecnológico, existia na organização: sistema de firewall simples com ACLs manuais; um controle de acesso à internet com pouca flexibilidade, sem controle de categoria, utilizando bloqueio por palavras de forma manual e não dinâmica; sistema de antivírus nas estações de trabalho e servidores e que não realizavam bloqueio de dispositivos de forma nativa; sistema de backup realizado somente em fita; rede sem fio mal estruturada; usuários genéricos em praticamente todos os setores; utilização de senhas fracas; pouco controle do acesso externo via VPN; hardware e sistemas operacionais obsoletos, entre outros problemas.

4. PROCESSO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS

O processo de adequação à LGPD na empresa em questão foi um grande desafio, pois as aplicações das mudanças organizacionais e tecnológicas ocorreram juntamente com o período de combate à pandemia. De forma semelhante à descrita por Winkert et al. (2022), os custos hospitalares na empresa também foram elevados no período da pandemia, resultando em alto impacto financeiro.

Neste período, o setor de infraestrutura de TI foi levado ao seu extremo, pois muitas ações precisavam ser feitas visando adequação à LGPD, ao mesmo tempo em que outros trabalhos eram realizados a fim de conter a pandemia, como criação de centros de combate a COVID-19 com toda infraestrutura tecnológica para apoio ao paciente e a equipe hospitalar.

Inicialmente, foi realizado um trabalho dentro da empresa a fim de identificar os principais problemas relacionados à segurança da informação, categorizando-os como de gravidade baixa, média e alta, e entender qual o cenário ideal que se deseja alcançar de acordo com investimentos atuais e futuros destinados a serem aplicados ao projeto.

A partir deste momento, foi gerado um plano de ação macro para toda a organização. De forma sucinta, podem-se destacar as seguintes ações/mudanças que compuseram o plano de ação macro em busca da adequação à LGPD:

- Criação do setor de Segurança da Informação e montagem da equipe;
- Definição do Data Protection Officer (DPO);
- Envolvimento da governança, através da criação do Comitê Gestor de Segurança da Informação;
- Criação e divulgação da Política de Segurança da Informação (PSI);
- Revisão dos contratos com os fornecedores;
- Entrevista técnica com todos os colaboradores da empresa;
- Estruturação do Firewall da empresa;
- Estruturação do sistema de Backup da empresa;
- Estruturação da segurança das Estações de Trabalho;
- Estruturação da segurança da Rede Local de Computadores;
- Estruturação da segurança da Rede Sem Fio;
- Estruturação da segurança do Active Directory;
- Estruturação da segurança do home office da empresa;
- Estruturação da criptografia de sistemas;
- Estruturação do processo de atualização e correção das vulnerabilidades em servidores e equipamentos de rede;

O detalhamento dessas mudanças será apresentado nas próximas subseções.

4.1 Criação do Setor de Segurança da Informação e Montagem da Equipe

Na empresa em questão, o passo executado logo após a criação do plano de ação macro foi à criação do setor de Segurança da Informação, responsável por conduzir o projeto de adequação à LGPD. Este setor contribui com a TI, porém atua de forma independente. Esta independência é importante, pois a partir de agora os conflitos de interesse poderão se aflorar, visto que a identificação de uma vulnerabilidade detectada por uma equipe será a geração de um "problema" a ser resolvida pela outra equipe.

Este setor deverá conter profissionais com sólidos conhecimentos em redes de computadores, servidores e serviços de rede, sistemas operacionais, entre outros. Inicialmente foi dedicado somente um profissional para esta nova hierarquia, profissional este que já pertencia à equipe de infraestrutura de TI, pois ele atendia aos requisitos iniciais e no momento não havia recursos financeiros para a contratação de outros profissionais de imediato.

4.2 Definição do Data Protection Officer (DPO)

A próxima etapa foi definir o DPO da instituição. É importante destacar que este profissional não é subordinado a TI, mas sim a governança. Ele precisa de sólidos conhecimentos em segurança da informação, jurídicos e de regulação, além de excelente capacidade de comunicação, diálogo, reação pró-ativa, entre outros.

Não há na lei impedimento deste profissional ser ligado a equipe de TI ou a de segurança da informação. Desta forma, o profissional de infraestrutura que foi migrado para o setor de segurança também passou a acumular o cargo de DPO.

4.3 Envolvimento da Governança, Através da Criação do Comitê Gestor de Segurança da Informação

O próximo passo do plano de ação macro foi garantir o envolvimento da governança perante a LGPD na organização. A norma ISO/IEC TR 13335-2 (1997), que descreve o processo completo de gerenciamento de riscos de segurança da informação de maneira genérica, recomenda que os representantes de todos os setores estejam comprometidos com a Segurança da Informação da empresa, sendo este comprometimento obtido através da criação de um comitê ou fórum de segurança da informação, que deve realizar encontros periódicos a fim de respaldar o trabalho da equipe de segurança da informação da empresa.

Este é um dos principais pilares da LGPD, pois tudo que faz referência a LGPD em uma organização não funcionará sem o comprometimento da alta gestão. Os diretores, principalmente dos setores que manipulam dados sensíveis, devem conhecer a LGPD, compreender a importância os dados empresariais na continuidade do negócio e acompanhar o tratamento das informações junto com o DPO.

Desta forma, foi criado o Comitê Gestor de Segurança da Informação, de natureza deliberativa, composto pelos executivos, gerentes setoriais que tratam os principais dados sensíveis da organização, gerência de TI e o DPO, que através de reuniões periódicas, cuidava das decisões relacionadas à Segurança da Informação.

4.4 Criação e Divulgação da Política de Segurança da Informação (PSI)

Uma das primeiras atividades realizada pelo DPO foi criação de uma Política de Segurança da Informação (PSI), que consiste em um documento que define os princípios e diretrizes visando à preservação da segurança da informação, sendo esta aprovada pelo Comitê Gestor de Segurança da Informação. A PSI tem como objetivo orientar o uso apropriado dos dados e dos recursos tecnológicos, sendo direcionada a todos os colaboradores inclusive terceirizados, visitantes e clientes, utilizando uma linguagem simples e de fácil entendimento (NAKAMURA; GEUS, 2007, p. 188).

A PSI visa promover um comportamento ético e profissional baseado nos pilares da segurança da informação: confidencialidade, integridade e disponibilidade. De forma resumida, a PSI elaborada continha disposições referentes aos seguintes assuntos: acessos físicos, lógicos e remotos que possam causar danos aos sistemas de informação; uso das estações de trabalho, recursos de rede e dos servidores; uso do e-mail corporativo; uso da internet; políticas de senha; uso e licenciamento de softwares; acesso a rede local e sem fio; uso dos recursos de impressão; trabalho e acesso remoto; gestão de incidentes de segurança e estabelecimento de punições, entre outros.

Após sua aprovação pelo Comitê Gestor de Segurança da Informação, a PSI foi divulgada aos colaboradores da empresa, visando conscientizar as pessoas sobre a importância da adequação à LGPD como um dos bens mais preciosos da organização. Foram definidos multiplicadores internos, que foram apoio em todo o processo de disseminação da PSI. A equipe de Marketing da empresa também participou do processo, através da divulgação de e-mails informativos e confecção de vídeos, mostrando a importância das boas práticas de segurança da informação.

Treinamentos foram realizados com o apoio do RH, onde os colaboradores entenderam como funcionam as políticas internas sobre segurança da informação. Ao final do treinamento, o colaborador foi orientado a assinar o "Termo de Compromisso e Responsabilidade", que é um documento complementar a PSI, que resume que o colaborador tem ciência sobre o programa de segurança da informação da empresa, e consequentemente arquivada em sua pasta junto ao RH. Este documento inclusive referencia as penalidades para os colaboradores que violarem o conteúdo da PSI.

4.5 Revisão dos Contratos com os Fornecedores

O próximo passo do plano de ação macro foi à revisão dos contratos com os fornecedores, que é um documento onde estão previstas as entregas e os prazos entre duas empresas de acordo com os seus vínculos. É neste documento que ambas as partes terão seus direitos e deveres listados, o que evita possíveis danos ao negócio.

A responsabilidade principal desta atividade é do setor Jurídico da empresa com o apoio do DPO. É de suma importância que o setor Jurídico esteja alinhado com o projeto na íntegra, pois a LGPD torna necessário realizar aditivos em praticamente todos os contratos vigentes e aos novos contratos que forem chancelados, com adição de novas cláusulas que façam referências à LGPD.

Esta atividade não foi simples, sendo uma das atividades mais trabalhosas do projeto. Contratos em andamento tiveram aditivos e novos contratos passaram a ser firmados com cláusulas de proteção de dados, conforme exemplo a seguir:

> A CONTRATADA, por si e por seus colaboradores, obriga-se a atuar no presente Contrato em conformidade com a Legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial a Lei 13.709/2018, além das demais normas e políticas de proteção de dados de cada país onde houver qualquer tipo de tratamento dos dados dos clientes, o que inclui os dados dos clientes desta (LIMA, 2022).

4.6 Entrevista Técnica com Todos os Colaboradores da Empresa

O próximo passo do plano de ação macro foi realizado pelo DPO em todos os setores da empresa, com o apoio de gerentes setoriais, realizando entrevista técnica com todos os colaboradores de forma individualizada, a fim de identificar os processos e procedimentos que possam vir a gerar algum incidente de segurança da informação. Ao final, foi gerado um relatório individualizado por setor, sugerindo os pontos que necessitavam de atenção, classificando o nível de risco como baixa, média ou alta.

Buscou-se identificar e diminuir o fluxo de dados sensíveis que não eram utilizados de forma objetiva para o andamento do negócio. Foram implementadas diversas ações/políticas, tais como: evitar impressão de dados pessoais desnecessários, introdução da política de papel zero, criação de pastas compartilhadas na rede para armazenamento de arquivos, instalação de desfragmentadores de papel em setores chaves, incentivo ao uso de assinatura via certificado digital, entre outras.

4.7 Estruturação do Firewall da Empresa

No aspecto técnico/tecnológico do plano de ação macro, o próximo passo foi à estruturação do firewall de forma imediata. Esse é um importante equipamento na segurança de redes de computadores corporativas, pois atua como um filtro entre um conjunto de dispositivos e sua conexão com a internet ou com a rede externa, decidindo o tráfego de rede que poderá passar ou não de acordo com regras preestabelecidas ou aprendidas dinamicamente (NAKAMURA; GEUS, 2007, p. 221).

O firewall de borda que controlava a comunicação da rede da empresa para o mundo externo era antigo, e com o passar do tempo diversos problemas puderam ser observados: sua administração era trabalhosa e complexa, visto que toda configuração era realizada somente através de linha de comando; a quantidade de portas de comunicação era limitada, tornando difícil a administração vários links de internet em um mesmo equipamento; o equipamento não fazia controle de cache de pacotes, sendo necessário um servidor de proxy externo para complementá-lo, tornando o processo de administração mais difícil; a integração do firewall com sistema de autenticação Radius integrado ao Active Directory da Microsoft era complexa, o que na maioria das vezes tornava autenticação dos usuários inviável, entre outros.

Portanto, houve a necessidade de aquisição de um firewall de nova geração da linha Sophos Next-Gen da Série XG que possuía diversas características, tais como: maior simplicidade na criação de regras de firewall; integração nativa com o sistema de autenticação do Active Directory, permitindo usar a mesma autenticação dos usuários no sistema operacional para a navegação na internet; maior quantidade de portas de comunicação disponíveis, tornando possível balancear os links de internet corporativos; dashboard de monitoramento em tempo de execução, com relatórios centralizados; inspeção SSL em tempo real; sistema de prevenção de intrusão (IPS); VPN/IPSec ilimitado para acesso dos colaboradores; uso de machine learning integrados a sistemas de inteligência artificial na filtragem dos pacotes, entre outros.

4.8 Estruturação do Sistema de Backup da Empresa

O próximo passo do plano de ação macro foi a reestruturação do sistema de backup, que armazena cópias de segurança de todos os dados da empresa com o objetivo de preservá-lo e garantir sua recuperação em caso de incidentes/desastres (TANENBAUM; BOS, 2016, p. 211).

O antigo sistema de backup da empresa era composto por robôs usando fitas LTO de geração passada, com pouca capacidade de armazenamento e baixa velocidade de leitura e gravação, onde o backup/restauração de um grande volume de dados demorava dias/semanas. Outro problema era a quantidade de fitas geradas para cada volume de backup, fazendo com que o processo envolvesse dezenas de fitas, sem contar o alto custo destas fitas.

Como volume total de dados na empresa era grande e partindo do pressuposto que no decorrer dos anos a tendência era que a massa de dados aumentasse devido a novos sistemas, serviços e clientes, administrar todo este volume de dados ficou complexo. Com ataques de ransomwares cada vez mais frequentes, a decisão a ser tomada foi buscar um sistema de backup robusto, que possuísse integração com novas estruturas de armazenamento e compatibilidade com a nova geração de storages.

As principais características de um sistema moderno de backup que foram levadas em consideração neste projeto foram: integração com os melhores storages de mercado; existência de interfaces de rede do tipo fibre channel, necessárias para que a comunicação dos servidores com o storage seja realizada em alta velocidade; existência de tecnologia de snapshot nativa no nível de hardware; alto poder de processamento e grande quantidade de memória RAM; compatibilidade com o sistema de armazenamento em fitas LTO existente atualmente na empresa, pois ele continuaria em funcionamento junto com o novo sistema de backup; interface simples e unificada de administração na criação dos planos de backup/restauração de dados; entre outros.

Após análise de diversas soluções, a empresa adquiriu o sistema de backup Arcserve UDP. O antigo sistema usando fitas LTO continua em operação para o armazenamento do backup mensal, sendo realizado ao final do mês.

4.9 Estruturação da Segurança das Estações de Trabalho

O próximo passo do plano de ação macro foi melhorar a segurança das estações de trabalho, composta por computadores e notebooks. Esta foi uma etapa onde a gerência de TI foi bem atuante junto governança, pois nas etapas anteriores houve um investimento considerável na estruturação de firewall e backup, e agora seria necessário mais investimento, o que não foi fácil devido aos gastos no combate à pandemia.

De forma sucinta, a implementação da segurança dos computadores e notebooks da empresa passou pelos seguintes passos: realizar a atualização do parque de hardware, se necessário; manter o Sistema Operacional e os aplicativos atualizados; instalar apenas aplicações homologadas e devidamente licenciadas pela empresa; utilizar um sistema de antivírus confiável; utilizar um sistema de Endpoint Detection and Response (EDR) confiável.

Inicialmente, foi elaborado o inventário de hardware e software das estações de trabalho, com o objetivo de traçar todo o perfil de hardware e software que precisavam ser substituídos no parque. A equipe de TI se esforçou em organizar todo o portfólio neste momento, mantendo apenas aplicações homologadas e devidamente licenciadas, removendo softwares indevidos e não licenciados, além de substituir, quando possível, algumas aplicações por softwares livres equivalentes. Cabe ressaltar aqui os altos valores das multas referentes ao uso indevido de software, além do fato de que softwares piratas podem conter vírus e outros malwares, comprometendo a segurança.

Com o inventário em mãos, o próximo passo foi realizar a substituição dos equipamentos obsoletos do parque. Foram identificadas centenas de micros com mais de 15 anos de utilização contendo sistemas operacionais obsoletos. Foi priorizada a aquisição de micros ao estilo mini, com baixo consumo de energia, alto poder de processamento e com tecnologia SSD nativa. A atualização do hardware de estações de trabalho permitiu o uso de versões mais novas do sistema operacional Microsoft Windows, tornando possível a ativação das atualizações automáticas de segurança em todas as estações de trabalho.

Os hardwares obsoletos foram reaproveitados em setores que exigem menos processamento, como o setor de serviços gerais, que utilizava uma aplicação única, de simples implementação. Nesses computadores foram instaladas versões recentes do sistema operacional Linux, que é gratuito e requer pouco poder de processamento.

O próximo passo foi a reestruturação do sistema de antivírus, que é um software que detecta, impede e atua na proteção contra os softwares maliciosos (TANENBAUM;

BOS, 2016, p. 475). Na empresa em questão, o sistema de antivírus vigente era antigo, complexo, ineficiente, com poucos recursos para ambientes corporativos, baixas taxas de ameaças detectadas e sem bloqueio nativo de dispositivos removíveis.

A empresa buscou por soluções de antivírus que não possuíam os problemas supracitados, que fosse moderno, leve, possuísse instalação simplificada, se possível realizada através da rede em modo silencioso, com alto nível de proteção atestado por instituições como a Gartner. Após análises de diversos fornecedores, neste projeto foi aplicado o sistema de antivírus da Sophos, que inclusive funciona integrado ao Firewall.

O próximo passo do plano de ação macro foi a aquisição de um Endpoint Detection and Response (EDR), visando complementar a proteção das estações de trabalho. EDR consiste em um sistema muito poderoso de prevenção e proteção ao tráfego de rede, trabalhando de forma complementar ao firewall, monitorando todas as estações de trabalho do ecossistema, antecipando e neutralizando os principais tipos de ataques (MONTENEGRO, 2018).

O EDR trabalha em nível de deep learning, emitindo alertas, gerando um monitoramento eficiente e informativo das principais ações suspeitas em seu ecossistema de forma centralizada, com geração de notificação instantânea para os graus de severidade e grupos receptores desta informação, possibilitando uma visão macro dos principais acontecimentos e identificando o grau de risco de cada incidente (MONTENEGRO, 2018). Após análises de diversos fornecedores, a ferramenta de EDR adquirida pela empresa foi a Sophos Intercept X.

4.10 Estruturação da Segurança da Rede Local de Computadores

O próximo passo do plano de ação macro foi a estruturação da segurança na rede de computadores da empresa. Neste projeto foi necessário mapear de forma detalhada todos os equipamentos fora do padrão de conectividade, identificando todas as vulnerabilidades existentes.

Diante das vulnerabilidades encontradas, as seguintes ações foram realizadas: identificação e organização de todos os equipamentos de rede, tais como switches e roteadores, além da atribuição de IP para todos esses equipamentos; identificação das VLANs existentes e criação de VLANs rígidas para equipamentos hospitalares de alto custo, como tomógrafos e equipamentos de ressonância, isolando-os da rede de computadores convencional e desativado o acesso à internet desses equipamentos; ativação do protocolo de acesso remoto SSH em todos os equipamentos de rede, sem

permitir acesso através de logins genéricos; compra de switches camada 3 para um melhor gerenciamento da rede; atualização dos firmwares de todos os equipamentos de rede; eliminação de qualquer equipamento desnecessário da rede.

O próximo passo foi a aplicação de regras de seguranças rígidas nos pontos de rede, pois de acordo com Grustniy (2019), intrusos podem penetrar em sua rede local por meio de pontos de rede existentes em áreas comuns. Na empresa existem aproximadamente 800 estações de trabalho e cerca de 1300 pontos de rede.

Foi aplicado um plano piloto de controle de segurança nas portas, recurso conhecido como Port Security, nos switches existentes em um prédio que possuía aproximadamente 100 estações de trabalho. Foi limitado a quantidade de um endereço MAC por porta do switch, com violação habilitado para “shutdown”, ou seja, caso um usuário comum desconecte o cabo de rede de qualquer estação de trabalho e coloque em outro equipamento sem informar a TI, a porta é desativada automaticamente.

4.11 Estruturação da Segurança da Rede sem Fio

O próximo passo foi organizar a rede sem fio da empresa, pois este tipo de rede mal projetada pode ser uma porta de entrada de invasão para a rede corporativa, podendo significar simples fatos desagradáveis, como o uso não autorizado da internet, até perdas de recursos financeiros significativos, como invasão a sistemas e roubo de dados (NAKAMURA; GEUS, 2007, p. 139).

Em um local com volume expressivo de clientes, fornecedores e colaboradores, é importante usar um sistema profissional de rede sem fio. Esta estruturação foi muito trabalhosa, pois a rede sem fio da empresa estava desorganizada antes da LGPD.

Inicialmente, os profissionais de TI atuaram detectando e removendo qualquer Access Point sem gerenciamento da equipe de TI. O próximo passo foi desenhar a topologia da rede de forma que a rede sem fio opere de forma separada da rede cabeada da empresa, além de buscar fornecedores de equipamentos sem fio para uso em ambientes corporativos.

Neste projeto foi realizada parceria com a empresa Wifire, especialista em projetos profissionais de Wi-Fi corporativo. Toda a rede sem fio foi configurada com SSID único, e os Access Points foram distribuídos de forma que não ocorresse perda de conexão quando o usuário transitasse pelas dependências da empresa. Os Access Points possuíam a tecnologia Power over Ethernet (PoE), nos quais a alimentação elétrica era fornecida diretamente pelo switch através do cabo de rede.

O mais interessante deste projeto foi a possibilidade de fornecer acesso à internet aos pacientes. Eles usavam o seu número de cliente, presente em sua carteirinha, para autenticação através de uma API, que consultava a base de dados da empresa, ou seja, o acesso à internet era liberado somente para clientes autenticados que aceitasse os termos e condições de uso da internet. Desta forma, era garantida a autenticidade do usuário, um dos pilares da segurança da informação (NAKAMURA; GEUS, 2007, p. 363).

4.12 Estruturação da Segurança do Active Directory

O Active Directory (AD) é uma estrutura hierárquica presente no sistema operacional Microsoft Windows Server, que armazena informações sobre os objetos na rede por meio da autenticação de logon e do controle de acesso a objetos nos diretórios. É onde se concentra toda a estrutura de autenticação dos usuários da rede, grupos e políticas de grupo, que consegue integrar toda uma estrutura de autenticação e de direito de acessos de uma forma simples e poderosa (DESMOND et al., 2013).

Nakamura e Geus (2007, p. 363) destacam que autenticação dos usuários tem um papel fundamental para a segurança de um ambiente cooperativo, pois além da identificação dos usuários, o sistema pode controlar de forma individualizada o acesso aos recursos da rede corporativa. Em ambientes que usam o sistema operacional Microsoft Windows, o Active Directory é a principal ferramenta para possibilitar a autenticação dos usuários e autorização no acesso aos recursos.

Desta forma, o próximo passo do plano de ação macro foi organizar a estrutura do Active Directory com as seguintes ações voltadas a segurança: remoção dos usuários genéricos; atribuições de acesso à internet baseado em grupos; aplicação da política de complexidade das senhas e de expiração de senhas a cada 60 dias; bloqueio de usuários inativos; definição de horário de logon.

Esta foi uma das atividades mais complexas do projeto, pois levou alguns meses para ser completada e gerou grande insatisfação dos usuários com a equipe de TI. Infelizmente uma prática comum na empresa era a utilização de logins genéricos para autenticação nas estações de trabalho, tais como “recepcao”, “enfermagem”, “uti”, entre outros. O uso de logins genéricos vai contra o princípio de não repúdio em segurança da informação, pois torna difícil identificar o causador de um incidente de segurança.

Iniciou-se então pela equipe de TI um movimento remoção dos usuários genéricos existentes, e após a estruturação do Active Directory, todos os funcionários tinham suas

próprias contas de usuário e passaram a usá-la para efetuar login nos computadores e demais sistemas.

Com um logon de rede individualizado para cada funcionário, os administradores de rede podem gerenciar permissões de acesso a arquivos e recursos em toda a rede, e os usuários autorizados podem acessar esses recursos a partir de qualquer estação de trabalho da empresa. As contas de usuários foram organizadas em grupos de usuários de acordo com a estrutura organizacional, por exemplo, contas de usuário dos funcionários da contabilidade foram inseridas no grupo de "Contabilidade", herdando as permissões atribuídas a esse grupo.

Por fim, aplicou-se à política de acesso à internet através da integração com o novo firewall, no qual os gerentes setoriais passaram a ser responsáveis por definir e monitorar através de relatórios o acesso à internet de suas equipes, tendo como ponto de atenção a privacidade do usuário.

4.13 Estruturação da Segurança do Home Office da Empresa

O próximo passo do projeto foi organizar o home office, no qual funcionários atuam a distância utilizando-se de meios computacionais como se estivesse fisicamente na empresa. Esta etapa foi coordenada pelo setor de Recursos Humanos, ficando a cargo da equipe de TI somente o apoio tecnológico. Em paralelo a esse processo, também foi organizado o acesso remoto dos fornecedores aos sistemas da empresa.

A aquisição do novo firewall facilitou a organização tecnológica do trabalho de home office, pois o firewall possuía recurso nativo de VPN/IPSec integrado aos grupos do Active Directory, o que tornou o processo extremamente simples, aproveitando as contas de usuários e grupos organizados anteriormente na estruturação do Active Directory. Desta forma, cada colaborador utilizava para acesso remoto via VPN/IPSec o mesmo login/senha usado dentro da empresa para autenticação nas estações de trabalho.

Outro processo que precisou ser colocado em ordem nesta etapa foi o acesso remoto dos fornecedores, pois anteriormente alguns fornecedores conectavam diretamente nos bancos de dados Oracle através de NAT direto, sendo que estes acessos ficavam invisíveis na rede. Desta forma, o próximo passo foi identificar esses acessos ocultos na rede e eliminá-los imediatamente.

Foi criada uma política rígida de cadastramento de acesso dos fornecedores, com regras de horários de conexão somente para o servidor que o fornecedor precisava de

acesso para realizar a manutenção do serviço. Com a adequação dos acessos remotos dos fornecedores, houve uma maior transparência e controle das informações acessadas.

4.14 Estruturação da Criptografia de Sistemas

Nakamura e Geus (2007, p. 301) destacam que o uso da criptografia nas organizações tem função e importância cada vez maior para a segurança dos dados, pois ela permite sigilo, integridade, autenticidade e não repúdio dos dados armazenados em discos e trafegados pela rede de computadores. Desta forma, o próximo passo do plano de ação macro foi criptografar tudo que fosse possível.

Foi necessário adquirir um certificado wildcard, que apesar de ser mais caro, é o mais completo e possibilita a criação de vários subdomínios abaixo do seu domínio principal (*.empresa.com.br) com certificação SSL/TLS em apenas um único certificado, sendo o mais indicado para organizações que possuem muitos sistemas dentro de um domínio principal.

Foi possível aplicar certificação SSL/TLS em praticamente todos os sistemas WEB internos e externos, com a utilização do modelo de certificado SSL wildcard, que controlou todo o domínio da empresa e facilitou a criação de diversos subdomínios no servidor de DNS. Também foi aplicado criptografia no servidor de e-mail, principalmente nos portais de webmail acessíveis pela internet.

4.15 Estruturação do Processo de Atualização e Correção das Vulnerabilidades em Servidores e Equipamentos de Rede

O próximo passo do projeto foi aplicar atualizações de segurança nos servidores e equipamentos de rede e criar um processo rígido de aplicação dessas correções. Mohurle e Patil (2017) destacam que manter sistemas atualizados ajuda a evitar a exploração de vulnerabilidades conhecidas, sendo uma das principais ações de defesa contra diversos tipos de ataques. Como este trabalho é contínuo, pois constantemente surgem novas atualizações/patches/firmwares para os servidores e equipamentos de rede, foi definido um analista para ser o responsável por este processo.

O ponto de destaque deste trabalho inclui manter os firmwares atualizados dos servidores e equipamentos de rede de acordo com a disponibilização do fabricante, além de manter os drivers atualizados. Especificamente nos servidores com Windows Server, foi ativado a atualização automática presente no próprio sistema operacional. Os

hypervisors também precisavam estar com suas vulnerabilidades corrigidas em tempo real, para que estes não se tornassem alvos de ataque às máquinas virtuais.

Outro importante trabalho realizado foi isolar os servidores do acesso à internet, através da criação de regras específicas no firewall para servidores que não necessitavam de acesso à internet, liberando somente para os sistemas de atualizações do próprio sistema operacional, bloqueando o restante.

5. RESULTADOS E DISCUSSÕES

Diversas ações foram realizadas visando adequação à LGPD. No aspecto organizacional, a criação do setor de Segurança de Informação na empresa foi o passo inicial de todo o processo. A transferência de um profissional que já pertencia à equipe de infraestrutura de TI para este setor foi uma excelente decisão, pois ele já conhecia o portfólio de serviços da empresa e já estava familiarizado com os processos internos.

Esse profissional também acumulou a função de DPO da empresa. O trabalho de mapeamento interno dos dados sensíveis realizada pelo DPO através de entrevistas aos colaboradores da empresa foi importante, pois foi possível identificar os setores mais vulneráveis e criar planos de ações simples que diminuíram o risco de exposição de dados. Foi sua responsabilidade também conduzir as reuniões do Comitê Gestor de Segurança da Informação, elaborar a PSI, propor e conduzir as mudanças necessárias, entre outras atribuições.

O destaque deste projeto foi o envolvimento através do Comitê Gestor de Segurança da Informação das principais gerências da empresa, que entenderam a importância do processo de adequação para a continuidade do negócio. Este comitê foi responsável por aprovações, revisões, planejamento de aquisições e investimentos no que faz referência a Segurança da Informação. Foi responsável também pela aprovação da PSI, sobre o processo de segurança da informação e gerenciamento dos incidentes.

Através do comitê foi possível estabelecer uma cultura das melhores práticas de segurança da informação perante seus colaboradores com o envolvimento de todos os setores. Com a aprovação do comitê, ocorreram treinamentos e campanhas de envolvimento massivas direcionadas as gerências e seus colaboradores, principalmente nos setores que manipulam dados sensíveis.

O comitê também mediava conflitos, principalmente entre os setores de Segurança da Informação e de Infraestrutura de TI, principalmente quanto aos prazos definidos para

a resolução dos problemas de segurança identificados, pois era um período conturbado e de sobrecarga da equipe de TI, devido aos trabalhos direcionados ao combate à pandemia.

O envolvimento do setor Jurídico junto ao DPO na revisão dos contratos com os fornecedores não ocorreu da forma esperada no início do projeto. Não ocorreu por parte da empresa capacitação do setor jurídico para se adaptar as novas legislações, o que gerou sobrecarga nas equipes de Segurança da Informação e de TI. Por fim, no decorrer do projeto, houve mudanças de postura com relação à LGPD e o envolvimento do setor Jurídico da empresa melhorou, tendo um bom alinhamento para avanço do projeto.

Com a revisão dos contratos dos fornecedores e aplicação de cláusulas referentes à LGPD, houve um movimento involuntário de transparência e percepção por parte do fornecedor da seriedade que a empresa dava a segurança dos dados.

No aspecto técnico/tecnológico da infraestrutura de TI da empresa, a aquisição de um firewall de alto nível aumentou a segurança da rede de computadores e a produtividade dos administradores de rede, pois o que antes era um processo amarrado, engessado e dificultoso, a partir deste momento passa a ser simples, seguro, eficiente, documentado, auditável e escalável.

Com a atualização do sistema de backup, houve uma evolução significativa nos backups/restore, principalmente no tempo necessário para a realização destes. O sistema antigo de backup usando fitas LTO foi reaproveitado, sendo este responsável pelo o armazenamento do backup mensal da empresa.

Novas estações de trabalho foram adquiridas, permitindo o uso das versões mais recentes do sistema operacional Microsoft Windows, que periodicamente recebe atualizações de segurança de forma automática. O antigo sistema de antivírus foi substituído por um novo, mais moderno e integrado ao firewall da empresa, além da introdução de um sistema de EDR nas estações de trabalho, aumentando a segurança destas e de toda a rede de computadores. Por serem do mesmo fabricante, foi possível integrar o firewall, antivírus e EDR, possibilitando assim identificar várias intercorrências de segurança que antes ficavam praticamente invisíveis aos administradores de redes, e que passou a ser alarmada de forma eficiente.

Com a organização do Active Directory, usuários genéricos foram desativados, e todos os funcionários passaram a ter suas contas de usuário individualizadas, com complexidade de senha, horário de logon, políticas de acesso a internet, entre outros. Essa organização tornou as autenticações mais seguras e facilitou também a aplicação do

acesso externo remoto via VPN de forma segura e controlada através do novo firewall integrado com o Active Directory.

Mudanças na arquitetura da rede de computadores foram realizadas visando garantir isolamento de redes dentro da organização. Com a ativação de recursos de segurança em switches, como o Port Security, diminuíram-se os perigos de uso indevido dos pontos de rede existentes nos prédios, principalmente nas recepções dos escritórios.

Após a aplicação do Port Security na rede de computadores de um dos prédios, chamou atenção da equipe de TI a quantidade de chamados que chegava com referência a pontos de rede violados, ou seja, desativados automaticamente pelo recurso de Port Security, pois o sistema controlava o acesso indevido, principalmente para os desavisados que conectavam notebook em pontos de rede estratégicos. Após o sucesso deste plano piloto, iniciou-se um projeto para no futuro implantar este recurso de segurança em todos os pontos de rede da empresa.

A reestruturação da rede sem fio foi realizada em seis prédios da empresa. Os pacientes, que antigamente não acessavam a rede da empresa, passaram a ter acesso à rede sem fio para uso da internet, utilizando o número da sua carteirinha como identificação, proporcionando assim autenticação dos usuários. Na matriz houve pico de acesso à internet de 800 conexões diárias intercaladas e 503 conexões simultâneas, sendo que em aproximadamente dois anos de projeto, foram realizadas 51 mil conexões de pessoas diferentes, cerca de 10% da população da cidade onde a empresa se encontra.

Criptografia SSL/TLS foi aplicada a sistemas e websites, garantindo assim confidencialidade, um dos pilares da segurança da informação. Foi criado um processo contínuo de atualização de sistemas, firmwares e aplicação de patches de segurança em servidores e equipamentos de rede, a ser realizada pela equipe de TI. Buscou-se, desta forma, garantir que equipamentos de rede, servidores e estações de trabalho estejam sempre com seus softwares atualizados, minimizando desta forma brechas de segurança que possam vir a ser exploradas por hackers ou softwares maliciosos.

6. CONSIDERAÇÕES FINAIS

Foram anos de trabalho árduo aplicado neste projeto visando aumentar a segurança dos dados corporativos e alcançar o mínimo de adequação às boas práticas de segurança. Conforme os processos vão tomando forma e os resultados vão sendo atingidos, compreende-se que a LGPD é bem mais ampla do que se imagina.

Nesse novo cenário, este artigo busca contribuir na seguinte questão de pesquisa: Quais ações/mudanças as organizações devem realizar visando adequação à LGPD? Na empresa do estudo de caso, diversas ações foram realizadas. No aspecto organizacional, os pontos de destaque foram: a criação o setor de Segurança da Informação, a definição o DPO, a criação do Comitê Gestor de Segurança da Informação envolvendo as principais gerências da empresa, a criação da PSI e a sua disseminação através de treinamentos, além da atualização dos contratos existentes com fornecedores através da adição de cláusulas sobre a LGPD, tornando-se padrão também para novos contratos.

No aspecto técnico/tecnológico, muito investimento foi feito. Equipamentos físicos como firewall, sistema de backup, equipamentos de rede e novas estações de trabalhos foram adquiridos. Softwares específicos de segurança, como antivírus e EDR foram comprados e instalados nas estações de trabalho, proporcionando proteção contra ameaças virtuais, como vírus e outros malwares. Criptografia foi habilitada em diversos serviços, possibilitando segurança dos dados enquanto eles trafegam pela rede de computadores. A rede de computadores e a rede sem fio foram reestruturadas, habilitando funcionalidades de segurança de redes. O acesso aos computadores e o acesso externo via VPN ocorre de forma mais segura e auditável, através de um sistema de autenticação dos funcionários centralizado no Active Directory.

Considerando que empresas de grande porte frequentemente compartilham semelhanças em suas infraestruturas de TI, este estudo desempenha um papel relevante para a sociedade, pois apresenta ações que foram executadas no âmbito da empresa em questão e que possivelmente serão adotadas por outras organizações que buscam ajustar suas operações conforme as diretrizes da LGPD. Este trabalho oferece, portanto, insights valiosos para outras organizações que buscam realizar ajustes similares nesse novo contexto regulatório de segurança da informação.

Certas limitações devem ser consideradas ao interpretar os resultados deste trabalho. Em primeiro lugar, devido ao estudo ser baseado em uma única empresa, o resultado pode não ser generalizável para outras organizações. Desta forma, recomenda-se que pesquisas futuras explorem múltiplas empresas a fim de avaliar a aplicabilidade das ações realizadas, possibilitando compreensão mais abrangente das melhores práticas no processo de adequação à LGPD.

Além disso, a pesquisa se concentrou em aspectos internos da empresa. Desta forma, recomenda-se que investigações futuras busquem fontes adicionais de

informações, tais como indicadores setoriais e econômicos, a fim de contextualizar de forma mais completa os resultados obtidos.

Felizmente a partir do trabalho realizado, não foi identificado nenhum incidente grave relacionado à segurança da informação. E a continuidade do ciclo perdura, pois o processo da LGPD é vivo, não existe a assinatura do termo de encerramento do projeto, e a tendência é que se vislumbre novos objetivos para os próximos anos, a fim de melhorar a proteção dos dados empresariais e garantir a continuidade do negócio.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 2018.

CARVALHO, L. et al. **Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais.** In: Anais do VII Workshop de Transparência em Sistemas. SBC, 2019. p. 21-30.

DESMOND, B. et al. **Active Directory: Designing, Deploying, and Running Active Directory.** 5. ed., O'Reilly Media, 2013.

GRUSTNIY, L. **Os perigos dos pontos de LAN nas recepções dos escritórios.** 12 dez 2019. Disponível em: https://www.kaspersky.com.br/blog/dangerous-ethernet-ports/13800/. Acesso em: 15 set. 2022.

ISO/IEC TR 13335-2. **Information Technology - Guidelines for the Management of Information Technology Security - Part 2: Managing and Planning IT Security**, 1st ed., Switzerland, 1997.

LIMA, J. E. M. R. **Modelo de cláusula de proteção de dados - Contratante de serviços – LGPD.** Disponível em: https://www.mercadoadvocacia.com.br/advogado-lojas-virtuais-online/modelo-de-cláusula-de-proteção-de-dados-contratante-de-serviços-lgpd. Acesso em: 15 set. 2022.

MOHURLE, S.; PATIL, M. **A brief study of wannacry threat: Ransomware attack 2017.** International journal of advanced research in computer science, v. 8, n. 5, p. 1938-1940, 2017.

MONTENEGRO, F. **Expanding Machine Learning Applications on the Endpoint.** 451 Research, 2018. Disponível em: https://www.blackberry.com/content/dam/cylance/documents/pdf/451ResearchExpandingMLApplicationsontheEPReport.pdf. Acesso em: 15 set. 2022.

NAKAMURA, E.; GEUS, P. L. **Segurança de Redes em ambientes cooperativos.** 1. ed. São Paulo: Novatec Editora, 2007.

NETO, N. N. et al. **Developing a Global Data Breach Database and the Challenges Encountered.** ACM Journal of Data and Information Quality, vol. 13, n. 1, 2021.

PEREIRA, V. P. R. G. **O processo de adequação da Universidade Federal de Santa Catarina à Lei Geral de Proteção de Dados Pessoais.** Monografia, Departamento de Administração, Universidade Federal de Santa Catarina, Florianópolis, SC, 2023.

ROJAS, M. A. T. **Avaliação e adequação do Instituto Federal de Santa Catarina à Lei Geral de Proteção de Dados Pessoais.** Monografia, Pós Graduação em Gestão Pública na Educação Profissional e Tecnológica, Instituto Federal de Santa Catarina, Florianópolis, SC, 2020.

SILVA, M. **Lei Geral de Proteção de Dados.** 7 jul. 2020. Disponível em: https://criainovacao.com.br/lei-geral-de-protecao-de-dados/. Acesso em: 15 set 2022.

SOARES, R. D. F. **Adequação à lei geral de proteção de dados pessoais: um estudo de caso em uma empresa de tecnologia em Aracaju/SE.** Monografia, Departamento de Administração do Centro de Ciências Sociais Aplicadas, Universidade Federal de Sergipe, São Cristóvão, SE, 2023.

TANENBAUM, A. S.; BOS, H. **Sistemas Operacionais Modernos.** 4. ed., São Paulo: Pearson Education do Brasil, 2016.

WINKERT,A. et al. **Custos hospitalares na pandemia Sars-Cov-2: um estudo sobre equipamentos de proteção individual (EPI's) em duas unidades hospitalares no oeste do Paraná.** Revista de Ciências Empresariais da UNIPAR. Umuarama. v. 23, n. 2, p. 1024-1044, 2022.