PROPOSTA DE UM PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO PARA UMA EMPRESA DO SETOR DE IMPLEMENTOS RODOVIÁRIOS

Felipe Ronchi Paes[1]

Felipe Gulert Rodrigues[2]

Resumo: As informações e os dados pessoais disponíveis em organizações representam um ativo extremamente importante para o ambiente de negócios. A criação de estratégias e planos para controle de danos é fundamental para a continuidade do negócio, sendo o plano de resposta a incidentes de segurança um dos principais recursos estratégicos para garantir a segurança da empresa. Levando-se em consideração o fato de que o plano de resposta a incidentes de segurança é essencialmente um processo, a questão da pesquisa é: quais são as ações necessárias para um plano de resposta a incidentes de segurança da informação em uma empresa do setor de fabricação de implementos rodoviários? O objetivo desse artigo é apresentar uma proposta de plano de resposta a incidentes de segurança da informação em uma empresa do ramo de fabricação de implementos rodoviários. Verificou-se que ainda não foi desenvolvido um plano de resposta na empresa objeto dessa pesquisa devido ao fato de o departamento de tecnologia da informação ter sido alçado ao patamar de setor estratégico há apenas 2 anos. Por se tratar de uma empresa familiar que está há muitos anos no mercado, o objetivo era fazer o negócio funcionar, nem sempre se atendo a aplicação de boas práticas em segurança da informação. Essas implementações passaram a ter relevância nos processos a partir da contratação de mais profissionais, para a equipe, com foco no tema e apoio da alta gestão. Conclui-se que o plano resposta deve sempre se ater ao porte da organização, bem como suprir as exigências normativas em relação à política de segurança da informação e a legislação brasileira.

Palavras-Chave: LGPD, Segurança da Informação, Incidentes Cibernéticos, Plano de Resposta, Proteção de Dados.

1 INTRODUÇÃO

As informações e os dados pessoais disponíveis em organizações representam um ativo extremamente importante para o ambiente de negócios. Atualmente, há uma grande atenção envolvendo os cidadãos, as empresas e governo

[1] Graduando em Engenharia de Computação. Ano 2023-1. E-mail: ronchipaes@yahoo.com.br
[2] Professor do Cento Universitário UniSATC. E-mail: felipe.rodrigues@satc.edu.br

com os cuidados relacionados à privacidade e proteção dos dados pessoais presentes em bancos de dados, arquivos e contas em redes, e demais meios físicos e digitais.

Diante deste cenário, como descrevem Doles e Cárnio (2020) a partir da mobilização a nível internacional visando à proteção de dados pessoais iniciado pela União Europeia, por meio da edição e implementação do Regulamento Geral de Proteção de Dados da União Europeia (RGPD), é visível que os países estão se organizando internacionalmente para regulamentar a proteção de dados pessoais de seus cidadãos.

No Brasil a Lei Geral de Proteção de Dados (LGPD) nº 13.709/2018 expôs normas específicas referentes à proteção de dados, além de uma penalização em caso de vazamento de dados (DOLES; CÁRNIO, 2020). A adequação a essa Lei não diz respeito unicamente à inserção de medidas tecnológicas que consigam assegurar maior segurança das informações, mas também a necessidade de elaborar e revisar de maneira contínua os documentos que garantem a já mencionada segurança dos dados. Sendo assim, a criação de estratégias e planos para controle de danos é essencial, e é aí que entram os planos de respostas a incidentes de segurança.

Levando-se em consideração o fato de que o plano de resposta a incidentes de segurança é essencialmente um processo, a questão da pesquisa é: quais são as ações necessárias para um plano de resposta a incidentes de segurança da informação, em uma empresa do setor de fabricação de implementos rodoviários?

A pesquisa tem sua relevância e importância, uma vez que, apresenta dados coletados que demonstram a necessidade da adoção de uma política de segurança de dados para conformidade com as diretrizes da Lei Geral de Proteção de Dados Pessoais (LPGD), para um eficaz tratamento e proteção de dados pessoais, assim como para garantir que a empresa esteja alinhada com as melhores práticas de segurança da informação, promovendo um ambiente de trabalho seguro e preparando os profissionais para estarem aptos a realizarem a gestão dos incidentes de segurança, tornando o departamento de tecnologia em uma área cada vez mais estratégica para o negócio.

O objetivo desse artigo é apresentar uma proposta de um plano de resposta a incidentes de segurança da informação em uma empresa do setor de fabricação de implementos rodoviários.

2 SEGURANÇA DA INFORMAÇÃO

A informação é um bem de extrema importância, especialmente, em ambientes de negócios e representam um ativo imensamente relevante e valioso para as empresas, pois são essenciais em diversas fases e transações, e em alguns casos são alvos de ameaças que podem gerar instabilidade e prejuízos expressivos. Sendo assim, é necessário a implementação de políticas de segurança da informação para atenuar as chances de adulteração ou perda de informações das empresas (ROCHA *et al.,* 2019).

Ainda, de acordo com Rocha et al. (2019), a Política de Segurança de Informação (PSI) consiste em um documento que deve compreender um agrupamento de regras, técnicas e mecanismos, que devem ser repassados a todos os colaboradores, para análise, verificação e revisão criteriosa em períodos constantes ou caso haja necessidade de alterações vigentes.

Ao passo que, conceitua Segurança da Informação (SI) como sendo a proteção concedida para um sistema de informação autorizado com a finalidade de atingir os objetivos de manter a integridade, a disponibilidade, a confidencialidade dos recursos do sistema de informação compreendendo o hardware, o software, o firmware, as informações, os dados e telecomunicações (STALLINGS, 2015).

Como argumenta Campos (2007, p.17), “a segurança da informação apoia-se em três princípios: confidencialidade, integridade e disponibilidade”. Quanto a confidencialidade, representa a preservação de que a informação está disponível somente para pessoal autorizado a disporem permissão (CAMPOS, 2017).

Conforme Brasil (2018), caso seja acessada por individuo sem autorização, intencionalmente ou não, ocorre a ruptura de confidencialidade, resultando em falhas sem dimensão para empresas ou pessoas físicas. Já a integridade consiste na preservação da certeza e absoluto da informação e da metodologia de seguimento. Quando a informação é adulterada, fraudulenta ou furtada, a integridade é interrompida. A integridade garante que a informação seja preservada com suas características originais. Por fim, a disponibilidade consiste na certeza de que os colaboradores habilitados têm acesso à informação e aos ativos correlatos sempre que necessários. Quando não existe acesso à informação, seja porque os

colaboradores estão fora de funcionamento por ataques ou violações ou por paradas instintivas do sistema, acontece a ruptura da disponibilidade.

Adicionalmente, como destacado por Lyra (2008, p.4), há outros aspectos suplementares essenciais para assegurar a segurança da informação. A autenticação se refere à garantia de que um usuário é realmente quem alega ser. O não repúdio se trata da habilidade do sistema em confirmar que uma ação específica foi executada por um usuário determinado. A legalidade, por sua vez, assegura que o sistema esteja em conformidade com as leis e regulamentos aplicáveis. A privacidade diz respeito à capacidade de um sistema manter um usuário anônimo, impossibilitando a associação entre o usuário e suas ações. Por fim, a auditoria envolve a habilidade do sistema em registrar todas as atividades realizadas pelos usuários, permitindo a detecção de fraudes ou tentativas de ataque.

Enquanto, a segurança de dados trata de uma técnica de proteção de arquivos, banco de dados, contas em uma rede, entre outros. Sendo assim, a adoção de um conjunto de regras, controles e métodos é fundamental para detectar a importância de diversos conjuntos de dados, seu grau de sensibilidade e requisitos de conformidade com normas com a finalidade de empregar proteções de modo efetivo para proteger os dados. A segurança dos dados é um procedimento que objetiva a análise e redução de riscos para o armazenamento de todos os tipos de dados (ROCHA et al., 2019).

2.1 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

No entanto, para assegurar a privacidade e a segurança dos dados pessoais, a legislação, a princípio a nível mundial, e na sequência, a nível nacional foi alterada. Inicialmente, como relatam Ribas e Guerra (2020), o Regulamento Geral de Proteção de Dados da União Europeia (RGPD), desde sua criação em 2016, vem se destacando por sua abrangência expandindo-se para países além do continente europeu, coletando dados pessoais de cidadãos europeus para oferecer bens e serviços, assim como, demonstra maturidade conceitual levando em conta a privacidade como um valor a ser tratado e considerando vários princípios, como por exemplo, o do livre consentimento do usuário titular dos dados pessoais, o da boa-fé, o da finalidade e o da não discriminação, entre outros. Desta forma, o RGPD se tornou

a fonte de inspiração legislativa para demais países, entre estes o Brasil não tinha nenhuma legislação neste sentido e baseado no RGPD criou a Lei Geral de Proteção de Dados (LGPD).

Como enfatizam Doles e Cárnio (2020) a Lei Geral de Proteção de Dados, Lei nº 13.709/18, de 13 de agosto de 2018, entrou em vigor em agosto de 2020, tem por princípios proteger os direitos fundamentais de liberdade e de privacidade, bem como, possibilitar o livre desenvolvimento da personalidade da pessoa natural.

A LGPD concretiza um regulamento para uso, armazenamento e transferência de dados no Brasil, tanto para o setor privado, como para o setor público. Assim como, de modo transparente, expõe quais as instituições e pessoas implicadas e seus direitos, deveres e punições no âmbito civil, que pode chegar ao valor de 50 milhões de reais em multa por ocorrência, conforme art. 52 da Lei nº 13.709 de 14 de agosto de 2018 (BRASIL, 2018).

Anteriormente a LGPD, o Brasil aprovou a Lei nº 12.965 de 23 de abril de 2014, conhecida como Marco Civil da Internet, que garante aos usuários da internet o direito a informações transparentes relativas às fases de coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais (BOFF et al, 2018). A inclusão do termo privacidade em seu sistema legal, a LGPD modifica o Marco Civil da Internet no Brasil (SÁ et al, 2019).

O objetivo da LGPD é estabelecer princípios de confiabilidade e segurança para o processamento de dados, bem como, assegurar transparência e privacidade aos usuários (BOFF et al, 2018).

2.2 NORMAS E DIRETRIZES PARA POLÍTICAS DE SEGURANÇA

É importante adotar práticas de gestão e proteção de dados que garantam o cumprimento dos requisitos mínimos exigidos pela lei. Desta forma, a *International Organization for Standardization* ou Organização Internacional para Padronização, conhecida como ISO, tem por finalidade contribuir para que muitas empresas executem processos com a utilização de padrões e métricas, reconhecidas e validadas internacionalmente visando guiar a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), adaptáveis a variados tipos e tamanhos de empresas. Diante deste contexto, as normas da família ISO 27000, atualizadas de

acordo com as determinações do Regulamento Geral de Proteção de Dados da União Europeia (RGPD), representam orientações fundamentais com o propósito de melhorar a segurança e controle de riscos referentes à utilização de dados pessoais (BOFF et al, 2018).

De acordo com Doles e Cárnio (2020), em 2005, com o propósito de regulamentar conteúdo técnico relativo à proteção de dados pessoais, a ISO elaborou a ISO 27001, seguida de várias outras normativas, as quais geraram padrões de segurança que devem ser adotados por inúmeras organizações. A norma ISO 27001 determina instruções e princípios globais com intuito de guardar, preservar e aperfeiçoar o gerenciamento de segurança da informação nas organizações. Esta norma abrange uma fragmentação quanto ao método de análise e tratamento de riscos que incluem 11 seções diferentes: (1) política de segurança da informação; (2) organização da segurança da informação; (3) gestão de ativos; (4) segurança em recursos humanos; (5) segurança física e do ambiente; (6) gestão de operações e comunicações; (7) controle de acesso; (8) aquisição, desenvolvimento e manutenção de sistemas de informação; (9) gestão de incidentes de segurança da informação; (10) gestão de continuidade dos negócios e (11) conformidade (BRASIL, 2018).

Quanto à gestão de risco pode ser executada baseada na ISO 27005, uma vez que esta norma contém orientações e oferece suporte para estabelecer o processo de gestão de risco de segurança da informação (ABNT, 2011). Alguns procedimentos para o plano de resposta são disponibilizados pela norma ISO/IEC 27005, conforme Bergamaschi e Zuchi (2018), este plano de risco inclui: (1) mitigação (redução); (2) aceitação (ou tolerância); (3) transferência (ou compartilhamento) e (4) evitando (ou eliminando) riscos. O Ministério da Economia (2020) descreve que a ISO/IEC 27005 expõe diretrizes visando o processo de gestão de riscos de segurança da informação de organizações, satisfazendo em especial as exigências de um SGSI, de acordo com a NBR ISO/IEC 27001.

Outra norma essencial para políticas de segurança consiste na norma ABNT NBR ISO/IEC 29100 de 2020 que disponibiliza uma estrutura de privacidade que especifica um vocabulário comum de privacidade, assim como, caracteriza os agentes e os seus papéis para o tratamento de dados pessoais, além de apontar as considerações de proteção de privacidade e viabiliza as referências para princípios conhecidos de privacidade para tecnologia da informação (ABNT, 2020).

A NBR ISO 31000 apresenta princípios e diretrizes que contemplam a gestão de riscos e podem ser aplicadas por qualquer organização pública ou privada. O processo de gestão de riscos desta norma engloba quatro etapas: (1) Identificação de riscos; (2) análise de riscos; (3) avaliação de riscos e (4) tratamento de riscos (ABNT, 2020).

Além disso, a ISO 31000, de acordo com seus princípios, leva em consideração as capacidades, percepções e intenções do pessoal interno e externo como condição favorável ou agravante para concretização dos objetivos da organização. Desta forma, o processo de gestão de risco tem como base este conceito para concepção de todos os seus elementos, principalmente, nos elementos de análise e avaliação (CAMPOS. 2007)

2.3 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Um sistema de gestão da segurança da informação apropriado, adequado e eficaz fornece garantia à direção da organização e a outras partes interessadas de que suas informações e outros ativos associados estão mantidos razoavelmente seguros e protegidos contra ameaças e danos, permitindo assim que a organização atinja os objetivos de negócios declarados.

Cabe mencionar que incidente de segurança é “uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento” (BRASIL, 2023).

Os incidentes de segurança da informação devem ser respondidos de acordo com os procedimentos documentados. Um incidente de segurança da informação pode ou não envolver Tecnologia da Informação e Comunicação (TIC). Um exemplo pode ser os incidentes que ocorrem a partir de documentos em meios físicos.

A norma ABNT NBR ISO/IEC 27035-3:2021 (Gestão de Incidentes de Segurança da Informação) foi publicada no Brasil em 15 de julho de 2021. No que diz respeito às diretrizes para operações de resposta a incidentes, a referida norma considera apenas operações de resposta a incidentes relacionados à TIC. É

importante ressaltar que estar norma suporta os controles da NBR 27001, Anexo A, relacionados à gestão de incidentes.

A NBR 27035-3 apresenta orientações para a resposta a incidentes de segurança da informação em operações de TI e cobre aspectos operacionais de segurança de TI sob a perspectiva de pessoas, processos e tecnologia. Adicionalmente, ela se aprofunda na resposta a incidentes de segurança da informação em operações de TI, incluindo identificação de incidentes de segurança da informação, relatórios, triagem, análise, resposta, contenção, erradicação, recuperação e conclusão.

Esta norma é fundamentada no modelo de fases de gestão de incidentes de segurança da informação, exposto na ISO/IEC 27035-1:2016: identificação e geração de relatórios; avaliação e decisão; e respostas. Os princípios propostos neste documento são genéricos e visam ser aplicáveis a todas as organizações, independentemente de seu tipo, tamanho ou características. Cabe a cada organização adaptar as disposições apresentadas nesta norma em relação à situação de risco à segurança da informação.

2.3.1 Construção do plano resposta

Por outro lado, resposta a incidentes representa o procedimento que especifica como uma organização deve abordar um incidente de segurança, seja um ataque cibernético, uma violação dos dados, a presença de um software malicioso (como um vírus) ou um descumprimento das diretrizes e normas de segurança da organização. A meta é mitigar os prejuízos que poderiam ser provocados pelo incidente, diminuir o período de resposta e os custos de recuperação.

O plano de resposta a incidentes é um documento formal composto de um conjunto de procedimentos e ferramentas que os profissionais de tecnologia da informação (TI) devem adotar para superar os problemas relativos à segurança que surgem no dia a dia organizacional e busca assegurar uma resposta eficiente e eficaz a tais incidentes. Para tanto, é importante que a organização estabeleça e comunique os procedimentos de resposta aos incidentes de segurança da informação para todas as partes interessadas pertinentes. É crucial que os incidentes de segurança da

informação sejam respondidos por uma equipe designada com a competência necessária (BURKART, 2021).

O plano de resposta deve incluir: contenção, visto que as consequências do incidente podem se espalhar aos sistemas afetados pelo incidente; coleta de evidências o mais rápido possível após a ocorrência; escalonamento, conforme necessário, incluindo atividades de gestão de crises e possivelmente invocação de planos de continuidade de negócios; garantia de que todas as atividades de resposta envolvidas sejam devidamente registradas para análise posterior; comunicação da existência do incidente de segurança da informação ou quaisquer detalhes relevantes deles a todas as partes interessadas internas e externas seguindo o princípio da necessidade de conhecer; coordenação com partes internas e externas, como autoridades, grupos de interesse externo e fóruns, fornecedores e clientes para melhorar a eficácia da resposta e ajudar a minimizar as consequências para outras organizações; uma vez que o incidente foi tratado com sucesso, formalmente fechá-lo e registrá-lo; análise forense de segurança da informação, conforme necessário; análise pós-incidente para identificar a causa-raiz; identificação e gestão de vulnerabilidades e fragilidades de segurança da informação, incluindo aquelas relacionadas com os controles que causaram, contribuíram ou falharam em prevenir o incidente.

A ISO 27002 teve sua versão atualizada em fevereiro de 2022 e foi elaborada no Comitê Brasileiro de Tecnologias da Informação e Transformação Digital (ABNT/CB-021), pela Comissão de Estudo de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade (CE-021:004.027). O Projeto de Revisão circulou em Consulta Nacional conforme Edital nº 07, de 19.07.2022 a 17.08.2022.

Este documento foi projetado para empresas de todos os tipos e tamanhos. É para ser utilizado como referência para determinar e implementar controles para tratamento de riscos de segurança da informação em um sistema de gestão de segurança da informação (SGSI) baseado na ABNT NBR ISO/IEC 27001.

Também pode ser usado como um documento de orientação para organizações determinando e implementando controles de segurança da informação comumente aceitos. Além disso, este documento é destinado a ser utilizado no desenvolvimento de diretrizes de gestão de segurança da informação específicas para

a indústria e a organização, considerando seu ambiente específico de riscos de segurança da informação.

Controles organizacionais ou específicos do ambiente que não sejam os incluídos neste documento podem ser determinados através do processo de avaliação de riscos, conforme necessário.

3 METODOLOGIA

A metodologia utilizada foi a descritiva e quanto a sua abordagem foi qualitativa dos resultados e com caráter exploratório, fundamentada em fontes primárias como livros, artigos, dissertações e teses voltadas a Lei Geral de Proteção de Dados e resposta a incidentes de segurança da informação e privacidade.

A pesquisa descritiva é apropriada a casos em que objetiva-se ter conhecimento acerca de características de determinado grupo, estabelecer, conhecer as relações existentes entre variáveis, bem como avaliar os impactos de implantação de um determinado programa.

Os dados obtidos através de uma pesquisa descritiva também fornecem importantes direções a serem seguidas em estudos futuros, principalmente quando indicam a existência de relação entre variáveis e quer conhecer a extensão dessa relação.

Vergara (2017) afirma que a pesquisa descritiva expõe as características de determinada população ou fenômeno, estabelece correlações entre variáveis e define sua natureza. Segundo a autora, esse tipo de pesquisa "Não têm o compromisso de explicar os fenômenos que descreve, embora sirva de base para tal explicação". Já a pesquisa qualitativa,

Segundo Minayo (2002, p,22)

> trabalha com o universo de significados, motivações, aspirações, crenças, valores e atitudes, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variável.

De acordo com Minayo (2002, p.43) “esse tipo de pesquisa (qualitativa) não pode basear-se no critério numérico, para poder garantir sua representatividade. A

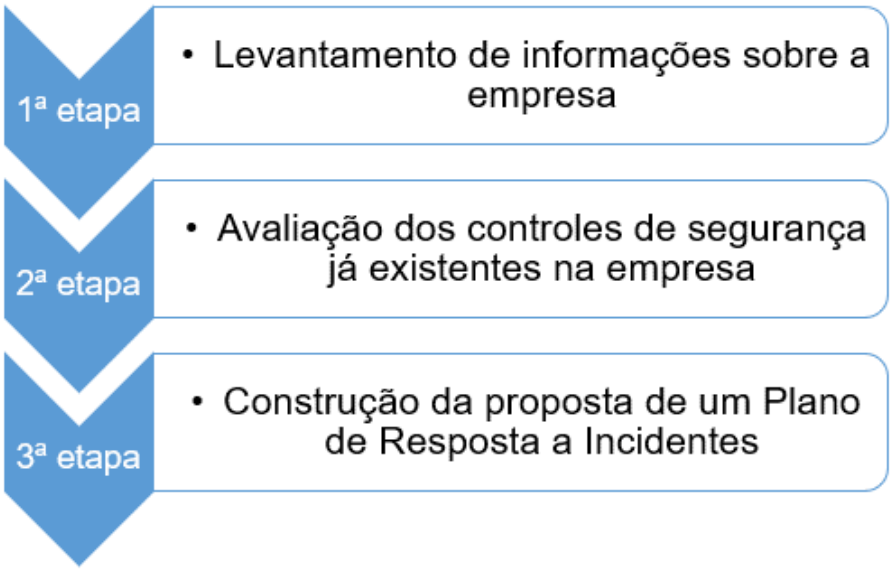
amostragem boa é aquela que possibilita abranger a totalidade do problema investigado em suas múltiplas dimensões".

Quanto ao método de procedimento foi elaborada uma proposta de resposta a incidentes de segurança da informação em uma empresa do ramo de fabricação de implementos rodoviários.

A coleta de dados ocorreu preliminarmente em base de dados que abordam a temática objeto desse estudo. Posteriormente, para a elaboração da proposta, foram obtidos dados da empresa do ramo de fabricação de implementos rodoviários e tendo também como base planos de resposta a incidentes de segurança da informação e privacidade implantados em outras empresas.

A Fig. 1 ilustra o fluxograma com as fases da pesquisa realizada nesse trabalho.

Figura 1: Fluxograma das fases da pesquisa.



Fonte: Do autor (2023)

A primeira etapa envolve a coleta de informações detalhadas sobre a empresa, seus ativos de informação, processos de negócio e infraestrutura tecnológica. Isso inclui identificar e categorizar os dados críticos, entender como esses dados são usados, guardados e transferidos, e identificar possíveis pontos de vulnerabilidade.

Uma vez que uma compreensão clara da empresa e de seus ativos de informação seja estabelecida, a próxima etapa é avaliar as medidas de segurança

existentes. Isso envolve uma análise completa dos controles de segurança atualmente em vigor, incluindo firewalls, programas antivírus, sistemas de detecção e prevenção de intrusão, políticas de acesso e outras medidas de segurança física e lógica.

A avaliação deve identificar quaisquer lacunas ou deficiências nas medidas de segurança existentes. Além disso, ela deve considerar a eficácia das respostas a incidentes passados, se houver.

A última etapa do processo é a criação de um plano abrangente de resposta a incidentes de segurança, abordando desde pequenas a grandes violações de dados. O plano deve cobrir a identificação, preparação, contenção, erradicação, recuperação, comunicação e preceitos assimilados. É um processo contínuo que deve ser atualizado regularmente e envolver treinamento da equipe. Este plano é apenas um componente de uma estratégia de segurança da informação mais ampla, incluindo prevenção e mitigação de incidentes.

4 RESULTADOS E DISCUSSÕES

4.1 PERFIL DA EMPRESA

A empresa atua há 54 anos na cidade de Içara, em Santa Catarina. Conta atualmente com 2.000 colaboradores diretos. Até o momento, a empresa não enfrentou nenhum incidente de segurança de nível crítico que viesse a ocasionar uma parada operacional ou vazamento de dados na internet.

Ainda não foi desenvolvido um plano de resposta devido ao fato de o departamento de tecnologia da informação ter sido alçado ao patamar de setor estratégico há apenas 2 anos. Por se tratar de uma empresa familiar que está há muitos anos no mercado, o objetivo era fazer o negócio funcionar, nem sempre se atendo a aplicação de boas práticas em segurança da informação.

Essas implementações passaram a ter maior relevância nos processos a partir da promulgação da LGPD, com a contratação de mais profissionais para a equipe, com foco no tema de segurança da informação, e apoio da alta gestão.

4.2 PROPOSTA DE PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Preliminarmente, cabe mencionar que o objetivo de propor a inserção de um plano de resposta a incidentes de segurança da informação é propiciar que a empresa objeto desse estudo tenha condições de responder a situações emergenciais. O plano de resposta a incidentes é pautado em um documento formal que deve ser prático e de extrema confiabilidade e que auxilia na prevenção de novos incidentes, sem deixar de atender as exigências legais, tanto de transparência como de comunicação.

O plano proposto nesse trabalho deve conter as funções e as responsabilidades de cada integrante da equipe de colaboradores, bem como quais são as medidas que precisam ser adotadas para que a empresa tenha condições de responder a um incidente de maneira adequada, tendo como meta a preservação da integridade tanto dos processos como dos sistemas de forma a proteger os dados e sua privacidade.

Tal plano precisa ser aplicável em qualquer tipo de incidente que envolva dados pessoais e precisa ser analisado levando em consideração todas as políticas da empresa.

A equipe que será responsável pela resposta aos incidentes precisa ser delimitada previamente da seguinte forma:

- Notificador: indivíduo ou sistema de monitoramento que reporta o incidente;
- Acionador(es): profissional responsável pelo recebimento das notificações e por realizar o tratamento inicial (triagem) do incidente;
- Time de Resposta a Incidentes (TRI): conjunto de funcionários da organização, com permissões, competências, obrigações, capacitação e saberes para lidar com uma ampla gama de incidentes. O TRI será acionado de acordo com as particularidades de cada incidente, sendo formado pelo Encarregado de Dados (DPO) e por profissionais de outros setores que possuam conhecimento especializado para tratar do assunto ou cujos procedimentos tenham sido impactados pelo incidente.

A Tab. 1 ilustra os profissionais que fazem parte do Time de Resposta a Incidentes (TRI).

Tabela 1: Time de Resposta a Incidentes (TRI).

Profissionais	**Habilidades necessárias**
Gestor / líder da equipe	Capacidade de liderar equipes; Integridade e confiança para manter a reputação da equipe.
Equipe de triagem	Discernimento para levantar os pontos mais relevantes ao analisar uma situação; Condições de tratar de vulnerabilidades.
Equipe de análise de artefatos	Gerenciamento de incidentes; Habilidade de lidar com estresse e trabalho sob pressão.
Especialistas em plataformas	Conhecimento sobre: a Infraestrutura de redes e protocolos; o funcionamento da internet e deep web; os protocolos de aplicação e serviços.
Responsável pelo sistema	Conhecimento sobre: os princípios de segurança; os riscos e as ameaças a redes e sistemas de computadores; as tecnologias de criptografia e certificação digital; a segurança de endpoints; capacidade de propor soluções de resposta, bem como, autorizar ou vetar procedimentos de emergência.
Responsável por processo	Gerente ou chefe do setor identificado na estrutura organizacional, com capacidade de propor soluções de resposta; Conhecer as recentes estratégias de ataque e vulnerabilidades e as formas de combater as ameaças emergentes.

Fonte: Do autor (2023)

Este plano de resposta a Incidentes está estruturado de acordo com as macro etapas a seguir descritas.

a) Identificação

Identificar o incidente de segurança é essencial para que o plano de respostas seja implementado. É preciso que a organização possua as principais medidas que detectam e identificam incidentes e, para tanto, necessitam de ferramentas que ajudem a monitorar possíveis motivadores desses incidentes. É necessário que os colaboradores sejam capacitados, para que tenham condições de identificar os vazamentos de dados a que venham a tomar conhecimento.

b) Preparação

As práticas de emergência precisam ser executadas e os tempos de respostas precisam ser mensurados, para que a resposta a um incidente seja executada prontamente. Para tanto, é necessária a elaboração de uma metodologia que propicie a agilidade e a exatidão necessárias.

c) Contenção

Posteriormente à identificação de um incidente é necessário que esse seja contido e isolado para que não sejam afetados outros sistemas e processos. Dessa forma, será possível evitar maiores danos. Tal etapa tem em seu escopo a contenção de curto e longo prazo, bem como o backup do sistema.

De forma simultânea à etapa de contenção é necessária a adoção de medidas que propiciam a documentação do incidente, para que esta seja registrada.

d) Erradicação

A remoção da ameaça bem como a restauração dos sistemas e processos que foram afetados deve ocorrer após a contenção.

e) Recuperação

Buscando garantir que nenhuma ameaça permaneça é necessário que os sistemas e processos que foram afetados retornem ao ambiente de produção.

f) Preceitos assimilados (Lições aprendidas)

A última etapa é atualizar o plano de resposta a incidentes contendo todas as ações que foram realizadas. Isso irá contribuir para que a equipe verifique o que pode ser melhor executado nos futuros incidentes.

g) Documentação do Incidente

O incidente precisa ser documentado de maneira detalhada, incluindo todas as ações implementadas nas etapas anteriores e as lições aprendidas com o caso.

Será necessária a realização de simulações de acionamento do plano de reposta a incidentes de forma periódica, com o objetivo das equipes se manterem treinadas. Essa simulação propicia maior compreensão do grau de maturidade em privacidade da empresa no que diz respeito a possíveis incidentes de segurança. A proposta é que a empresa simule um episódio de incidente de segurança de dados, a fim de verificar se a programação de resposta é executada com a velocidade adequada, envolvendo as áreas e gestores que precisam ser envolvidos e com a preservação correta das evidências relacionadas.

O fluxograma, que será apresentado na Fig. 2, foi elaborado para ilustrar, de forma clara e visual, as etapas essenciais e as decisões que a equipe de resposta a incidentes precisa tomar após o registro de um incidente de segurança da informação.

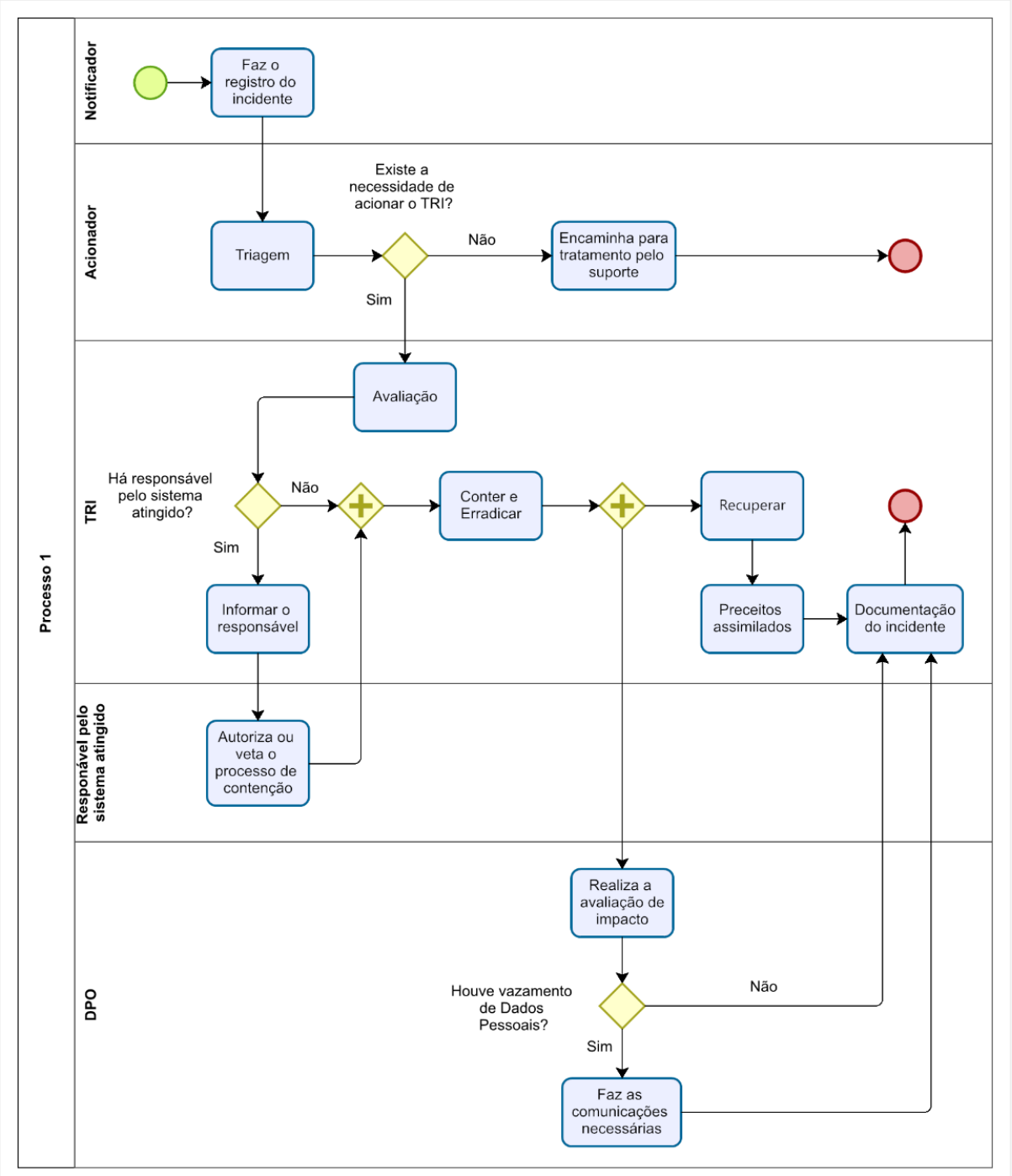
O processo tem início quando um incidente é relatado pelo notificador. Esse relatório inicial é então direcionado para um profissional encarregado de realizar a triagem. Durante essa etapa é avaliado a gravidade do incidente e se determina a necessidade da intervenção do time de resposta a incidentes.

Se a situação não requer uma ação especializada, o chamado é direcionado para tratamento ordinário, que pode envolver soluções de rotina ou reparos menores. No entanto, se o incidente for sério o suficiente, o time de resposta a incidentes é acionado.

Uma vez que a time de resposta a incidentes é acionado, inicia-se o processo de avaliação. Isso envolve uma análise detalhada do incidente e seus possíveis impactos. Se o sistema afetado tiver um responsável específico, essa pessoa também é notificada.

O time de resposta a incidentes então trabalha para conter e erradicar o problema. Isso pode envolver uma variedade de ações, dependendo da natureza do incidente, incluindo o isolamento de sistemas afetados, a remoção de *malware* ou a correção de falhas de segurança.

Figura 2: Diagrama do processo de resposta a incidentes de segurança da informação.



Fonte: Do autor (2023)

Durante essa fase, o Encarregado de Dados (DPO) também realiza uma avaliação de impacto. Isso envolve determinar se houve qualquer vazamento de dados pessoais e, se sim, quão grave foi o vazamento, acionando o plano de comunicação.

A etapa seguinte é a recuperação dos sistemas afetados. Que pode envolver a restauração de dados a partir de backups, a reparação de hardware ou software danificado, ou a implementação de novas medidas de segurança.

Finalmente, após a conclusão do processo de resposta, a equipe realiza uma revisão do incidente. Isso inclui a análise das ações tomadas, a identificação de lições aprendidas e a documentação do incidente. Esse passo é crucial para melhorar a resposta a futuros incidentes e para fortalecer as medidas de segurança da organização.

A utilização do plano resposta pode auxiliar, inclusive, no que será ou não comunicado. Importante mencionar que o plano de resposta deve sempre se ater ao porte da instituição, bem como suprir as exigências normativas em relação à política de segurança da informação.

O plano resposta cria um mecanismo de evolução orgânica da empresa, bem como diminui gastos futuros em razão de incidentes de segurança da informação.

5 CONCLUSÕES

Diante do exposto conclui-se que é imprescindível que as empresas possuam um plano de resposta a incidentes, que seja aplicado em qualquer caso de incidentes envolvendo dados, devendo ser observado em conjunto com as demais políticas da empresa por todas as áreas, colaboradores e prestadores de serviços que possam vir a ter acesso às informações, arquivos e dados.

Os sistemas relativos ao tratamento de dados não são impenetráveis e, sendo assim, estão sujeitos a falhas e invasões. Desse modo, no momento da ocorrência de incidentes de segurança o ponto chave a ser analisado é a forma de atuação da empresa, ou seja, se possui uma política de prevenção e plano de resposta, este último para adequar, corrigir e melhorar os erros que o sistema apresentou.

O plano de resposta é um meio de lidar com o incidente, no intuito de limitar os danos à organização, reduzir os custos e o tempo de recuperação desta. Não só isso, com um bom plano, a empresa consegue atualizar sua forma de atuação a fim de melhorar o seu sistema e cumprir a legislação com maior eficácia.

Em futuros trabalhos, será relevante explorar o plano de continuidade do negócio, que se alinha ao plano de resposta a incidentes de segurança da informação e foca em garantir a continuidade operacional durante incidentes significativos. O estudo deverá abordar a identificação de processos críticos, soluções de recuperação, estratégias de comunicação e treinamento. Tal pesquisa poderá fornecer valiosos esclarecimentos para a preparação efetiva das organizações contra incidentes de segurança da informação.

REFERÊNCIAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005: **Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro. 2011.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 29100: **Tecnologia da informação – Técnicas de segurança – Estrutura de Privacidade**. Rio de Janeiro. 2020.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 31000: **Tecnologia da informação – Técnicas de segurança – Gestão de riscos** Rio de Janeiro. 2020.

BERGAMASCHI, A.A.; ZUCHI, J.D. Gerenciamento de tempo com base em informação e metodologias ágeis. **Revista de interface tecnológica**, v.15, n.1, 2018.

BRASIL. Constituição (2018). Lei nº 13.709, DE 14 DE AGOSTO DE 2018., de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República. Secretária-Geral. Subchefia Para Assuntos Jurídicos, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 ago. 2022.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018, p. 13-15.

BURKART, Daniele Vincenzi Villares. **Proteção de dados e o estudo da LGPD**. 2021. 141 f. Dissertação (Mestrado) - Curso de Programa de Pós-Graduação Mestrado em Mídia e Tecnologia, Faculdade de Artes, Arquitetura e Comunicação, Universidade Estadual Paulista Júlio de Mesquita Filho, Bauru, 2021. Disponível em: https://repositorio.unesp.br/handle/11449/204091. Acesso em: 15 ago. 2021.

CAMPOS, Andre L. N.. **Sistema de Segurança da Informação**: controlando os riscos. 2. ed. Florianópolis: Visual Books, 2007.

CELIDONIO, Tiago; NEVES, Paulo Sergio; DONÁ, Claudio Melim. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira - Um estudo de caso. **Brazilian Journal Of Business**, [S.L.], v. 2, n. 4, p. 3626-3648, 2020. Brazilian Journal of Business. http://dx.doi.org/10.34140/bjbv2n4-012.

DOLES, Luiz Gustavo da Silva; CÁRNIO, Thaís Cíntia. A Lei Geral de Proteção aos Dados e as alterações no cotidiano das empresas na ordem ibero-americana. In: VEIGA, Fábio da Silva *et al*. **Governança e direitos fundamentais**: revisitando o debate entre o público e o privado. Porto, Portugal: Instituto Ibero-americano de Estudos Jurídicos, 2020. p. 25-32.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação** Rio de Janeiro. Ciência Moderna, 2008.

MINAYO, M. C. de S. (Org.). **Pesquisa social**: teoria, método e criatividade. 19. ed. Petrópolis: Vozes, 2002.

RIBAS, Brenno Henrique de Oliveira; GUERRA, Caroline Cardoso. O impacto do regulamento geral de proteção de dados pessoais da União Europeia no Brasil. In:

VEIGA, Fábio da Silva *et al*. **Governança e direitos fundamentais**: revisitando o debate entre o público e o privado. Porto, Portugal: Instituto Ibero-americano de Estudos Jurídicos, 2020. p. 75-83.

ROCHA, Camila Pereira da *et al*. Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD. **Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará**, [S.l.], v. 2, n. 3, p. 78-97, ago. 2019.

SÁ, Marcelo Dias de. **Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas**: aplicações mobile do governo. 2019. 39 f. Monografia (Especialização) - Curso de Especialização em Informática, Departamento de Ciência da Computação, Universidade Federal de Minas Gerais, Brasília, 2019.

STALLINGS, Willian. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015. 560p.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas: Parlamento Europeu; 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 16 ago. 2021.

VERGARA, Sylvia Constant. **Métodos de Pesquisa em Administração**. 10ª. ed. São Paulo: Atlas, 2009. Capítulo 4, pp. 46-53.