PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

SECURITY INCIDENT RESPONSE PLAN

JULIANA TORRES FERRAZ[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. IMPACTOS GERAIS DO VAZAMENTO DE DADOS. 3. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA. 4. SANÇÕES AO CONTROLADOR. 5. BREVE COMPARATIVO À LEGISLAÇÃO E JURISPRUDÊNCIA EUROPEIA. 6. PROPOSIÇÕES CONCLUSIVAS. REFERÊNCIAS BIBLIOGRÁFICAS.

RESUMO

O presente artigo tem por objetivo discorrer sobre a importância de uma reação rápida e efetiva na hipótese de um incidente de segurança, bem como explicitar a forma de elaboração de um plano de resposta. A problemática enfrentada pela pesquisa é fornecer elementos concretos para implementação das exigências da Lei Geral de Proteção de Dados (LGPD), haja vista que a jurisprudência brasileira ainda não se encontra consolidada. Assim, realiza-se um estudo breve de comparação com a jurisprudência e legislação europeias, especificamente, quanto à General Data Protection Regulation (GDPR). O artigo conclui que é essencial a implementação pelo controlador de dados de um plano de respostas eficaz, a fim de que o impacto das sanções previstas na LGPD seja minimizado. A pesquisa foi realizada pela técnica de pesquisa documental e bibliográfica.

Palavras-chave: Direito digital; Incidentes de segurança; Plano de resposta; Sanções; LGPD e GDPR;

ABSTRACT

This article aims to discuss the importance of a quick and effective reaction in the event of a security incident, as well as to explain how to prepare a response plan. The problem faced by the research is to provide concrete elements for implementing the requirements of the General Law of Data Protection (LGPD), given that Brazilian case law is not yet consolidated. Thus, a brief study of comparison with European jurisprudence and legislation is conducted, specifically with regard to the General Data Protection Regulation (GDPR). We conclude that it is essential that the data controller implement an effective response plan, so that the impact

[1]Estudante do 4º ano diurno do curso de graduação em Direito na Faculdade de Direito de Sorocaba.

of the sanctions provided for in the LGPD is minimized. The research was conducted by the technique of documentary and bibliographic research.
Keywords: Digital law; Security incidents; Response plan; Sanctions; LGPD and GDPR;

1 INTRODUÇÃO

Neste trabalho serão estudados alguns regulamentos da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que regula as atividades de tratamento de dados pessoais. Pretende-se abordar, especificamente, sobre a necessidade da elaboração de um plano de respostas a incidentes de segurança, a fim de preservar os dados do titular, em conjunto com uma análise dos meios necessários para minimizar o impacto das sanções.

Entretanto, percebe-se que a LGPD não define o que são incidentes de segurança, mas exemplifica as possíveis situações que se encaixam como incidentes, ou seja, aquelas capazes de afetar a tríade de segurança de informação, composta pela confidencialidade, integridade e disponibilidade de dados, conforme art. 46 da LGPD. É imprescindível que, para ser considerado um incidente de segurança, haja a ocorrência de diversos eventos de segurança de informação, capazes de comprometer as operações de negócios e ameaçar a segurança de informação, verificados em um curto espaço de tempo, de mesma origem, em uma tentativa de acesso por força bruta.

O tema torna-se mais presente no século XXI, visto que, frequentemente, é possível observar casos de perda ou roubo de dispositivos físicos, perda ou roubo de documentos com dados pessoais, acesso não autorizado de dados, divulgação inadvertida ou realização de golpes para utilização de dados. A presente situação é decorrente da revolução tecnológica, iniciada entre o final dos anos 1950 e dos anos 1970, com a expansão do uso de computadores digitais. Todavia, a regulação dessas medidas permanecia ainda muito precária, contando atualmente com as primeiras bases de um efetivo controle seguro de dados por meio da LGPD. É perceptível que os controladores de dados ainda não dispõem de um conhecimento vasto sobre o tema, haja vista que a jurisprudência ainda não se encontra estabelecida.

Sendo assim, pretende-se conduzir uma análise da forma mais adequada para implementação de um controle prévio e posterior de vazamento de dados, pela elaboração de um plano de respostas, a fim de diminuir os impactos das sanções aplicadas pela LGPD, por meio de uma breve comparação com a legislação e jurisprudências europeias.

2 IMPACTOS GERAIS DO VAZAMENTO DE DADOS

O impacto do vazamento de dados afeta pessoas físicas e jurídicas, com danos morais e materiais. Para os agentes de tratamento, os riscos são inúmeros, como perda do controle dos dados, desvalorização no mercado de ações, danos reputacionais e, consequentemente, sua difícil recuperação. Além disso, haverá aplicação de sanções e a necessidade de notificação de órgãos reguladores e de entidades. Quanto aos titulares, verificar-se-ão danos psicológicos, financeiros, emocionais, somados de discriminação, extorsão, fraudes e até mesmo roubo de identidade. Em suma, os riscos podem ser divididos em três grupos, quais sejam: riscos jurídicos, reputacionais e operacionais.

Na gama de riscos jurídicos, provavelmente se verificará uma multiplicação de ações, promovidas pelos titulares de dados expostos, assim como investigações e sanções por parte das autoridades responsáveis, tal como a Secretaria Nacional do Consumidor (Senacon) e o Ministério Público, bem como constantes ações coletivas e a ocorrência de violação a cláusulas contratuais. No que se refere aos riscos reputacionais, percebe-se que os procedimentos das empresas passarão a ser questionados. Ainda, na ocorrência de um incidente, é muito provável que ocorra a exposição desta nos meios de comunicação. Além disso, quanto aos prejuízos operacionais, a consequente perda de ativos e as perdas operacionais.

O tema tem grande relevância entre as instituições financeiras, fato este potencializado com a recente criação dos bancos digitais. Sabe-se que o Banco Inter, em 2018, sofreu um relevante incidente de segurança, capaz de vazar dados de diversos clientes. Diante desse episódio, o Banco Inter alegou pela inexistência de ataque hacker, justificando que o vazamento teria ocorrido por meio de pessoa autorizada internamente. Ocorre que nenhuma justificativa foi capaz de controlar as consequências do vazamento de dados de milhares de clientes, em que se forneceu acesso a informações pessoais, senhas, cópias de cheques, imagens de contratos, chaves de segurança, entre outros. Em suma, percebeu-se que o Banco Inter não protegeu adequadamente os dados pessoais dos clientes e daqueles que mantiverem transações bancárias.

A situação motivou a Comissão de Valores Mobiliários (CVM) a entrar com um processo contra o Banco Inter. Além disso, o Ministério Público do Distrito Federal ajuizou uma ação civil pública por danos morais, com amparo no artigo 14, parágrafo 1º, do CDC, no qual prevê a responsabilidade do fornecedor de serviços, independentemente da existência de culpa. Lembre-se, ademais, que o Código de Defesa do Consumidor é aplicável às instituições financeiras, conforme definido pela Súmula 297 do STJ, e que as instituições financeiras

respondem, objetivamente, pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros, no âmbito de operações bancárias, de acordo com o disposto na Súmula 479 do STJ.

Outrossim, a Comissão de Proteção dos Dados Pessoais do Ministério Público do Distrito Federal e Territórios ajuizou uma ação civil pública por danos morais coletivos contra o Banco Inter S/A, requisitando a condenação no pagamento de 10 milhões de indenização, visto que a ré não tomou os cuidados necessários de segurança de dados pessoais de milhares de indivíduos, clientes e não clientes. Na ocasião, sabe-se que o Banco não avisou às autoridades acerca do acontecimento, ao falhar contra um dos pressupostos básicos de um plano de resposta aos incidentes de segurança, os quais serão analisados de forma mais detalhada adiante.

3 PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

A atuação preventiva contribui para a diminuição da ocorrência de incidentes, que, por consequência, minimiza o impacto dos prejuízos ao responsável. A LGPD, na seção de "Boas Práticas e de Governança", descreve uma série de providências a serem tomadas para situações concretas. Nesse sentido, aqueles que se atrasarem nessas adequações estarão em dissonância com a GDPR Europeia (General Data Protection Regulation) e a própria LGPD.

Essas medidas se demonstram ainda mais essenciais no momento da aplicação das sanções, visto que a existência de prevenção se torna um diferencial para o abrandamento das penalidades. Nas condenações por danos morais, por exemplo, o que se demonstra é que quando a organização não fez nada para impedir o dano, o arbitramento é definido em valores altíssimos se comparados aos que a organização agiu para impedi-los, ou quando o titular foi informado e se buscou identificar e responsabilizar o responsável. Assim sendo, é importante verificar um recente julgado do Tribunal de Justiça do Estado de São Paulo, em que houve majoração dos danos morais, devido à grave violação à intimidade e à privacidade:

> APELAÇÃO – AÇÃO CONDENATÓRIA – PRESTAÇÃO DE SERVIÇOS EDUCACIONAIS – VAZAMENTO DE DADOS PESSOAIS POR PREPOSTO – CELULAR DA AUTORA PASSADO A UM TERCEIRO – RECEBIMENTO DE MENSAGENS DE ASSÉDIO SEXUAL – RECURSO DE AMBAS AS PARTES – LEGITIMIDADE PASSIVA DA RÉ – RESPONSABILIDADE PELOS DANOS DECORRENTES DA VIOLAÇÃO AO TRATAMENTO DE DADOS PESSOAIS – LEI GERAL DE PROTEÇÃO DE DADOS **– DANOS MORAIS EVIDENTES – MAJORAÇÃO – GRAVE VIOLAÇÃO À INTIMIDADE E À PRIVACIDADE** 1 – A empresa controladora de dados pessoais é figura legítima para figurar no polo passivo de demanda que objetive a indenização pelo vazamento de dados da autora orquestrados por preposto da ré, que repassou o celular da autora para um colega

> para fins de assédio sexual (LGPD, art. 42). 2 – A ré, ao dar causa ao vazamento de dados, responde pelos danos morais sofridos (LGPD, art. 5º, VI e 42, caput). 3 – É cabível a indenização por danos morais, considerando a violação grave ao direito à intimidade e à privacidade causado pela quebra do dever de proteção de dados pessoais, o que propiciou assédio sexual agressivo. 4 – **Indenização majorada, pois a gravidade da situação, a séria negligência da empresa, a postura recalcitrante em reconhecer o erro, e a incipiente jurisprudência estadual autorizam resposta mais enérgica.** Valor de dez mil reais que se mostra mais condizente com o cenário narrado. RECURSO DA RÉ NÃO PROVIDO. RECURSO DA AUTORA PROVIDO. (TJSP; Apelação Cível 1006311-89.2020.8.26.0001; Relator (a): Maria Lúcia Pizzotti; Órgão Julgador: 30ª Câmara de Direito Privado; Foro Regional I - Santana - 8ª Vara Cível; Data do Julgamento: 01/09/2021; Data de Registro: 01/09/2021) "grifo nosso".[2]

Nesse viés, percebe-se que é imprescindível a criação e aplicação de um plano de resposta aos incidentes, que, em síntese, divide-se em três etapas: preparação, resposta e avaliação.

A *preparação* é uma etapa prévia de medidas anteriores a um possível incidente, em que ocorre a confecção de um documento com todos os procedimentos a serem adotados, incluindo as devidas atribuições aos agentes no processo de resposta. Nessa fase, torna-se fundamental a criação de um *"war room",* ou seja, um comitê de gestão de crise, responsável por tomar as medidas necessárias nas primeiras horas de um incidente, composto por perfis de diversas áreas, como compliance, jurídico, recursos humanos, negócios, além de representantes de tecnologia e segurança de informação.

Entende-se que os membros desse comitê serão estabelecidos por uma questão de estruturação interna, mas recomenda-se que, ao menos, estejam presentes o encarregado ou o DPO (*Data Protection Officer)*[3] e os demais agentes das áreas de controle. Eventualmente, poderá ser preciso contar com profissionais externos, especializados, que devem ser antevistos, deixando-os de *standy by* para atuarem imediatamente quando ocorrer um episódio.

Veja-se que o papel do *Data Protection Officer (DPO)* é essencial, aquele que é encarregado de cuidar das questões referentes à proteção dos dados da organização e seus clientes, o qual deve supervisionar o responsável pelo tratamento, a fim de que cumpra as obrigações estabelecidas em lei. Nos termos do art. 5º, inciso VIII, da LGPD é o: "encarregado: pessoa indicada pelo controlador e operador para atuar como canal de

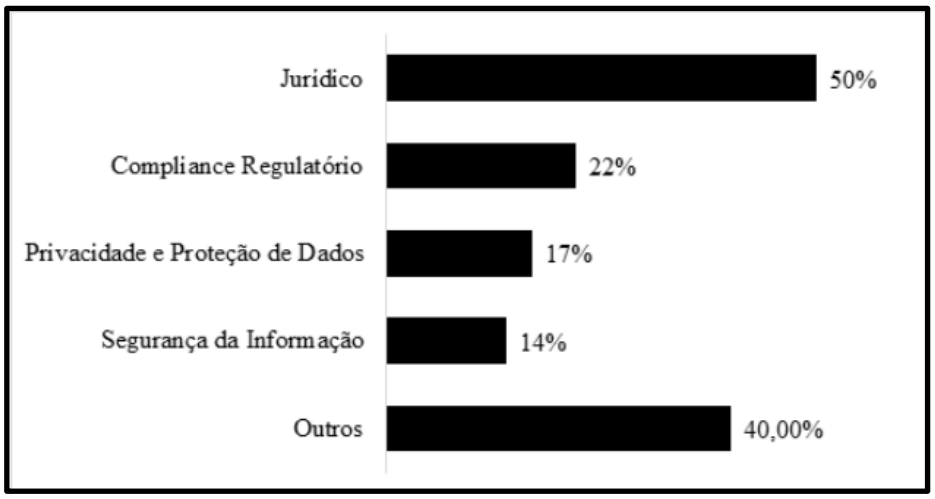
[2]BRASIL. TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Apelação Cível 1006311-89.2020. 8.26.0001. Relatora Maria Lúcia Pizzotti. 30ª Câmara de Direito Privado. Foro Regional I - Santana, 8ª Vara Cível. 01/09/2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14982708&cdForo=0. Acesso em 24 nov. 2021.

[3]Oficial de Proteção de Dados.

comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". Aliás, é imprescindível considerar que o ponto de referência sempre será o DPO, de modo que este deve estar atento às atuações do controlador de dados ou da organização.

Dessa maneira, torna-se necessário apontar o resultado da pesquisa publicada pela *International Association of Privacy Professionals*[4] (IAPP), da divisão de funções de privacidade nas organizações, em que se percebe um comitê com alta força jurídica (50%):

Figura 1[5]



Ainda nessa etapa de preparação, treinamentos devem ser realizados, por meio dos quais são simulados incidentes de segurança, a fim de pôr os procedimentos à prova. Deverá haver um mapeamento e a manutenção dos registros das operações de tratamento de dados pessoais, identificando-se, assim, o volume e a criticidade dos dados tratados, permitindo uma organização mais eficiente e também verificando os riscos jurídicos, em uma etapa chamada de "registro das operações".

Posteriormente, deverá ser instaurada a etapa de *resposta*, ou seja, o acionamento do plano firmado em um caso concreto de incidente de segurança. Para tanto, sugere-se a elaboração de um *checklist* de ações imediatas e de esquemas, para facilitar a ação e não ocorrerem descuidos. De modo imediato, assim que um incidente de segurança for detectado,

[4]Traduzido para Associação Internacional de Profissionais de Privacidade.
[5]BLUM, Opice. E-book: Melhores práticas de Governança e conformidade com a LGPD. Disponível em: https://opiceblumacademy.com.br/wp-content/uploads/2020/02/lgpd-governanca-melhores-praticas.pdf. Acesso em 10 set. 2020.

deve-se analisar qual a extensão do dano, isolando o perímetro, certificando-se que a área violada está segura, preservando-se, dessa forma, outros sistemas. Ademais, é necessário certificar-se sobre a segurança do ambiente e, desde já, implementar novas medidas para evitar outras ameaças.

Os integrantes do comitê, por sua vez, precisam estar cientes de suas responsabilidades, além de funcionarem de forma harmônica, para que não ocorram decisões isoladas ou inviáveis aos procedimentos da empresa. No entanto, caso o dano tenha sido em grande escala, torna-se importante obter uma consultoria técnica externa, apresentando também o dano para os órgãos reguladores, as autoridades policiais e os parceiros de negócios.

Além disso, é substancial realizar a documentação de todo o processo, exemplificando a causa, como o incidente foi descoberto, bem como todos os outros dados relacionados. Ainda, recomenda-se que sejam feitas entrevistas com as pessoas envolvidas, identificação de IPs, catalogação de informações por meio de *softwares*, e avaliação dos riscos para os titulares de dados, por um pequeno núcleo de gestores e, posteriormente, a informação às autoridades e aos órgãos reguladores das jurisdições afetadas.

Logo, após o incidente de segurança, inicia-se a terceira etapa intitulada *avaliação***,** em que se pretende adotar medidas para a remediação. O objetivo principal passa a ser a incorporação de experiências e o aprimoramento de procedimentos, sendo oportuna a elaboração de um relatório final do incidente e revisão dos procedimentos. Conforme orientação da Opice Blum:

> [...] A ideia é que esse relatório apresente, ao menos: (i) o que aconteceu de fato;(ii) quais providências de preservação das evidências foram adotadas; (iii) quem integrou o comitê de crise responsável pelos trabalhos; (iv) quais foram as funções desempenhadas pelos colaboradores envolvidos; (v) quais os parceiros envolvidos e por quais motivos; (vi) os questionamentos dos titulares, da imprensa e das autoridades recebidos; (vii) as respostas apresentadas; e (viii) quais as medidas de correção técnicas e de Governança adotadas. [...][6]

O relatório será extremamente importante como meio de comprovação da atuação da organização diante do incidente, principalmente na defesa de fiscalizações e ações judiciais. Aliás, sempre se sugere que novos relatórios sejam confeccionados diante da ocorrência de novos incidentes, possibilitando uma análise da evolução dos procedimentos. Somado a isso, recomenda-se que a empresa possua um dossiê com as comprovações de seus cuidados, que

[6]BLUM, Opice. E-book: Melhores práticas de Governança e conformidade com a LGPD. Disponível em: https://opiceblumacademy.com.br/wp-content/uploads/2020/02/lgpd-governanca-melhores-praticas.pdf. Acesso em 10 set. 2020.

contenha, por exemplo, contratos com consultorias especializadas, contratos com sistemas e operadores, termos de uso, políticas de privacidade, políticas internas, atas, registros, entre outros.

Por conseguinte, os planos de resposta aos incidentes podem ser atualizados, contratos revistos, procedimentos reavaliados, além de revisão das diretrizes de notificação, dos sistemas e ferramentas de segurança. Ademais, considera-se importante a contratação prévia de um "*cyber insurance*[7]", para resguardar a organização dos prejuízos de um incidente de segurança, no entanto, isso deve ser somado às práticas de boa governança dispostas na LGPD, nos arts. 50 e 51. Em síntese, a identificação das obrigações legais ou regulatórias é elemento fundamental de qualquer plano de resposta.

De modo geral, deverá ser observada a LGPD, em consonância com as eventuais regulações setoriais a que estiverem submetidas, tais como as ISO (International Organization for Standardization), que tem vínculo intrínseco com o tema deste artigo. A ISO 27001[8] contempla requisitos para estabelecer, manter e melhorar um Sistema de Gestão de Segurança de Informação (SGSI). O SGSI preserva a confidencialidade, integridade e disponibilidade de informação, por meio de uma gestão de riscos. Logo, vê-se que a ISO 27001 está fortemente ligada à existência de um plano de resposta, que visa a mitigar riscos e proteger os dados, fornecendo confiança para as partes interessadas.

De acordo com a ISO 27001, o sistema de gestão de segurança precisa ser planejado em conformidade às necessidades da organização. O primeiro passo é verificar qual é o contexto dessa organização, isto é, definir quais são as questões internas e externas que podem afetar os resultados pretendidos do SGSI. Diante disso, deverão ser determinadas: a) as partes interessadas que são relevantes para o sistema de gestão da segurança da informação; e b) os requisitos dessas partes interessadas relevantes para a segurança da informação. Além de que, devem ser definidos os limites de aplicabilidade do SGSI.

A Direção da organização deve agir com liderança e comprometimento, assegurando que a política de segurança de informação é compatível com a direção estratégica da organização, garantindo a integração do SGSI com os processos, assegurando recursos necessários, propiciando que o sistema alcance seus resultados e comunicando a importância

[7]Seguro cibernético.
[8]ISO 27001. Disponível em: https://www.academia.edu/36980100/ABNT_NBR_ISO_IEC_27001_Tecnologia_da_informa%C3%A7%C3%A3o_T%C3%A9cnicas_de_seguran%C3%A7a_Sistemas_de_gest%C3%A3o_de_seguran%C3%A7a_da_informa%C3%A7%C3%A3o_Requisitos. Acesso em 27 set. 2021.

dessa gestão eficaz. A política de segurança de informação precisa se basear em uma tríplice: 1) estar disponível documentalmente; 2) ser comunicada dentro da organização; 3) estar disponível para as partes interessadas.

O planejamento é etapa essencial no SGSI, visto que tem por objetivo prevenir ou reduzir os efeitos indesejados, como em uma hipótese de ocorrência de um incidente de segurança. Nesse viés, a organização precisa planejar ações que considerem esses riscos e oportunidades, integrando e implementando essas medidas, dentro dos processos do SGSI e avaliando a eficácia dessas ações.

Em linhas gerais, a organização deve definir e aplicar um processo de avaliação de riscos de segurança de informação, no qual estabeleça critérios de aceitação do risco e critérios para o desempenho das avaliações dos incidentes. Além disso, deve assegurar contínuas avaliações, comparando resultados, identificando os riscos, os níveis e os responsáveis por estes; reter informações documentadas sobre o processo de avaliação de risco de segurança da informação; definir e aplicar um processo de tratamento dos riscos, selecionando as opções e determinando todos os controles necessários para a implementação daquelas que forem escolhidas; elaborar uma declaração de aplicabilidade que contenha os controles necessários e a justificativa para inclusões e obter a aprovação dos responsáveis pelos riscos e a aceitação desses riscos residuais de segurança de informação.

Ademais, os objetivos da organização precisam estar claros, sendo eles consistentes com a política de segurança de informação, e ser mensuráveis, comunicados e atualizados. Em suma, deverão estar definidos no planejamento: o que será feito; quais recursos serão necessários; quem será responsável; quando estará concluído e como os resultados serão avaliados.

A comunicação é etapa essencial nesse processo e é imprescindível que seja estabelecido: o que será comunicado; quando comunicar; quem comunicar; e o processo em que a comunicação será realizada. Somado a isso, a organização deve avaliar o desempenho do SGSI, determinando o que precisa ser melhorado e quais os métodos para monitoramento, medição, análise e avaliação. Precisa também ser estabelecido quando o monitoramento será realizado e o que será medido.

Após a obtenção desses resultados, estes serão analisados pelos responsáveis, previamente estipulados. Usualmente, deverá haver a realização de uma auditoria interna, capaz de prover informações sobre o SGSI, sendo que o modo como essa auditoria se dará precisa ser previamente estipulada. A Direção da organização tem de analisar criticamente o

sistema de gestão de segurança de informação, para assegurar sua contínua adequação e eficácia, considerando resultados da avaliação dos riscos, não conformidade, ações corretivas, mudanças nas questões internas e externas e oportunidades para melhoria contínua.

O conhecimento da ISO 31000[9] também é muito importante para que se crie um plano de respostas. O gerenciamento de riscos externos e internos auxilia as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas. É etapa essencial da governança e liderança, contribuindo para a melhoria dos sistemas de gestão. Com base nisso, a gestão de riscos deve ser parte integrante de todas as atividades organizacionais; possuir uma abordagem estruturada e abrangente que contribua para resultados consistentes e comparáveis; ser personalizada conforme o contexto da organização; ser inclusiva, dinâmica, haja vista que os riscos podem transfigurar ou desaparecer com a própria evolução da organização e sempre em melhoria contínua.

A gestão de riscos carece de entender o contexto da organização, enraizado em fatos sociais, culturais, políticos, tecnológicos, de relacionamento, valores, estratégias, relações e compromissos contratuais. Logo, é de suma importância que aquele que tratar o dado, não faça uso de um "plano de gestão de crise" genérico, mas, sim, personalizado, conforme as necessidades reais.

É também vital que os órgãos de supervisão assegurem os papéis organizacionais e as responsabilidades. Além do mais, devem ser alocados recursos apropriados para essa gestão, com pessoas experientes, competentes, com ferramentas de organização, procedimentos documentados, SGSI e realização de constantes treinamentos.

Nesse viés, deve ser elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), um documento essencial para demonstrar como os dados pessoais são coletados, tratados, utilizados e compartilhados, além de demonstrar quais são as medidas utilizadas para mitigação de riscos. Aponta-se que, segundo o inciso XVII do art. 5º da LGPD, o RIPD é uma documentação que deve ser mantida pelo Controlador dos dados pessoais, sendo que o conteúdo do RIPD é indicado pelo parágrafo único do art. 38.

Nesse sentido, inicialmente verificar-se-á quem são os agentes de tratamento e o encarregado, as necessidades de elaboração do relatório e a descrição do tratamento. Em seguida, o reconhecimento de quem são as partes interessadas, as necessidades e a proporcionalidade do relatório e da gestão, a identificação/avaliação dos riscos, a adoção das

[9]ISO 31000. Disponível em: https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso em 27 nov. 2021.

medidas para tratar os riscos, a aprovação do relatório e, por fim, continuar mantendo a revisão deste procedimento. Certos casos específicos impõem a necessidade da elaboração de um relatório, tais como para o tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32); e a qualquer momento sob determinação da ANPD[10] (art. 38).

Além disso, a organização tem de estabelecer uma abordagem de comunicação e consulta, facilitando uma aplicação eficaz da gestão de riscos. A comunicação consiste no compartilhamento de informações com o público-alvo, e a consulta, o fornecimento de retorno pelos participantes, capaz de contribuir com as futuras decisões. Essa etapa envolve diferentes áreas de especialização para cada fase de gestão e assegura que diferentes pontos de vista sejam observados.

À vista disso, compete a organização implementar a estrutura de gestão de riscos, mediante o desenvolvimento de um plano apropriado, incluindo prazos e recursos; a identificação de onde, quando e como diferentes tipos de decisões são tomadas pela organização, e por quem; a modificação dos processos de tomada de decisão aplicáveis, onde necessário; e a garantia de que os arranjos da organização para gerenciar riscos sejam claramente compreendidos e praticados.

Posteriormente, deverão ser avaliados os procedimentos, mensurando periodicamente o desempenho dessa gestão de riscos, sempre adequando aos objetivos da organização. Caso seja necessário, precisará haver adaptações. Além disso, é imprescindível instituir um escopo, personalizando o processo de gestão de riscos, ou seja, convém definir em qual nível essa gestão se estabelece: se estratégica, operacional, de programa, projeto ou outras atividades, e planejar o que se inclui nesse plano, por exemplo as ferramentas e técnicas apropriadas para o processo de avaliação de riscos.

A organização também precisará identificar os riscos, especificamente, em comunhão com todos os colaboradores, considerando fontes tangíveis e intangíveis de risco; causas e eventos; vulnerabilidades; ameaças; mudanças no controle externo e interno; indicadores de risco emergentes; consequências e seus impactos; fatores temporais; vieses e crenças dos envolvidos, além de tudo o mais que puder ser verificado no caso concreto.

[10]Autoridade Nacional de Proteção de Dados.

A ISO IEC/27701,[11] no tópico 6 "*guidance related to iso* 27002", traz uma série de informações complementares ao tema tratado. No que se refere às políticas de segurança de informação, a ISO dispõe que organização deve produzir uma declaração sobre o apoio e o compromisso de alcançar a legislação de proteção de dados aplicável e com os termos contratuais acordados entre a organização e seus parceiros, seus subcontratados e seus terceiros aplicáveis, que devem alocar claramente as responsabilidades entre eles. Qualquer organização que processa dados, seja um controlador ou um processador, deve considerar a legislação e regulamentação de proteção de dados aplicável - no Brasil, a LGPD, durante o desenvolvimento e manutenção de políticas de segurança da informação.

Ainda, a organização deve designar um ponto de comunicação, para que o cliente possa entrar em contato acerca do processamento. Para tanto, observe-se que essa disposição da ISO IEC/27701 se encontra em consonância com os artigos 9º, inciso IV e 41, §1º da LGPD. Além disso, há necessidade de nomear uma ou mais pessoas responsáveis por desenvolvimento, implementação, manutenção, monitoramento e governança, em toda a organização e programa de privacidade, para garantir a conformidade com todas as leis e os regulamentos aplicáveis.

Outrossim, a ISO IEC/27701 dispõe expressamente sobre a necessidade de contato com as autoridades, contato com grupos de interesses especiais, se for o caso, e que a organização sempre preze pela segurança de informação na gestão de projetos. As medidas devem ser postas em prática, incluindo a conscientização de relatórios de incidentes, para garantir que a equipe esteja ciente das possíveis consequências para a organização, o membro da equipe e o principal controlador.

Como parte do processo geral de gerenciamento de incidentes de segurança da informação, a organização deve estabelecer responsabilidades e procedimentos para identificação e registro de violações. Adicionalmente, a organização deve estabelecer responsabilidades e procedimentos relacionados à notificação às partes requeridas e à divulgação às autoridades, levando em consideração a LGPD.

O relatório de eventos de segurança da informação deve: reportar pontos fracos de segurança da informação; conter avaliações e decisões sobre eventos de segurança da informação; descrever a resposta aos incidentes de segurança da informação; possuir registros tais como descrição do incidente, o período de tempo, as consequências do incidente, para

[11]ISO IEC/27701. Disponível em:<https://br1lib.org/book/11682064/7571fb?dsource=recommend. Acesso em 27.nov.2021.

quem o incidente foi relatado, as medidas tomadas para resolver o incidente e, evidentemente, qual o fato de o incidente ter resultado em indisponibilidade, perda, divulgação ou alteração de dados, para fins regulatórios e forenses.

Como parte das análises técnicas de conformidade com as políticas e os padrões de segurança, a organização deve incluir métodos de análise dessas ferramentas e desses componentes relacionados ao processamento de dados, com o monitoramento contínuo para verificar se apenas o processamento permitido está ocorrendo e com testes específicos de vulnerabilidade.

Como verificado, é indispensável a comunicação do controlador à autoridade nacional e ao titular, quanto à ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, tal como prevê o art. 48 da LGPD. Entretanto, vige uma dúvida quanto ao prazo que essa comunicação deve se dar, já que a LGPD apresentou apenas a necessidade de que esse prazo seja *razoável*, conforme se extrai do §1º. Nesse sentido, utiliza-se como parâmetro, a legislação europeia (General data protection regulation - GDPR), na qual estabelece prazo de 72 horas, embora não de forma decisiva, com o objetivo de que a investigação não seja muito extensa.

Ademais, caso o incidente de segurança apresente dano relevante aos titulares ou possa acarretar risco, a empresa controladora dos dados deve notificar a Autoridade Nacional de Proteção de Dados (ANPD). O controlador deve notificar o titular sobre o incidente de segurança, informando-lhe a possibilidade de danos ou riscos, bem como informações para mitigação dos prejuízos. Adicionalmente, os prestadores de serviço e parceiros envolvidos, diretamente, precisam ser informados, evitando-se vulnerabilidades em situação de reincidência.

Como penalidade, a LGPD prevê a publicização da infração, para obrigar a empresa a informar sobre o incidente, caso não tenha feito isso de forma espontânea e clara. Por isso, evidencia-se a importância das empresas assinarem contratos ou termos aditivos com a cláusula de que devem ser informados no caso de ações irregulares, para que não sejam responsabilizadas por omissão de terceiros. Pela mesma razão, a LGPD determina que, na atividade de tratamento de dados pessoais, na hipótese de causar dano patrimonial, moral, individual ou coletivo, existe a obrigação de repará-lo.

Caso o incidente envolva a prática de algum crime, deve-se buscar a instauração do inquérito policial, como no caso de *ransomware*, em que há o sequestro da base de dados e a

exigência de valor em contrapartida para liberação. Nesse caso, a organização apenas demonstrará que fez o que estava ao seu alcance.

4 SANÇÕES AO CONTROLADOR

O tema deste artigo tem estrita relação com as sanções administrativas previstas no art. 52 da LGPD, haja vista que estas somente serão aplicadas após procedimento administrativo, com oportunidade de ampla defesa, considerando as peculiaridades do caso concreto com previsão no §1º, das quais ressaltam-se a adoção de política de boas práticas governança, a pronta adoção de medidas corretivas e a adoção reiterada de mecanismos e procedimentos internos capazes de minimizar o dano. Assim, é de suma importância que o plano de respostas ou um sistema de gestão de riscos esteja vigente na organização, isto porque, caso a ANPD observe que o controlador previu possíveis riscos e tomou medidas para se prevenir, as sanções poderão ser reduzidas.

Desse modo, é perceptível que a LGPD sanciona gravemente aqueles que agem de má-fé e preza por considerar cada caso de maneira única, atendendo ao princípio da proporcionalidade. Em resumo, a gravidade, a boa-fé, o grau do dano e as intenções do controlador serão os pontos mais considerados para o cálculo da sanção. Acrescenta-se, ainda, que tais previsões não substituem a aplicação de sanções administrativas, civis ou penais, conforme prevê o §2º do art. 52 da LGPD.

5 BREVE COMPARATIVO À LEGISLAÇÃO E JURISPRUDÊNCIA EUROPEIA

Os principais pontos da LGPD refletem disposições do *General Data Protection Regulation*[12] (GDPR), em vigor na União Europeia (UE). Ressalta-se, entretanto, que a legislação brasileira não realizou uma cópia do modelo europeu, sendo que a LGPD se apresenta como a primeira legislação no Brasil responsável por tratar a proteção de dados com afinco.

Evidentemente, não se despreza a importância do Marco Civil da Internet (Lei n.º 12.965, 23 de abril de 2014), da Lei de Acesso a Informações Públicas (Lei n.º 12.527, de 18 de novembro de 2011) e de certas disposições do Código de Defesa do Consumidor (Lei n.º 8.078, de 11 de setembro de 1990), que, por sua vez, devem ser utilizadas, sistematicamente, com a LGPD. Além disso, é necessário ressaltar que a própria Constituição Federal de 1988, traz a temática com muitos fragmentos e de forma indireta, sendo imprescindível, considerar a

[12]Regulamento Geral sobre Privacidade de Dados.

presença do instituto do Habeas Data, disposto no Art. 5º, LXXII, que, no entanto, apenas respalda a pessoa privada.

No que diz respeito à notificação da violação dos danos, conforme mencionado, a LGPD não detalha prazo para que seja feita a notificação do vazamento, mas apenas informa que esta seja feita em prazo razoável. Em contrapartida, a GDPR prevê prazo de 72h. Ademais, a legislação brasileira determina que os indivíduos que tiveram seus dados violados devem ser notificados do incidente, o que não é requisito do regulamento europeu.

Quanto às sanções, para a GDPR, em caso de incidente de violação de dados, pode haver aplicação de multas que variam de 10 a 20 milhões de Euros ou de 2% a 4% do faturamento anual total do exercício financeiro anterior, o que for maior, sendo que a LGPD estabelece multas simples de até 2% da receita global do exercício anterior até 50 milhões de reais por violação.

Além dessas diferenças evidentes, é importante considerar que a GDPR é uma legislação que busca ser mais objetiva e direta em seus termos, ao passo que a LGPD tem cláusulas mais abertas e subjetivas, permitindo que haja interpretações diferentes, sendo imprescindível a consulta da jurisprudência e regulamentos pela ANPD (Autoridade Nacional de Proteção de Dados). A problemática maior está no fato de que a jurisprudência ainda não se vê consolidada, já que o instituto é recente.

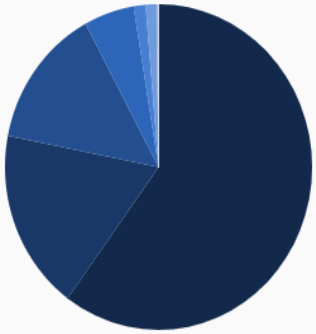
Com base em uma estatística extraída do "*CMS. Law GDPR Enforcement Tracker*[13]" em 23 de novembro de 2021, pode-se observar que a quarta maior causa de aplicação das multas pertence a "medidas técnicas e organizacionais insuficientes para garantir a segurança de informação, o que só reforça a importância da existência de um plano de respostas rápido e efetivo:

Figura 2[14]

Estatística: multas por tipo de violação

[13]Traduzido por "Rastreador de aplicação da GDPR". Disponível em: https://www.enforcementtracker.com/.
[14]GDPR Enforcement Tracker. Disponível em: https://www.enforcementtracker.com/. Acesso em 23 nov. 2021.

Pela soma total das multas:



Violação	Soma das multas
Não conformidade com os princípios gerais de processamento de dados	€ 783.975.044 (a 182 multas)
Cumprimento insuficiente de obrigações de informação	€ 234.950.395 (a 64 multas)
Base jurídica insuficiente para processamento de dados	€ 183.067.138 (a 301 multas)
Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação	€ 68.993.519 (a 181 multas)
Cumprimento insuficiente dos direitos dos titulares dos dados	€ 16.321.825 (a 79 multas)
Desconhecido	€ 14.700.500 (a 4 multas)
Cumprimento insuficiente das obrigações de notificação de violação de dados	€ 1.362.091 (a 21 multas)
Acordo de processamento de dados insuficiente	€ 993.580 (a 5 multas)
Envolvimento insuficiente do oficial de proteção de dados	€ 260.200 (a 10 multas)
Cooperação insuficiente com a autoridade supervisora	€ 216.929 (a 35 multas)

Ainda, considerando que a jurisprudência brasileira é escassa no assunto, é importante contemplar algumas nuances das decisões de alguns países pertencentes à União Europeia, as quais foram obtidas pelo "Rastreador da GDPR":

Na Espanha, por exemplo, ocorreu um caso de violação ao art. 37 da GDPR, em que se verificou a ausência de nomeação de um oficial de proteção de dados (Procedimento nº: PS/ 00251/2020[15]). O artigo violado estabelece que os responsáveis pelo tratamento devem designar um "delegado" de proteção de dados. Como fatores agravantes, tem-se que o número de interessados é alto, considerando-se que é responsável por realizar o processamento de dados pessoais em grande escala, sendo que identificadores pessoais básicos foram afetados. Para tanto, foi fixada multa de € 50.000 (cinquenta mil euros). Portanto, conclui-se que, assim como a LGPD prevê a necessidade da nomeação de um DPO, a GDPR também ressalta essa informação, sendo certo que a inexistência desse importante agente, em acréscimo com os outros fatos agravantes, resultou em uma sanção de valor vultoso.

Além disso, é oportuno apresentar outro exemplo de violação da proteção de dados pessoais, retirado de um incidente ocorrido na Polônia, por violação ao art.32 da GDPR, referente à insuficiência de medidas técnicas e organizacionais para garantir a segurança de informação (Decisão: ZSOŚS.421.25.2019[16]). No caso em apreço, foi constatada uma violação na proteção de dados pessoais pela Universidade de Ciências da Vida de Varsóvia,

[15]ESPANHA. AGENCIA ESPOÑOLA PROTECCIÓN DATOS. Procedimiento Nº: PS/00251/2020. RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR. Disponível em: https://www.aepd.es/es/documento/ps-00251-2020.pdf. Acesso em 8 out. 2020.

[16]POLÔNIA. DECISÃO ZSOŚS.421.25.2019. Escritório de Proteção de Dados Pessoais. Varsóvia, 21.ago.2020. Disponível em: https://www.uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019. Acesso em 8 out. 2020.

devido à livre circulação de dados, tendo sido aplicada multa à Universidade no valor de 50.000 PLN (cinquenta mil PLN).

Ademais, torna-se interessante analisar um episódio ocorrido na Irlanda[17], por violação ao Art. 5 e Art. 32 da GDPR, também referente a medidas técnicas organizacionais insuficientes para garantir a segurança de informação. No caso concreto, a comissão de Proteção de Dados (DPC) aplicou uma multa de € 65.000 ao Hospital Maternidade da Universidade de Cork (CUMH) depois que os dados pessoais de 78 de seus pacientes foram descartados em uma instalação de reciclagem pública em outro lugar no condado. Sabe-se que os dados em apreço possuíam informações de natureza sensível, sendo que, se acredita que a violação envolveu dados confidenciais de saúde de pacientes, incluindo históricos médicos e futuros programas planejados de atendimento. Independentemente da razão pela qual ocorreu esse descarte indevido de dados, o hospital, como controlador de dados, foi considerado responsável. É importante frisar que o hospital informou que todos os pacientes afetados pela violação foram notificados a respeito, e a Comissão de Proteção de Dados acabou por aplicar uma multa administrativa de € 65.000.

Por fim, tendo em vista os exemplos acima extraídos da União Europeia, e diante de todos os tópicos dissertados neste artigo, verifica-se que as sanções sempre serão agravadas diante da insuficiência de medidas capazes de garantir a segurança dos dados.

6 PROPOSIÇÕES CONCLUSIVAS

Conclui-se, portanto, que a Lei Geral de Proteção de Dados é de suma importância para a regulação da vida em sociedade, no século XXI, tendo em vista o número massivo e crescente de incidentes de segurança, inviolabilidade de dados e dos diversos impactos que podem ser causados ao titular e ao controlador. Além disso, percebeu-se que a atuação preventiva contribui para a diminuição da ocorrência de incidentes, bem como minimiza, significativamente, o impacto das sanções.

De plano, restou fornecido elementos concretos para a elaboração de um plano de respostas, no qual se compõe das fases de preparação, resposta e avaliação. Em síntese, verificou-se a importância da criação de um comitê de gestão de crise, bem como a importância dos responsáveis jurídicos e do DPO. Ademais, viu-se que é imprescindível a

[17]BRENNAN, CIANAN. O hospital de Cork multou € 65.000 após os dados pessoais dos pacientes serem encontrados em uma instalação pública de reciclagem. Disponível em: https://www.irishexaminer.com/news/arid-40075673.html. Acesso em 8 out. 2020.

implementação de treinamentos, simulações de incidentes, registro das operações e o aprimoramento dos procedimentos. Conjuntamente a esses pontos, reforçou-se a necessidade de complementação do tema com as ISO's (27001; 31000; IEC/27701), as quais fornecem bases ainda mais concretas.

Outrossim, constatou-se que a adoção das políticas de boa governança está intimamente ligada à redução das sanções, visto que estas são aplicadas de acordo com as peculiaridades do caso concreto. Ainda, restou observado alguns aspectos da GDPR e jurisprudências europeias, que reforçam, sobretudo, a importância do DPO e a adoção de medidas técnicas e organizacionais para prevenir e remediar danos, em que se encontra na quarta maior causa de aplicação de multas na União Europeia.

Finalmente, entende-se que a existência de um plano de respostas é tarefa primordial que não pode ser deixada em segundo plano, sendo certo que o presente artigo não esgota o tema, o qual está em constantes atualizações.

REFERÊNCIAS BIBLIOGRÁFICAS

APÓS SANÇÃO DO GOVERNO, LEI GERAL DE PROTEÇÃO DE DADOS COMEÇA A VALER. **Consultor jurídico**, 2020. Disponível em: https://www.conjur.com.br/2020-set-18/sancao-governo-lgpd-comeca-valer-nesta-sexta. Acesso em: 10 out. 2020.

AS FUNÇÕES DO DPO DE ACORDO COM A GDPR. **Assis e Mendes Advogados**, 2020. Disponível em: https://assisemendes.com.br/funcoes-dpo/. Acesso em: 19 nov.2021.

BANCO INTER CONFIRMA VAZAMENTO DE DADOS E CULPA PESSOA AUTORIZADA. **UOL**, 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/08/17/banco-inter-confirma-vazamento-de-dados-apos-ataque-hacker.htm. Acesso em: 15 set. 2020.

BLUM, Renato Opice. Plano de resposta a incidentes de segurança de dados pessoais: uma prevenção importante. **Opce blum**, 2020. Disponível em: https://noomis.febraban.org.br/especialista/renato-opice-blum/plano-de-resposta-a-incidentes-de-seguranca-de-dados-pessoais-uma-prevencao-importante. Acesso em: 26 ago. 2020.

BRASIL. **Lei Geral de Proteção de Dados (LGPD) nº 13.709**, de 14 de agosto de 2018. Diário Oficial, Brasília, 14 de agosto de 2018.

BRASIL. Apelação Cível 1006311-89.2020.8.26.0001**.** Tribunal de Justiça do Estado de São Paulo. Relatora Maria Lúcia Pizzotti. 30ª Câmara de Direito Privado. Foro Regional I - Santana, 8ª Vara Cível. **Tjsp,** 01/09/2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14982708&cdForo=0. Acesso em: 24 nov. 2021.

BRAZ, Marcilio. Considerações sobre a notificação de incidentes de segurança da informação no contexto da lei geral de proteção de dados. **Migalhas**, 2020. Disponível em: https://www.migalhas.com.br/depeso/295440/consideracoes-sobre-a-notificacao-de-incidente-de-seguranca-da-informacao-no-contexto-da-lei-geral-de-protecao-de-dados-e-alem#:~:text=Art.,ou%20dano%20relevante%20aos%20titulares.&text=VI%20%2D%20as%20medidas%20que%20foram,mitigar%20os%20efeitos%20do%20preju%C3%ADzo>. Acesso em: 22 set. 2020.

BRENNAN, Cianan. O hospital de Cork multou € 65.000 após os dados pessoais dos pacientes serem encontrados em uma instalação pública de reciclagem**. Irish examiner**, 2020. Disponível em: https://www.irishexaminer.com/news/arid-40075673.html. Acesso em: 8 out. 2020.

BRUNO, M.; VAINSOF, R. et al. Melhores práticas de Governança e conformidade com a LGPD. São Paulo: **Opce blum**. E-book: Disponível em: https://opiceblumacademy.com.br/wp-content/uploads/2020/02/lgpd-governanca-melhores-praticas.pdf. Acesso em: 10 set. 2020.

DECISÃO ZSOŚS.421.25.2019. **Escritório de Proteção de Dados Pessoais. Polônia, Varsóvia**, 21.ago.2020. Disponível em: https://www.uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019. Acesso em: 8 out.2020.

DPO: UM NOVO CARGO EXIGIDO PELA LGPD**. Delphos**. Disponível em: https://www.delphos.com.br/dpo-e-lgpd/. Acesso em: 19 nov. 2021.

EFEITOS E PROJEÇÕES SOBRE A VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O PAPEL DO ENCARREGADO DOS DADOS PESSOAIS**. Contecsi.** Disponível em: http://contecsi.submissao.com.br/arquivos/6598.pdf. Acesso em: 13 out. 2020.

É PRECISO APRENDER A LIDAR COM INCIDENTE DE DADOS. **SERPRO**. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/aprender-lidar-indicendes-dados-lgpd. Acesso em: 26 ago. 2020.

GDPR ENFORCEMENT TRACKER**. Enforcementtracker.** Disponível em: https://www.enforcementtracker.com/. Acesso em: 23 nov. 2021.

GUIA LGPD GOVERNANÇA DE DADOS**.** Brasília, DF: Presidência da República. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 28 set. 2020.

GESTÃO DE INCIDENTES DE SEGURANÇA DE INFORMAÇÃO. **IBLISS, Digital Security.** Disponível em: https://www.ibliss.digital/gestao-de-incidentes-de-seguranca-da-informacao/. Acesso em: 26 ago.2020.

HERRERO, Vagner Henrique. A lei de proteção de dados pessoais brasileira e os desafios a esta administração pública**. Repositório Institucional Universidade Federal de Minas Gerais**, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/32044/1/VagnerHenriqueHerrero.pdf. Acesso em: 10 set. 2020.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO. **Superintendência de Tecnologia da Informação e Comunicação - UFRJ.** Disponível em: https://www.security.ufrj.br/denuncie-um-incidente/. Acesso em: 26 ago. 2020.

ISO 27001**. Academia.edu**, 2021. Disponível em: https://www.academia.edu/36980100/ABNT_NBR_ISO_IEC_27001_Tecnologia_da_informa%C3%A7%C3%A3o_T%C3%A9cnicas_de_seguran%C3%A7a_Sistemas_de_gest%C3%A3o_de_seguran%C3%A7a_da_informa%C3%A7%C3%A3o_Requisitos. Acesso em: 27 nov.2021.

ISO 31000. **Gestravp**, 2013. Disponível em: https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso em: 27 nov. 2021.

ISO IEC/27701. **Br1lib**. Disponível em: https://br1lib.org/book/11682064/7571fb?dsource=recommend. Acesso em: 27 nov.2021.

KOHN, Stephanie. Maior ataque da história estremece a internet. **Olhar digital.** Disponível em: https://olhardigital.com.br/fique_seguro/noticia/maior-ataque-cibernetico-da-historia-estremece-a-internet/33511. Acesso em: 26 ago.2020.

LGPD X GDPR: QUAIS AS SEMELHANÇAS E DIFERENÇAS. **Alleasy.** Disponível em: https://www.alleasy.com.br/2020/03/09/lgpd-x-gdpr-semelhancas-diferencas/#:~:text=A%20LGPD%20n%C3%A3o%20possui%20prazos,notificados%20dentro%20de%2072%20horas. Acesso em: 28 set.2020.

MACHADO, José Mauro Decoussau *et al.* LGPD e GDPR: Uma análise comparativa entre as legislações. **Pinheiro Neto Advogados**, 2018. Disponível em: http://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes. Acesso em: 28 set. 2020.

MASSENO, Manuel David. A segurança dos dados na LGPD, brasileira: Uma perspectiva europeia, desde Portugal. **Revista do Direito**. Santa Cruz do Sul, v. 3, n. 50, p. 80-103, jan./abr. 2020. Disponível em: https://online.unisc.br/seer/index.php/direito/index.

NETO, Thaís. Aplicação de Sanções Administrativas na LGPD – Lei Geral de Proteção de Dados**. Instituto de Diretório Real**, 2020. Disponível em: https://direitoreal.com.br/artigos/aplicacao-de-sancoes-administrativas-na-lgpd-lei-geral-de-protecao-de-dados. Acesso em: 10 out.2020.

NUNES, Natália Martins. LGPD: Como as startups devem se preparar para casos de incidentes de segurança. **Jusbrasil**, 2020. Disponível em: https://ndmadvogados.jusbrasil.com.br/artigos/853810779/lgpd-como-as-startups-devem-se-preparar-para-casos-de-incidentes-de-seguranca?ref=feed. Acesso em: 10 set. 2020.

O QUE ESTÃO FAZENDO COM OS MEUS DADOS? A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS. Coordenação: Paloma Mendes Saldanha. Recife:

SerifaFina, 2019. **Udop.** Disponível em: https://apphotspot.com.br/wp-content/uploads/elementor/forms/OAB-PE-Oque-est%C3%A3o-fazendo-com-meus-dados-LGPD.pdf.

PALMA, Fernando. Incidentes de Segurança da Informação: conceitos, exemplos e cases. **Portalgsti**, 2014. Disponível em: https://www.portalgsti.com.br/2014/01/incidentes-de-seguranca-da-informacao-conceito-exemplos-e-cases.html. Acesso em: 26 ago.2020.

POR QUE DEVO REPORTAR INCIDENTES? **Pró-reitora de Gestão da Informação e Comunicação da UFPEL**. Disponível em: https://wp.ufpel.edu.br/seginfo/reportar-incidente-de-seguranca/. Acesso em: 22 set. 2020.

PROCEDIMIENTO Nº: PS/00251/2020 RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR. Espanha. **Agencia Espoñola Protección Datos**. Disponível em: https://www.aepd.es/es/documento/ps-00251-2020.pdf. Acesso em: 8 out.2020.

RODAS, Sérgio. Senado aprova vigência imediata da LGPD, mas prazo depende de sanção. **Consultor jurídico**. Disponível em: https://www.conjur.com.br/2020-ago-26/lei-geral-protecao-dados-vigencia-imediata-senado. Acesso em: 10 out. 2020.

SOMBRA, Thiago Luís; CASTELLANO, Ana Carolina. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva. **Revista do Advogado.** AASP, 2019. v. 39, n. 144, nov, p. 168-173.

TECNOLOGIA E DA INFORMAÇÃO/OAB-PE. **Udop**. Disponível em: https://www.udop.com.br/download/noticias/2020/03_03_20_arquivo_oab_pe.pdf#page=19. Acesso em: 13 out. 2020.

VOCÊ SABE O QUE É RESPOSTA A INCIDENTES DE SEGURANÇA? **Real protect**. Disponível em: https://realprotect.net/blog/voce-sabe-o-que-e-resposta-incidentes-de-seguranca/. Acesso em: 15 set. 2020.