2021 | MARÇO

CONTRIBUIÇÃO À ANPD

TOMADA DE SUBSÍDIOS Nº 2/2021 DA ANPD

INCIDENTES DE SEGURANÇA, PROCESSO DE COMUNICAÇÃO E ANÁLISE DE RISCO

LAPIN

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

Realização:

Laboratório de Políticas Públicas e Internet - LAPIN

Autoria:

Cynthia Picolo Gonzaga de Azevedo

Gustavo Henrique Luz Silva

Isabela Maria Rosal Santos

Revisão:

Amanda Espiñeira

José Renato Laranjeira de Pereira

Imagem de Capa:

anyaberkut, Getty Images

LAPIN

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

lapin.org.br

@lapin.br

/lapinbr

/lapinbr

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2/2021

NOME DA INSTITUIÇÃO: Laboratório de Políticas Públicas e Internet - LAPIN[1]

O Laboratório de Políticas Públicas e Internet (LAPIN) é um think tank de composição multidisciplinar com sede na capital federal brasileira. Seu objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade. Para maiores informações sobre nossa atuação, visite nosso site: <https://lapin.org.br/>.

CNPJ: 36.965.428/0001-16

[1] Essa contribuição foi desenvolvida pelos seguintes membros do LAPIN: Amanda Espiñeira (e-mail: amanda@lapin.org.br), Cynthia Picolo Gonzaga de Azevedo (e-mail: cynthia.picolo@lapin.org.br), Gustavo Henrique Luz Silva (e-mail: gustavo.luz@lapin.org.br), Isabela Maria Rosal Santos (e-mail: isabela@lapin.org.br) e José Renato Laranjeira de Pereira (e-mail: joserenato@lapin.org.br).

CONTRIBUIÇÕES RECEBIDAS	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO - LAPIN**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Um incidente de segurança pode acarretar risco ou dano relevante ao titular quando há um aumento de risco de roubo de identidade, fraude ou danos à reputação[2], ainda que esses não se concretizem a ponto de configurar danos.** Isso está de acordo com a ideia que direciona, por exemplo, o GDPR[3], no sentido de que o risco relevante sobre o tema de incidente de segurança é o risco adverso para o titular[4]. Um elemento de extrema relevância na avaliação do risco relacionado a um incidente de segurança é a consideração das possíveis consequências negativas para os indivíduos. Já o dano é a concretização dessas

[2] SOLOVE, D; CITRON, D. K. **Risk and Anxiety: A theory of data-breach harms**. Texas Law Review 737. 2018. Disponível no SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638>. Acesso em 22 mar. 2021.

[3] O Considerando 75 do GDPR traz o conceito de risco: "O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza econômica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controle sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspectos de natureza pessoal, em particular análises ou previsões de aspectos que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou interesses pessoais, à confiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados".

[4] CIPL. **Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR**. 2016. Disponível em: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>. Acesso em 23 mar. 2021.

	possíveis consequências. Tais conceitos devem ser interpretados de maneira extensiva, abrangendo efeitos morais, patrimoniais, individuais e coletivos, conforme o art. 42 da LGPD. A interpretação dos efeitos negativos ao titular deve ser feita da maneira mais abrangente possível, uma vez que a compensação por danos na esfera informacional de um indivíduo é de difícil realização, pois um vazamento de dados muitas vezes é irreversível em sua completude. Por essa razão, o regime de proteção de dados brasileiro se utiliza de instrumentos preventivos, a fim de evitar possíveis riscos ou danos para não ser necessário alcançar a fase indenizatória[5]. A interpretação extensiva dos resultados de um incidente também está prevista no *caput* do art. 42 da LGPD, que prevê que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados, é obrigado a repará-lo". A ideia de consequências negativas para o titular para fins de avaliação de riscos e gravidade também é adotada em outros momentos na LGPD e deve ser o foco central na avaliação dos riscos, considerando a probabilidade de concretização do risco e sua gravidade. Isso consta inclusive no teste de balanceamento do legítimo interesse, previsto no art. 7º, IX da LGPD: quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[5] A prevenção é um princípio básico para o tratamento de dados, previsto no art. 6º, inciso VIII, da LGPD. Nesse mesmo sentido, no GDPR: Article 29 Working Party. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> p. 30-33; p. 37. Acesso em 23 mar. 2021.

	Outro fator que gera presunção de risco ou dano relevante ao titular é a **categoria** dos dados pessoais afetados pelo incidente. Se **dados sensíveis** ou **dados de crianças e adolescentes** forem afetados, já deve existir uma presunção de risco ou dano relevante ao titular. Nesse sentido, também deve haver a consideração de **grupos minoritários** ou **grupos em situação de vulnerabilidade** (como indivíduos com condenações penais ou até refugiados). Se os dados afetados contarem com informações sobre esses grupos, maior a relevância do risco ou dano. Além disso, para mensuração do risco ao titular, também deve ser considerada a **probabilidade de o dano se concretizar**. Quanto mais altas as chances de concretização de dano, mais grave ou relevante deve ser considerado o incidente de segurança. Nesse sentido, também devem ser considerados possíveis danos morais relevantes aqueles relacionados ao estresse e ao medo, mas há gravidade evidente quando houver risco de prejuízos financeiros ou à integridade física, por exemplo. Também se mostra necessária a avaliação do **volume de dados** afetados. De maneira geral, quanto mais dados são afetados, maior a relevância desse incidente. Cabe ressaltar que um alto volume de um único tipo de dado pode vir a ser menos grave do que um incidente que afete vários dados sobre um determinado indivíduo, possibilitando a sua completa identificação, incluindo a revelação de seu perfil comportamental ou inferências feitas por determinado algoritmo. Por isso, é essencial a **avaliação do contexto** em que se encontram os dados impactados, para entender o que esse volume significa para os titulares de dados afetados. Esses pontos estão relacionados com a metodologia para gestão de risco (2012)[6] e a metodologia para a formulação de relatório de impacto de dados pessoais (2018 — ver questão sobre metodologias)[7] apresentadas pela

[6] Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf>. Acesso em 22 mar. 2021.
[7] Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf>. Acesso em 22 mar. 2021.

autoridade francesa de proteção de dados, a *Commission Nationale de l'Informatique et des Libertés* – CNIL, e sintetizadas através das seguintes imagens (em tradução livre):

[Figura 1 - metodologia de gestão de risco]

[Figura 2 - relatório de impacto à proteção de dados pessoais]

Esses dois ciclos demonstram a importância da consideração dos riscos na gestão da proteção de dados. A avaliação do contexto e das consequências, possíveis ou concretas, nessa gestão de riscos e impactos é crucial para garantir a observância dos princípios e direitos do titular. Além disso, devem ser considerados os eventos esperados e as possíveis ameaças. Pretende-se endereçar todos esses pontos ao longo da tomada. A experiência

	francesa, inclusive, demonstra a importância da formulação de materiais didáticos sobre esse tema por parte da ANPD.[8] A prática australiana nos mostra o mesmo; a legislação australiana também prevê a necessidade de comunicação se um incidente de segurança tiver probabilidade de causar dano relevante e, em seu site, traz **exemplos de situações que configuram dano relevante**[9]: roubo de identidade que possa afetar finanças e relatório de crédito; perda financeira por fraude; um provável risco de dano físico, como por exemplo, por um ex-parceiro abusivo; danos psicológicos graves; e danos sérios à reputação de um indivíduo. Em síntese e diante do exposto, o LAPIN acredita que os **seguintes critérios devem ser utilizados para avaliar o risco ou dano como relevante**: ● A **categoria dos dados afetados** pelo incidente (dados sensíveis e dados de crianças e adolescentes já configurariam risco ou dano relevante — é necessário considerar o contexto dos dados para fazer essa análise) em conjunto com o **volume de dados** afetados; ● Se **terceiros não autorizados têm acesso aos dados afetados** (o fato desses terceiros serem desconhecidos agravaria o resultado da avaliação — p. ex., a divulgação dos dados afetados em listas ou a venda dos dados já traria a relevância do risco ou dano);

[8] Nesse sentido, o relatório do *Global Privacy Enforcement Network* (GPEN) demonstra que organizações sem políticas internas sobre incidentes de segurança utilizavam os guias das autoridades quando necessário. Disponível em: <https://privacy.org.nz/publications/statements-media-releases/gpen-sweep-finds-significant-awareness-of-managing-data-breaches-concerns-regarding-low-engagement>. Acesso em 23 mar. 2021.

[9] Disponível em: <https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach/>. Acesso em 22 mar. 2021.

	• A **probabilidade de concretização do dano** (essa avaliação deve considerar as possíveis consequências do incidente, sem menosprezar danos de natureza moral, como estresse e medo); • A **gravidade** dos possíveis danos; • **Características específicas** sobre os titulares afetados (se pertencem a algum grupo minoritário ou em situação de vulnerabilidade, se existe algum perigo relacionado à violação daqueles dados etc.); • O contexto da **origem** do incidente (considerando, inclusive, se a entidade já adotava um programa de *compliance* à proteção de dados e se a ameaça foi interna ou externa).
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto etc.)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	É bem-vinda a adoção de gradação das categorias de risco e de dano. Essa categorização possibilitará a compreensão sobre a urgência de comunicação à ANPD e também sobre a necessidade de comunicação do titular. A experiência internacional também utiliza dessa gradação para avaliar os riscos de incidentes de segurança, como a apresentada pela autoridade francesa[10], demonstrada pela imagem a seguir, em tradução livre:

[10] Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf>. p. 18. Acesso em 22 mar. 2021.

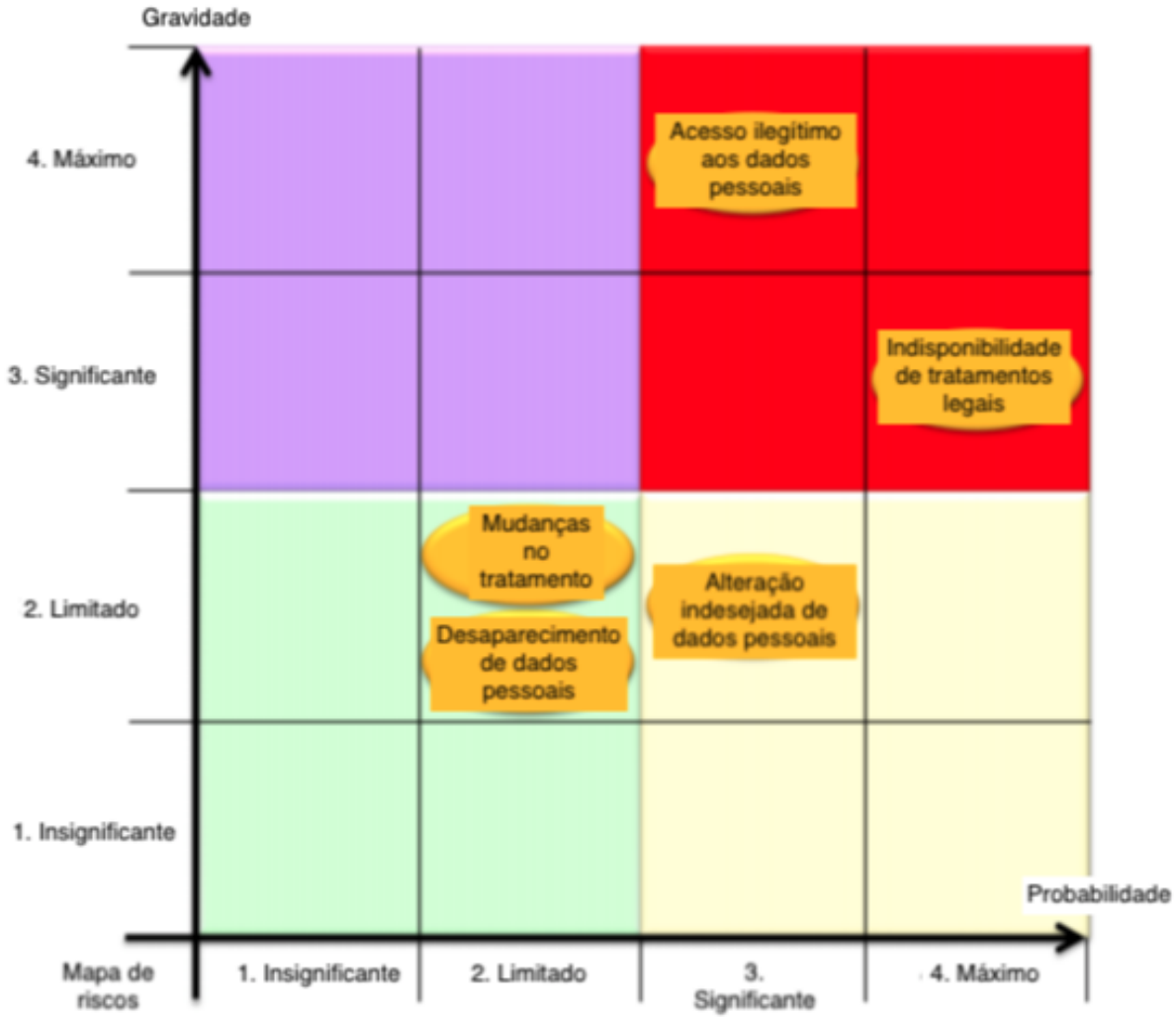

Figure 4 – Risk map

[Figura 3 - gráfico sobre gradação de riscos, a partir de avaliação de gravidade dos riscos e probabilidade de concretização dos riscos]

O gráfico apresentado demonstra a relação entre gravidade e probabilidade de concretização de um risco para classificar o risco em algumas das subdivisões – risco máximo, significante, limitado ou insignificante. Ou seja, riscos baixos têm probabilidade de concretização e gravidade das possíveis consequências também insignificantes. Assim, resta clara a relação direta da classificação do risco com a questão da gravidade do incidente de segurança, uma vez que, quanto mais grave o incidente, maior o risco relacionado a esse fato.

O GDPR também traz previsões sobre um "elevado risco", demonstrando certa subdivisão do risco, inclusive enumerando tratamentos de alto risco[11] em seu artigo 35(3):

a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou a afetem significativa de forma similar;

b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o art. 9 (1), ou de dados pessoais relacionados a condenações penais e infrações a que se refere o art. 10; ou

c) Controle sistemático de zonas acessíveis ao público em grande escala.

Com isso em mente, **propõe-se a seguinte distinção de níveis de risco**:

- **Irrelevante** → não existem possíveis consequências negativas para o titular (p. ex.: os dados afetados já eram públicos e não é possível nenhuma inferência adicional a partir do contexto em que os dados se inserem);

[11] CIPL. **Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR**. 2016. Disponível em: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>. Acesso em 23 mar. 2021.

- **Baixo** → as possíveis consequências negativas para o titular têm pouco impacto e ainda são reversíveis (p. ex.: basta o recadastramento do titular ou atualização de seus dados para reverter o dano gerado);
- **Médio** → as possíveis consequências negativas para o titular podem gerar impactos maiores, mas ainda reversíveis (p. ex.: atualização do cadastro em vários meios ou necessidade de pedido de exclusão de bancos de dados em que as informações foram adicionadas);
- **Alto** → as consequências negativas são mais severas e sua reversão depende do gasto de recursos de tempo e financeiros (p. ex.: intimações judiciais ou extrajudiciais, mudanças em scores de crédito);
- **Alarmante** → as possíveis consequências são significantes e não são passíveis de reversão (p. ex.: dificuldades financeiras, dificuldades em conseguir ou manter uma relação de trabalho).

Ainda é importante verificar tanto o **critério quantitativo** (relacionado ao número de titulares afetados e a quantidade de dados afetados em relação a cada indivíduo) quanto o **critério qualitativo** (análise contextual dos titulares e dados afetados, além da consideração de características específicas do controlador e de como se deu o incidente). Esses critérios, que merecem definição detalhada pela ANPD, também vão possibilitar que somente incidentes relevantes sejam comunicados à ANPD, evitando uma enxurrada de comunicações, o que impediria a análise efetiva por parte da Autoridade. Essa ideia ainda está completamente de acordo com o art. 52, §7º, da LGPD, que possibilita a conciliação direta do controlador com o titular afetado em caso de incidentes individuais.

A classificação do risco é aplicável à categorização do dano, uma vez que o dano é a concretização do risco, excluído o dano irrelevante, uma vez que é impossível existir dano sem consequências negativas ao titular. **Então, a subdivisão de dano será equivalente a dano baixo, médio, alto ou alarmante,** a partir da avaliação de quais riscos efetivamente se concretizaram. É importante ressaltar, no entanto, que, independentemente de sua classificação,

	uma vez comprovado dano, de qualquer natureza, ao titular, já há relevância nos efeitos do incidente de segurança, considerando que o dano é a concretização do risco. Dessa forma, o risco irrelevante não deve ser considerado como passível de ser comunicado à ANPD ou ao titular; o risco baixo, por sua vez, só poderá ser considerado relevante se houver fatores adicionais que agravem a situação (p. ex.: a volumetria dos dados afetados); já os riscos médio, alto e alarmante devem ser considerados todos como relevantes, gerando obrigação de comunicação à ANPD. Além disso, pelo menos os incidentes que gerem riscos alto ou alarmante devem ser comunicados também diretamente aos titulares. Por fim, nas situações em que houver dano, ou seja, risco concretizado, deverá haver, ao menos, comunicação à ANPD. Além disso, deve-se comunicar ao titular informações sobre o incidente no caso de dano médio, alto ou alarmante.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco é equivalente às consequências negativas hipotéticas, possíveis, oriundas do incidente de segurança. A avaliação dos riscos deve ser feita de forma abrangente a fim de se considerar riscos que podem gerar danos morais, materiais, individuais ou coletivos. Já o dano consiste na concretização do risco. É o momento em que a consequência hipotética se torna real. Por isso, o risco gera dever de prevenção, transparência e prestação de contas. Já o dano, além desses, também gera o dever de indenização, conforme dispõe o art. 42 da LGPD. Portanto, os conceitos se relacionam, uma vez que tratam de momentos diferentes de um mesmo efeito negativo ao titular: o risco em um momento anterior, a partir de avaliação hipotética; e o dano, algo posterior, que é a efetivação da probabilidade. Um exemplo dessa diferenciação seria um incidente envolvendo o funcionário de um escritório de advocacia que perdeu uma mochila que continha seu laptop e arquivos de papel com informações de clientes. O funcionário

	disse a seu gerente que acreditava que o laptop estava criptografado e que os dados nos arquivos em papel haviam sido marcados com caneta preta para evitar que pudessem ser lidos. O gerente, então, relatou o incidente ao departamento de TI, que limpou remotamente o laptop. Pelo fato de o risco, nessa situação, ser considerado baixo, já que a proteção contra invasão de seu computador era forte e os arquivos em papel não poderiam ser lidos, o controlador muito provavelmente não necessitaria informar o incidente à Autoridade. Ocorre que, posteriormente, o departamento de TI descobriu que o funcionário estava trabalhando em um laptop antigo, que não era criptografado nem protegido por senha. O funcionário também confirmou que os arquivos em papel eram de um julgamento criminal que se aproximava e que os dados pessoais, relacionados a condenações criminais e informações de saúde, talvez ainda pudessem ser lidos, porque descobriu que uma cópia dos documentos, dessa vez sem deleções, também estava na mochila perdida. Com isso, houve um aumento expressivo de risco de dano nessa situação, bem como uma potencial presunção de dano, já que muito provavelmente a pessoa que localizou o computador e os arquivos físicos pôde visualizá-los e ter amplo acesso aos dados pessoais ali presentes[12].
O que deve ser considerado na avaliação dos riscos do incidente?	Devem ser consideradas as características do incidente, do contexto do tratamento dos dados, dos titulares afetados e da entidade controladora. Além disso, é necessário considerar a gravidade das possíveis consequências e a possibilidade de concretização dessas. Esses pontos permitem uma avaliação completa e extensa dos riscos ao titular e à sociedade, ou seja, as possíveis consequências negativas oriundas do incidente.

[12] Disponível em: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/>. Acesso em 24 mar 2021.

	Esse direcionamento está de acordo com o guia sobre incidentes de segurança elaborado pelo Article 29 Working Party (ou WP29), órgão responsável por lançar guias sobre a aplicação da proteção de dados na Europa antes da entrada em vigor do GDPR, que recomenda a consideração dos seguintes pontos na **análise de risco**[13]: 1. o tipo de incidente; 2. a natureza, a sensibilidade e o volume de dados afetados - considerando as características especiais dos indivíduos afetados; 3. o número de indivíduos afetados. 4. a facilidade de identificação de indivíduos; 5. a gravidade das consequências para os indivíduos; e 6. as características do controlador. Já a *Agencia Española de Protección de Datos*[14] defende que os seguintes fatores devem ser considerados na **análise de risco** de um incidente: o tipo de ameaça; contexto ou origem da ameaça — interna ou externa; categoria de segurança dos sistemas utilizados; dados afetados; perfis dos titulares afetados; número e classificação dos sistemas afetados; impacto do incidente na organização; exigências legais e regulatórias; vetor ou método do ataque. Trazemos essas experiências internacionais por considerarmos que tais critérios, por garantirem uma abordagem objetiva para a avaliação de riscos do incidente, também podem ser adotados pela ANPD.

[13] Article 29 Working Party, **Guidelines on Personal data breach notification under Regulation 2016/679.** Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> p. 24-26. Acesso em 16 mar. 2021.

[14] Agencia Española de Protección de Datos. **Guide on personal data breach management and notification.** Disponível em: <https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf>. Acesso em 16 mar. 2021.

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As primeiras orientações trazidas pela ANPD através da disponibilização de formulário para comunicação de incidente de segurança[15] são oportunas, inclusive porque detalham melhor as informações necessárias a serem comunicadas. Destaca-se a necessidade de identificação do encarregado ou equivalente como ponto de contato com a ANPD, as circunstâncias em que ocorreu a violação de segurança de dados pessoais, possíveis problemas de natureza transfronteiriça, além da quantidade de dados e de titulares afetados. Esse último ponto é de suma importância para compreensão dos possíveis riscos oriundos do incidente, porque pode ser mais arriscado o vazamento de várias informações sobre um indivíduo do que o de um só tipo de informação menos sensível sobre diversos titulares — tal avaliação dependerá do caso concreto e por isso é importante a discriminação dessas informações na comunicação. Sendo assim, é fundamental a descrição da categoria dos dados afetados e o contexto que os dados estavam inseridos. Por exemplo: uma informação como o nome de um titular não parece ser tão prejudicial, mas se considerado o contexto do incidente, como um vazamento de pessoas diagnosticadas com uma doença, passa a ser uma informação sensível. Para melhor compreensão do período entre a data e hora da detecção e a comunicação, também pode ser requisitada como informação adicional maior detalhamento sobre o processo de comunicação interna de incidentes da organização. Essa informação pode justificar a demora em notificar a ANPD, porque o incidente pode ter ocorrido em uma área de baixo risco, por exemplo, e esse detalhamento de processos internos pode ajudar na compreensão de como se deu o incidente e sobre o nível de *compliance* da organização que sofreu o incidente. O LAPIN também apoia a ideia de possibilitar uma comunicação preliminar e outra completa, como já proposto pela ANPD. A comunicação preliminar deve contar com algumas informações mínimas: natureza dos dados pessoais afetados; os riscos relacionados ao incidente; uma estimativa do prazo para envio da comunicação

[15] ANPD, Comunicação de Incidentes de Segurança. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>. Acesso em 22 mar. 2021.

	completa; e informações sobre os titulares envolvidos, como a quantidade de pessoas, as regiões geográficas afetadas, o perfil geral dos afetados com informações que permitam um titular compreender as chances de ele estar envolvido nesse determinado incidente - principalmente nos casos em que não há comunicação individual e direta. A possibilidade de uma comunicação parcial tem por ponto positivo permitir que o controlador forneça informações sobre o incidente posteriormente à comunicação imediata, já que, dependendo do tipo de incidente, a investigação e avaliação internas serão mais complexas, e nem sempre informações relevantes estarão disponíveis rapidamente e com um grau de certeza mais elevado. Além disso, podem ser enviadas outras comunicações parciais até o envio da comunicação completa definitiva. Já a comunicação completa deve conter as demais informações já detalhadas no formulário preliminar da ANPD e, a depender do caso, o processo de comunicação interna de incidentes. Deve-se questionar em quanto tempo uma comunicação parcial deva ser completada, tendo em vista que um procedimento muito demorado aumenta as chances de concretizar riscos ou de agravar o dano, impactando diretamente nos direitos dos titulares (ver tópico seguinte). Ressalta-se que, da perspectiva do titular, o objetivo da comunicação é justamente limitar os danos. De qualquer forma, para possibilitar que as comunicações sejam feitas de modo adequado, a ANPD deve fornecer maiores orientações sobre o que será enquadrado como incidente de segurança — inclusive se será adotada a definição da Administração Pública federal trazida pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, por exemplo. Isso é fundamental, já que a possível definição que pode ser retirada do art. 46 da LGPD é muito ampla e pode afastar comunicações relevantes ou fazer com que sejam notificados incidentes que não apresentam riscos ao

	titular, aumentando de forma expressiva o número de notificações e impossibilitando uma verificação adequada por parte da ANPD. Considerando que as informações constantes da comunicação devem respaldar a averiguação do incidente de segurança pela ANPD, é essencial que elas proporcionem o máximo de clareza e entendimento sobre o fato. Essa compreensão não somente guiará a ANPD quando da análise da gravidade do incidente, mas também permitirá maior celeridade na solução dos problemas, na implementação de estratégias para mitigação de riscos e na eventual responsabilização, lembrando que em diversas circunstâncias a ANPD agirá em conjunto com outros atores. Em síntese, para além daquelas já solicitadas no formulário disponibilizado pela ANPD, as seguintes informações complementares devem constar na comunicação de incidentes de segurança à Autoridade: ● Indicação de **prazo estimado** para completar a comunicação parcial; ● Uma referência clara para que se informe o **período aproximado de ocorrência da violação** de dados no tópico "Quando o incidente ocorreu?" nos casos em que não se possa delimitar com exatidão a data/período do incidente; ● Detalhes de **quem potencialmente teve acesso aos dados pessoais**, quando possível. Essa informação ajudaria na avaliação de gravidade; o risco pode ser maior ou menor considerando o agente que possivelmente acessou os dados; ● Detalhes sobre o **processo de comunicação interna** de incidentes da organização;

	• Informações de quais **técnicas para segurança** dos dados haviam sido utilizadas, como anonimização, pseudonimização ou criptografia; • Detalhes sobre a **avaliação** feita para determinação da existência de risco ou dano relevante aos titulares, especialmente nos casos em que, a princípio, não for possível identificar com clareza o tipo de violação de dados; • Mais informações em relação ao **conteúdo da comunicação aos titulares**, já que é imprescindível que o controlador adote postura preventiva e forneça meios para que os titulares afetados possam, de fato, adotar medidas de mitigação de risco, incluindo através de canais disponibilizados pelo controlador. A depender do que foi ou pretende ser informado aos titulares, a ANPD poderá recomendar ações. Ademais, estas informações ajudarão a embasar a decisão da ANPD sobre a adoção de medidas complementares para a salvaguarda dos direitos dos titulares previstas no art. 48, §2º, da LGPD; • Informações sobre **organizações e/ou outras autoridades a serem notificadas**, especialmente considerando o cenário em que a ANPD atuará em conjunto com outras entidades.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O primeiro ponto a ser discutido é a partir de quando começa a correr o prazo para o controlador comunicar a ANPD. No âmbito do GDPR, o controlador deve comunicar o incidente à autoridade em até 72 horas a partir do *conhecimento do fato*, e muito se discutiu sobre quando seria este momento. De acordo com o Article 29 Working Party, o controlador deve ser considerado 'ciente' do fato quando existe um **grau razoável de certeza** que ocorreu um incidente de segurança que comprometeu dados pessoais[16].

[16] Article 29 Working Party, **Guidelines on Personal data breach notification under Regulation 2016/679.** Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> p. 11. Acesso em 16 mar. 2021.

	O WP29 discorre, ainda, que o momento exato em que o controlador pode ser considerado ciente de uma violação de dados dependerá das circunstâncias, que poderão ser mais ou menos claras. No entanto, o WP29 orienta que **a ênfase deve ser na ação imediata para investigar o incidente para determinar se os dados pessoais foram realmente comprometidos** e, em caso afirmativo, tomar medidas corretivas e comunicar, se necessário.[17] Na impossibilidade de determinar com precisão o momento em que o controlador toma ciência de um incidente que deva ser comunicado à ANPD, é importante que especialmente os princípios da boa-fé (art. 6º, *caput*), da segurança (art. 6º, VII), da prevenção (art. 6º, VIII) e da responsabilização e prestação de contas (art. 6º, X) sejam rigidamente observados. Além disso, deve-se ponderar que os agentes de tratamento são obrigados a utilizar sistemas que atendam aos requisitos de segurança (art. 49), o que pressupõe certa estruturação para lidar com incidentes de segurança de dados pessoais. Por fim, e seguindo a linha do WP29, um "grau razoável de certeza" que ocorreu um incidente de segurança de dados pessoais pode ser considerado como o ponto de partida no processo de comunicação. De qualquer forma, havendo dúvidas sobre comunicar ou não a ANPD, é importante que seja adotada uma abordagem baseada no risco e que o controlador elabore, pelo menos, uma comunicação parcial, reservando-se o direito de fornecer informações mais precisas em um segundo momento[18]. Em relação ao prazo razoável para comunicar a ANPD sobre o incidente de segurança, o LAPIN sugere o prazo de 72 horas a partir do conhecimento do incidente — pelo menos para o envio da comunicação parcial. O prazo sugerido segue a experiência internacional sobre o tema, como as seguintes:

[17] ibid.

[18] No entanto, não podemos deixar de pontuar que a comunicação à ANPD sem um grau de certeza razoável pode levar ao *notification fatigue* – conceito bastante utilizado na Europa para indicar a fadiga causada a controladores, autoridades de proteção de dados e titulares de dados quando não há critérios bem definidos para comunicações de incidentes de segurança, levando a um alto volume de incidentes comunicados.

	• União Europeia → comunicação deve ocorrer imediatamente e, se possível, em até 72 horas após o conhecimento da violação[19]; • Uruguai → em até 72 horas após o conhecimento da violação[20]; • Argentina → a Lei de Proteção de Dados Pessoais nº 25.326, em vigor na Argentina desde 2000, não prevê a obrigação de notificar incidentes de segurança aos titulares de dados pessoais ou à autoridade de controle. Porém, um projeto de lei em discussão prevê que a comunicação do incidente seja feita imediatamente ou, no mais tardar, em até 72 horas do conhecimento do fato[21]; • Singapura → imediatamente ou, no mais tardar, em até 72 horas da determinação que o incidente é passível de notificação[22]. Além disso, é importante a definição de um prazo para a apresentação da comunicação completa e, nesse caso, sugere-se o prazo adicional de 10 dias (equivalente ao prazo da Portaria do Ministério da Justiça e Segurança Pública nº 618/2019[23], que disciplina o *recall*), contados a partir do protocolo da comunicação parcial. Este prazo é importante pois, dependendo do tipo de incidente, a investigação e avaliação internas serão mais complexas, e nem

[19] Regulamento Geral sobre Proteção de Dados, art. 33(1). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em 22 mar. 2021.
[20] Decreto n° 64/020, art. 4°. Disponível em: <www.impo.com.uy/bases/decretos/64-2020>. Acesso em 22 mar. 2021.
[21] Diputados Argentina, Dirección Secretaría – Tramite Parlamentario n. 171, Proyecto de Ley de Protección de Los Datos Personales, art. 20. Disponível em: <https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2020/PDF2020/TP2020/6234-D-2020.pdf>. Acesso em 22 mar. 2021.
[22] Personal Data Protection Commission. **Advisory Guidelines on Key Concepts in the Personal Data Protection Act**, p. 141. Disponível em: <www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>. Acesso em 22 mar. 2021.
[23] Art. 2º, §10 da Portaria: A investigação do fornecedor de produtos e serviços, para determinar a comunicação de que trata o art. 3º desta Portaria não deve ultrapassar o prazo de dez dias úteis, a menos que o fornecedor demonstre circunstanciadamente que a extensão do prazo é necessária para a conclusão dos trabalhos.

	sempre informações relevantes estarão disponíveis rapidamente e com um grau de certeza mais elevado para constarem na comunicação imediata. Mas, de qualquer forma, a ANPD deve esclarecer perfeitamente quais casos podem contar com essas duas fases de comunicação — parcial e completa —, de forma a não incentivar a utilização da comunicação parcial como regra para todos os casos de incidente. Além disso, o prazo deve ser passível de flexibilização, a depender das justificativas apresentadas pela organização na comunicação. Outra solução possível apoiada pelo LAPIN é a definição de **prazos diferenciados,** talvez mais flexíveis, para determinados controladores. Alguns dos critérios que podem ser utilizados são: (i) a composição ou tamanho do controlador (relação com o tratamento diferenciado para PMEs) e (ii) o tratamento de dados ser atividade fundamental à organização. De qualquer forma, é muito importante a **adoção de uma forma de comunicação online,** que funcione ininterruptamente, para que os prazos sejam contados de forma corrida. Um prazo definido em dias úteis[24] pode causar mais demora no processo de comunicação do incidente já que não se consideram sábados, domingos e feriados. A celeridade na comunicação do incidente de segurança envolvendo dados pessoais garante uma tutela mais efetiva aos direitos dos titulares. Nesse sentido, ressaltamos que o sistema SEI não traz funcionalidades suficientes para garantir a agilidade que esse processo requer. A ANPD ainda deverá considerar formas de retorno do prazo em situações de instabilidade de seu próprio sistema ou por qualquer limitação imposta pelo próprio processo de comunicação (por exemplo: demora em conceder acesso ao SEI). Além disso, o LAPIN incentiva a adoção de outros meios de

[24] Como o da Lei do Cadastro Positivo, mencionado na Nota Técnica nº 3/2021/CGN/ANPD, que é de dois dias úteis a partir da data do conhecimento do incidente.

	comunicação que não dependam da utilização dos canais do SEI, principalmente para os titulares, como algum local para denúncias diretas no site. Ainda deve-se levar em conta que o descumprimento não justificado dos prazos definidos poderá impactar na aplicação, pela ANPD, dos critérios de definição de sanções administrativas previstos no parágrafo primeiro do artigo 52 da LGPD no caso concreto.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Em relação ao prazo para que os controladores informem os titulares de dados sobre o incidente de segurança, sugerimos que seja o mesmo para a ANPD, ou seja, de 10 dias, contados a partir da comunicação parcial. No entanto, recomendamos que a ANPD seja comunicada primeiro nos casos envolvendo dados sensíveis, para que a Autoridade eventualmente forneça orientações mais específicas ao caso concreto. A comunicação com o titular deve conter as informações listadas no §1º do artigo 48 da LGPD, mas essas informações devem ser apresentadas de forma simplificada e em linguagem acessível, de modo a não constarem informações excessivas que tornem o processo de compreensão do incidente extremamente complexo. Como referência, o site do OAG[25] da Califórnia conta com vários exemplos interessantes de comunicação ao titular. Além dos pontos já elencados, o controlador também deve informar quais precauções o titular deve tomar para evitar golpes ou fraudes ou qualquer outro risco oriundo do incidente e qual o contato do encarregado ou equivalente para esclarecimentos adicionais. Tais informações, inclusive, devem ser fornecidas de forma imediata, ainda dentro do prazo para comunicação parcial, preferencialmente. Também pode ser interessante a menção aos dados que **não** foram afetados pelo incidente para o titular ter real controle dos seus dados. Em suma, as

[25] Office of the Attorney General. Disponível em: <https://oag.ca.gov/privacy/databreach/list>. Acesso em 22 mar. 2021.

	informações a serem fornecidas ao titular devem ser aquelas essenciais para o exercício dos direitos previstos na LGPD e para compreensão do risco envolvido no incidente. Além disso, ao se considerar os custos relacionados à comunicação individual e direta, uma forma de atender a essa necessidade de comunicação direta é o envio de mensagens padronizadas simplificadas para os titulares**,** mas com direcionamentos caso o indivíduo queira maiores informações sobre o incidente. Para que esse tipo de comunicação seja suficiente para cumprir os critérios legais, é necessário que a organização disponibilize informes mais detalhados sobre o incidente, além de disponibilizar um sistema de respostas aos direitos do titular adequado (como em uma página facilmente acessível de perguntas frequentes), considerando que em um momento pós-incidente o número de requisições deve aumentar consideravelmente (seria o caso, p. ex., de envio de link que redireciona para página que possibilita o exercício de direitos do titular). Por fim, o LAPIN acredita que devem constar as seguintes informações na comunicação de incidentes de segurança aos titulares de dados[26]: ● Informações elencadas no §1º do art. 48, apresentadas **maneira de simplificada e em linguagem acessível**; ● Indicações de quais **medidas podem ser tomadas para mitigar riscos** (como evitar golpes ou fraudes, ou qualquer outro risco oriundo do incidente); ● O **contato do encarregado** ou equivalente para esclarecimentos adicionais;

[26] Essas indicações são próximas das recomendações trazidas pela Autoridade Australiana, que defende que a comunicação ao titular deve incluir: (i) o nome e as informações de contato da entidade controladora; (ii) as categorias de dados pessoais envolvidos no incidente; (iii) uma descrição do incidente; e (iv) recomendações de medidas que podem ser adotadas pelo titular como resposta ao incidente. Disponível em: <https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach/>. Acesso em 23 mar. 2021.

	• Quando cabível, informações sobre os **dados que <u>não</u> foram afetados** pelo incidente; e • Para comunicações simplificadas, incluir o **canal disponibilizado pela organização** para fornecimento de detalhes adicionais sobre o incidente de segurança.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A forma mais adequada de comunicação de incidentes entre a organização e o titular seria comunicação direta e individual, principalmente através de e-mails, SMS ou até mensagem de WhatsApp[27]. A escolha do meio deve manter a expectativa de relacionamento já estabelecido com aquele titular. Ou seja, se o titular fez o cadastro ou mantém comunicação com o controlador via e-mail, a comunicação deve ser feita por e-mail; agora, se a organização já dialoga por WhatsApp com aquele titular, pode escolher esse meio para informar o indivíduo do incidente ocorrido. O importante é garantir um meio hábil para informar o titular sobre quais medidas de segurança ele deve tomar e quais dados pessoais foram afetados e quais não foram. Dessa forma, há certo empoderamento do titular, impedindo que ele se coloque em maior risco através de qualquer atitude precipitada e movida pelo medo, insegurança ou falta de informação. Essa orientação veio da experiência dos megavazamentos que ocorreram nos últimos meses no Brasil, quando foram proliferados sites que supostamente ajudariam o titular, mas que na realidade coletavam mais dados, e o titular não conseguia diferenciar qual site tinha qual finalidade. Por isso, e até aproveitando da prática consumerista, o LAPIN acredita que a comunicação pública voltada para a conscientização deve ser incentivada em mais casos, visando o incentivo à cultura de privacidade, a observância do princípio da autodeterminação informativa, devendo ser considerada inclusive como uma prática

[27] Nesse sentido, temos a experiência da adoção de uso de WhatsApp para intimação em algumas jurisdições no Brasil, como a Justiça Federal de Pernambuco ou, ainda, o TJDFT. Disponível em: <https://www.cnj.jus.br/uso-de-whatsapp-para-intimacao-e-regulado-na-justica-federal-de-pe/> e <https://www.tjdft.jus.br/institucional/imprensa/destaques/intimacoes-por-whatsapp>. Acesso 22 mar. 2021.

	para mitigação de danos. Mesmo nos casos em que a comunicação à ANPD e aos indivíduos não seja obrigatória, a comunicação pública deve ser considerada como uma boa prática, inclusive mediante anúncios publicitários como disposto no art. 10 do Código de Defesa do Consumidor. Além disso, o LAPIN entende que a comunicação pública também poderá ser admitida em determinadas circunstâncias, como nos casos em que a comunicação direta possa gerar um esforço desproporcional à organização ou quando o controlador não possuir informações individualizadas de contato dos titulares de dados afetados.

Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Sugere-se como exceção para a obrigação de comunicação do incidente à ANPD a situação em que não houver risco ou dano, ou quando o risco for baixo. Isso dependerá dos critérios definidos pela ANPD para a gradação de risco, porém em alguns casos o baixo risco é notório. Para melhor exemplificar tal exceção[28]: um agente de insolvência de dívida enviou por e-mail o arquivo de um novo cliente por engano para um colega em um departamento diferente. O arquivo continha uma lista das dívidas pendentes do cliente, seus detalhes de contato, histórico financeiro básico, informações sobre sua saúde mental e motivos para buscar apoio para sua situação financeira. A organização considera o cliente vulnerável devido ao seu estado mental. O colega que recebeu o arquivo imediatamente apagou o e-mail e informou ao remetente o erro. Nesse caso, apesar de haver o compartilhamento de dados sensíveis para um remetente incorreto, foi realizado para um funcionário da mesma organização e, portanto, sujeito às mesmas políticas de governança de dados, o que reduz o risco significativamente. Ademais, o recipiente do e-mail o deletou e informou ao remetente sobre o erro, possibilitando ações corretivas.
Quais seriam as possíveis exceções da	Não é qualquer tipo de incidente de segurança que deve ser comunicado aos titulares de forma obrigatória. Deve existir uma análise de risco prévia por parte do controlador, de modo que não haja um excesso de comunicações enviadas aos titulares de dados, de forma a causar fadiga. Não há como existir a presunção de risco

[28] Disponível em: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/>. Acesso em 15 mar. 2021.

obrigatoriedade de informar os titulares?	ou dano relevante em todos os incidentes de segurança. Contudo, é relevante que haja critérios para que as comunicações gerem, inclusive, consequências educacionais. Sugere-se que não haja a obrigatoriedade de comunicação do incidente de segurança ao titular quando o risco for baixo ou médio combinado à não ocorrência de dano. Por outro lado, deve haver a obrigatoriedade da comunicação nos casos em que haja a ocorrência de dano ou alto ou alarmante risco. Após a comunicação à ANPD, eventual comunicação ao titular poderá ser recomendada ou determinada pela própria ANPD, caso se entenda pela não obrigatoriedade de comunicar aos titulares automaticamente. De qualquer modo, somente deve haver comunicação ao titular quando este deva se prevenir ou tomar ações para mitigar risco ou dano que possa ser ocasionado em razão do incidente, ou seja, nos casos em que haja a ocorrência de dano ou alto risco.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	A gravidade do incidente deverá ser avaliada tanto pelo controlador, antes da comunicação, quanto pela autoridade, após o processo de comunicação. Essa resposta trará um enfoque para a avaliação realizada pela ANPD, que inclusive poderá contar com a análise dos registros, relatórios e avaliações do controlador. Durante o processo de adequação, o controlador deve ter definido quem será responsável por administrar o procedimento relacionado ao incidente de segurança, incluindo a avaliação da gravidade. Sugere-se que a

	responsabilidade seja direcionada para o encarregado ou equivalente (podendo ser uma única pessoa ou um time)[29]. Essa definição auxiliará o diálogo com a ANPD[30]. Como já mencionado, a análise do risco perpassa a avaliação da gravidade do incidente, havendo relação de proporcionalidade entre esses conceitos - quanto maior a gravidade dos riscos do incidente, maior o risco em si e vice e versa. Mas, especificamente, a gravidade representa a magnitude do risco, se relacionando diretamente à natureza das possíveis consequências do incidente. Com isso em mente, o LAPIN entende que os seguintes critérios devem fazer parte da análise de gravidade do incidente de segurança por parte da ANPD, além daqueles que são considerados na análise dos riscos[31]: ● A **impossibilidade de reversão do incidente** (p. ex., se os dados forem alterados, não existir forma de atualização, ou se eles forem excluídos e não existir backup); ● A adoção de medidas de segurança da informação e de boas práticas **antes do incidente** (p. ex.: utilização de *softwares* certificados, utilização de tipos de criptografia, ter realizado um processo de adequação etc.), como mencionado no art. 46 e 50 da LGPD; ● Se agentes não autorizados têm acesso aos dados; ● O **contexto da ameaça** - origem externa ou interna;

[29] Esse é o direcionamento dado pelo Information Commissioner's Office - ICO - na página sobre "personal data breaches". Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>. Acesso em 16 mar. 2021.

[30] Sobre o tema, ver o relatório produzido pelo *Global Privacy Enforcement Network* (GPEN), disponível em: <privacy.org.nz/publications/statements-media-releases/gpen-sweep-finds-significant-awareness-of-managing-data-breaches-concerns-regarding-low-engagement/>. Acesso em 23 mar. 2021. Apesar da baixa adesão das empresas em participar respondendo o questionário, 84% (oitenta e quatro por cento) das entidades participantes haviam apontado time ou grupo responsável pelo gerenciamento de incidentes de segurança.

[31] Esses critérios também deverão ser considerados na análise de gravidade.

	• As **regiões** afetadas, levando em consideração se há possibilidade de consequências em outros países; ○ Se houver alguma possibilidade de consequência transfronteiriça, avaliar se tais jurisdições contam com um sistema de proteção de dados equivalente; • As medidas de **mitigação de dano** que serão adotadas no momento pós-incidente (ver as indicações sobre comunicação com o titular); • Se a organização irá adotar alguma forma de **comunicação aos titulares** (seja a comunicação direta ou alguma campanha de conscientização mais relacionada à mitigação dos danos); • O **impacto aos direitos e liberdades** do titular; e • A **facilidade de identificação dos indivíduos**.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A gravidade do incidente está diretamente relacionada com os riscos oriundos desse fato. A gravidade do incidente depende das consequências negativas que podem surgir desse fato, sejam potenciais ou efetivas, sejam consequências físicas, materiais ou imateriais, individuais ou coletivas[32]. Como disposto pela autoridade francesa, o nível de risco é mensurado a partir da gravidade e da probabilidade de concretização desse risco e a gravidade representa a magnitude do risco, se relacionando diretamente à natureza dos potenciais impactos[33].

[32] Article 29 Working Party. **Guidelines on Personal data breach notification under Regulation 2016/679.** Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>. Acesso em 16 mar. 2021.

[33] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS (CNIL). **Privacy Impact Assessment (PIA) methodology**. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf> p. 6.. Acesso em 16 mar. 2021.

Em relação à metodologia de análise da gravidade do incidente de segurança, a *European Union Agency for Network and Information Security* (ENISA)[34] propôs o seguinte modelo:

- **DPC x EI + CB = SE**
    - **DPC** (*data processing context*), que é a avaliação da sensibilidade dos dados em um contexto específico de tratamento de dados. Essa avaliação deve passar por 2 passos: (1) definição e classificação dos tipos de dados pessoais afetados; (2) ajustes a partir de fatores contextuais relacionados ao tratamento de dados pessoais. O *score* pode ser representado por 1, 2, 3 ou 4 (importante ressaltar que dados sensíveis começam com a classificação 4 e pode ter o valor minorado a partir da avaliação das circunstâncias concretas, ou dados financeiros começam com o valor 3 e também podem ter o *score* minorado ou majorado, o que demonstra a preocupação anterior relacionada a sensibilidade dos dados);
    - **EI** (*ease of identification*), que representa a facilidade de terceiro não autorizado acessar dados e conseguir identificar uma determinada pessoa. A classificação do EI segue critérios de relevância com atribuição de um valor para cada um, como se segue: insignificante (1); significante (2); e máximo (3). Para essa definição, também devem ser considerados fatores de majoração e de minoração.
        - **Fatores de majoração**: (i) o volume de dados afetados relacionados ao mesmo indivíduo; (ii) características específicas do controlador; e (iii) características específicas dos titulares afetados.

[34] ENISA. **Recommendations for a methodology of the assessment of severity of personal data breaches.** Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity>. Acesso em 16 mar. 2021.

- **Fatores de minoração**: (i) invalidade/imprecisão dos dados afetados; (ii) disponibilização pública (considerar se os dados já eram públicos); e (iii) natureza dos dados afetados.

- **CB** (*circumstances of the breach*), que considera a perda de segurança (confidencialidade, integridade e disponibilidade) e intenção criminosa/ilícita. A partir dessa análise, a pontuação equivalente pode ser acrescentada de 0.25 ou 0.5, podendo alcançar valores representados por 0 a 2.

- **SE** (severity *of a data breach*) é o valor final alcançado, que representa a gravidade do incidente e segue a seguinte classificação:

Gravidade do incidente de segurança		
SE < 2	**Baixa**	Os titulares ou não serão afetados ou poderão encontrar alguns pequenos inconvenientes, os quais serão superados sem qualquer problema (tempo gasto reentrando informações, aborrecimentos, irritações etc.).
2 ≤ SE < 3	**Média**	Os titulares podem encontrar inconvenientes significativos, que eles podem superar apesar de algumas dificuldades (custos extras, dificuldade de acesso a serviços comerciais, medo, falta de compreensão, stress, doenças físicas não-graves etc.).
3 ≤ SE < 4	**Alta**	Os titulares podem encontrar consequências significativas, as quais são passíveis de superação, embora com sérias dificuldades (apropriação indevida de fundos, scores de crédito negativos, danos materiais, perda de emprego,intimação, agravamento da saúde etc.).
4 ≤ SE	**Muito alta**	Os titulares podem se deparar com consequências significativas, ou mesmo irreversíveis, que não podem ser superadas (dificuldades financeiras, tais como dívida substancial ou incapacidade de trabalhar, doenças físicas e psicológicas graves, morte etc.).

Já a *Advisera*, companhia especializada em normas ISO de segurança da informação, através de publicação da *EU GDPR Academy*[35], propôs o seguinte modelo metodológico (aproximando-se de uma versão simplificada do modelo apresentado pela ENISA):

- **DPC x EI + CB = SE**
    - **DPC** (*data processing context*) é a avaliação da sensibilidade dos dados em um contexto específico de tratamento de dados e pode ser representado por 1, 2 ou 3, a depender da categoria dos dados pessoais envolvidos no incidente. Se o incidente só envolve dados não sensíveis, o **DPC deve ser igual a 1**. Se o incidente só afeta dados não sensíveis, mas os dados podem ser utilizados para compreensão do perfil dos titulares de dados afetados, o **DPC deve ser igual a 2**. Agora, se o incidente envolve dados sensíveis, **o DPC deve ser igual a 3**.
    - **EI** (*ease of identification*) reflete a facilidade de identificação dos titulares; ou seja, o EI avalia quão fácil será para uma parte não autorizada, mas com acesso aos dados afetados, identificar os titulares. O EI pode ser representado por 1 ou 2, a depender do tipo de criptografia utilizado para proteção dos dados pessoais. Se os dados pessoais afetados forem protegidos por um tipo de criptografia forte (como AES, RSA, Twofish etc.), dificultando a identificação dos titulares, o **EI deve ser igual a 1.** Em compensação, se as informações sobre o titular estão dispostas de modo compreensível e possibilitam a identificação de um titular específico, o **EI deve ser igual a 2**.

[35] ADVISERA. **Assessing the severity of personal data breaches according to GDPR.** Disponível em: <https://info.advisera.com/eugdpracademy/free-download/assessing-the-severity-of-personal-data-breaches-according-to-gdpr>. Acesso em 16 mar. 2021.

	○ **CB** (*circumstances of breach*) trata da avaliação das circunstâncias do incidente, considerando o tipo de incidente, a perda de segurança e controle dos dados afetados e qualquer intenção maliciosa (criminosa, danosa, ilícita) envolvida no incidente. O **CB deve ser igual a 1** se: (i) os dados são vazados para agentes não autorizados, mas conhecidos/identificados; (ii) os dados pessoais são alterados e utilizados incorretamente ou ilegalmente, mas tais alterações podem ser revertidas; ou (iii) o acesso aos dados foi perdido, mas os dados podem ser restaurados. Contudo, o **CB deve ser igual a 2** nas seguintes situações: (i) os dados são vazados para agentes não identificados; (ii) os dados pessoais são alterados ou utilizados de forma incorreta ou ilegal e tais alterações não podem ser restauradas; (iii) o acesso foi perdido e os dados não podem ser restaurados; ou (iv) o incidente foi causado por comportamento malicioso que afeta os titulares. No cálculo, somente uma circunstância deverá ser tomada em consideração, ou seja, o **CB será sempre igual a 1 ou a 2**. ● **SE** é a gravidade do incidente. ○ Se o resultado final for menor ou igual a 3 (**SE igual ou menor a 3**), o incidente provavelmente não causará riscos ao titular. Assim, tal incidente só deveria ser registrado, não sendo obrigatória a comunicação. ○ Quando o **SE for igual a 4,** é provável que o incidente resulte em algum risco relevante para o titular. Dessa forma, o incidente deve ser reportado para a Autoridade competente. ○ Nos casos em que o **SE for igual ou maior a 5,** existe uma alta probabilidade de riscos para o titular. Por isso, o incidente deve ser notificado para a Autoridade competente e para os titulares afetados.

	O *Information Commissioner's Office* (ICO)[36] disponibiliza um teste para definição da gravidade do incidente para compreender se esse fato deve ou não ser notificado ao ICO. As perguntas do teste, em tradução livre, são as seguintes: ● Uma violação de dados pessoais pode ser definida amplamente como um incidente de segurança que tenha afetado a confidencialidade, integridade ou disponibilidade de dados pessoais. Você já determinou se ocorreu uma violação de dados pessoais? ● Fazendo sua própria avaliação, a violação envolve os dados pessoais de indivíduos vivos? ● Após sua própria avaliação, é provável que haja um alto risco para os direitos e liberdades individuais? ○ Nesse ponto, você precisará avaliar tanto a gravidade do impacto potencial ou real sobre os indivíduos como resultado de uma violação e a probabilidade de que isso ocorra. Se o impacto da violação for mais severo, o risco é maior; se a probabilidade das consequências for maior, então novamente o risco é maior. O WP29 diz que "Este risco existe quando a infração pode levar a danos físicos, materiais ou não materiais para as pessoas cujos dados foram violados" e essa definição deve ser considerada. Para ajudá-lo a avaliar a gravidade de uma violação, foram selecionados exemplos retirados de várias violações relatadas à ICO[37]. Estes também incluem conselhos úteis sobre os próximos passos a serem tomados ou coisas a serem pensadas. Este link será aberto em uma nova guia do navegador.

[36] Disponível em: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/>. Acesso em 16 mar. 2021.
[37] Documento disponível em: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/>. Acesso em 16 mar. 2021.

	● Se você diz sim a todas as perguntas do ICO, você recebe a seguinte orientação[38]: ○ É preciso dizer às pessoas afetadas pela violação sem demora. Você deve informá-las sobre quaisquer medidas que esteja tomando para mitigar os efeitos da violação e dar-lhes conselhos sobre o que fazer para se protegerem; Como você fez uma avaliação, é provável que haja um risco elevado, então você também deve notificar a ICO. Isto deve ser feito dentro de 72 horas após tomar conhecimento da infração. Você pode ligar para nossa Linha de Ajuda[39] para obter orientação sobre como administrar a violação, mitigar o efeito da violação e relatar a violação. A menos que você não possa acessar seu sistema, você deve reportar incidentes cibernéticos online[40]. Alternativamente, se você estiver confiante de que está gerenciando os efeitos da violação e não precisar de aconselhamento, você pode relatar os detalhes da violação on-line. As metodologias apresentadas são adequadas, já que apresentam critérios objetivos a serem considerados. Como é um processo que depende da atuação do controlador, a adoção de metodologias simples e objetivas é positiva e incentivada. Além disso, os modelos metodológicos levam em consideração questões de suma importância, como o contexto do tratamento de dados que foi afetado pelo incidente; a facilidade de identificação de determinado indivíduo, o que se relaciona com a probabilidade de dano; e, ainda, as circunstâncias do incidente. Esse processo ainda avaliará a categoria dos dados afetados e as características dos titulares afetados, o que representa uma síntese das propostas oferecidas pelo LAPIN nessa tomada de subsídios.

[38] Tradução livre.
[39] Iniciativas como essa, um SAC para sanar dúvidas, também podem ser adotadas pela ANPD para aprimorar o procedimento de comunicação.
[40] Essa preferência pelo procedimento e processo eletrônico também é positiva, gera menos burocracia e menos gastos.

	Sugere-se a adoção de critérios semelhantes aos adotados internacionalmente para facilitar o *enforcement* da LGPD tendo em vista o contexto de grande fluxo transnacional de dados. Para facilitar a compreensão de tais modelos, devem ser disponibilizados questionários como o oferecido pelo ICO na página da ANPD.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Uma forma interessante de atuação da ANPD é a consideração de que o incidente de segurança se relaciona diretamente com a segurança da informação (necessária a observância e reforço do princípio da segurança, previsto no art. 6º, VII, LGPD). Por isso, é possível aproveitar desse momento para garantir que novos incidentes não ocorram. Para entender qual seriam as melhores indicações por parte da ANPD, trazemos algumas experiências internacionais, que podem ser adotadas pela Autoridade. *Agencia Española de Protección de Datos Personales* recomenda[41] (essas medidas não ajudam necessariamente a mitigar ou reverter os efeitos do incidente, mas podem servir de inspiração para atitudes imediatas que o controlador poderá tomar): ● Uso de senhas seguras (incluindo o estabelecimento de política de senhas) e autenticação de dois fatores; ● Adoção de cópias de backup; ● Ter sistemas sempre atualizados, tanto o sistema operacional de equipamentos de trabalho e servidores, quanto programas utilizados em dispositivos. Além disso, deve ser estabelecida uma rotina de atualizações frequentes que seja documentada e rastreável; ● Adoção de política rígida dos serviços expostos na Internet. Da mesma forma, os acessos remotos devem sempre ocorrer por meio de sistemas VPN, proxy reverso ou medidas igualmente eficazes; e

[41] Disponível em: <https://www.aepd.es/en/prensa-y-comunicacion/blog/breaches-top-5-measures>. Acesso em 23 mar. 2021.

	• Tornar obrigatória a criptografia, pelo menos para dispositivos portáteis, que podem ser facilmente perdidos ou roubados, e levar em consideração a minimização de dados nos dispositivos. Já o ICO recomenda as seguintes medidas adicionais[42]: • Condução de treinamento obrigatório sobre proteção de dados; • Atualização de políticas e procedimentos e desenvolvimento de uma cultura de confiança para que os funcionários se sintam capazes de relatar casos de falhas de segurança; • Adoção interna do princípio "verificar duas vezes, enviar uma vez"; • Implementação de restrição de acesso a sistemas; • Desativação do preenchimento automático. **Outros endereçamentos possíveis e indicados pelo LAPIN são:** • Organização de uma equipe de resposta especializada que possa conter a violação, identificar e remover as vulnerabilidades; • Remoção imediata de conteúdo exposto de maneira indevida; • Proteção da área física e dos sistemas (tanto para conter o incidente quanto para fins de inspeção posterior); • Condução de investigação imediata junto ao funcionário que deu causa ao incidente; • Estabelecimento de canal de suporte aos titulares afetados para ajudá-los na redefinição de senhas; • Revisão dos softwares e programas utilizados internamente, impondo a utilização de programas com reconhecimento de segurança; e

[42] Disponivel em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>. Acesso em 22 mar. 2021.

	• Acordos de prevenção (motivando novo processo de *compliance* para evitar novos incidentes).