A Year in Privacy

powered by b/luz

VOLUME 3/10

Guia sobre Incidentes de Segurança da Informação e a LGPD

Perspectiva jurídica

A Year in Privacy

powered by b/luz

Autores

Dandara Ramos Silvestre da Silva

Fernanda Catão de Carvalho

Isabelli Gomes Magdaleno

Matheus Botsman Kasputis

Odélio Porto Júnior

Rafaella Resck Braoios

Revisão Técnica

Fernando Bousso

Projeto Gráfico

Fernanda Muchon

Laura Klink

Lucas Bittencourt

índice

Voltar para o índice

INTRODUÇÃO

Este Guia, elaborado pelo Baptista Luz Advogados, explica de forma objetiva as principais obrigações dos agentes de tratamento em relação a incidentes de segurança da informação, conforme previsto na Lei Geral de Proteção de Dados Pessoais ("LGPD"), Lei nº 13.709/2018. O Guia está dividido em temas que perpassam todo o ciclo de vida de um incidente, desde a definição legal do que configura um incidente, quais as medidas de prevenção a serem adotadas, até as recomendações do que fazer durante e após a ocorrência do evento.

Nesse sentido, é importante diferenciar **(i)** as medidas de prevenção de incidentes e **(ii)** as respostas a serem adotadas na ocorrência de um incidente.

Prevenção: medidas/procedimentos e tecnologias implementadas para evitar a ocorrência de um incidente.[1]

Resposta: são as medidas que a empresa deve adotar para responder da melhor forma possível a um incidente de segurança.[2]

Tanto as medidas de prevenção como de resposta devem estar previstas no Sistema de Gestão de Segurança da Informação, por meio de políticas, procedimentos e diretrizes, bem como pela implementação de recursos tecnológicos.[3]

O capítulo 1 deste Guia apresenta uma definição de incidente de segurança da informação para os fins da LGPD. O capítulo 2 busca elencar as principais medidas de governança em privacidade e proteção de dados pessoais que auxiliam os agentes de tratamento a evitar e a responder a um incidente de segurança da informação, em conformidade com a LGPD. Por fim, o capítulo 3 discute as medidas a serem adotadas após a ocorrência de um incidente.

[1]DENSMORE, Russell. Privacy Program Management. In: THOMAS, Liisa. Data Breach Incident Plans. 2ª ed. IAPP. 2019. Cap.9

[2]Ibid.

[3]International Organization for Standardization. ISO/IEC 27000 - Information technology - Security techniques - Information security management systems – Requirements. 2013. p. 11-12.

Voltar para o índice

01 Definição de Incidente

A LGPD não define expressamente o que é um incidente de segurança da informação. Contudo, é fácil extrair uma definição do artigo 46, o qual estabelece que os agentes de tratamento deverão "proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

A descrição da LGPD é semelhante à definição técnica tradicional de incidente de segurança, o qual é definido como a violação a uma ou mais das seguintes **características da informação**:

(i) confidencialidade (acessos ou divulgações não autorizados);

(ii) integridade (quando a informação é alterada indevidamente); e/ou

(iii) disponibilidade (quando, de forma indevida, uma informação fica indisponível para uso).[4]

Imagem 1-princípios de segurança da informação

A Autoridade Nacional de Proteção de Dados (ANPD), em disposições preliminares sobre a matéria, reforçou ainda que o incidente deverá constituir um evento adverso confirmado e que ocasiona riscos para os direitos e as liberdades do titular dos dados pessoais. Embora a definição refira-se apenas a eventos adversos confirmados, no contexto dos planos de governança das empresas, os eventos adversos potenciais (ou iminentes) também deverão ser considerados, visando à prevenção efetiva.

[4] Ibid. p.4.

Nesse sentido, é importante a ressalva de que os incidentes abrangidos pela LGPD são **apenas aqueles envolvendo dados pessoais**, ou seja, caso o incidente de segurança não envolva dados pessoais, a LGPD não se aplicará ao caso.

Exemplo prático

Devido a uma falha elétrica na operação de servidores, uma importante empresa de e-commerce sofre com a interrupção temporária de seu canal online referente ao Serviço de Atendimento ao Consumidor (SAC). Embora a falha tenha sido amplamente noticiada, acarretando danos reputacionais à empresa e prejudicando o acesso dos consumidores a meios de assistência, não ocorreu qualquer violação da segurança dos dados pessoais tratados pelo e-commerce. Diante disso, é possível concluir que também não houve incidente de segurança nos termos da LGPD.

Voltar para o índice

02 Medidas de Prevenção

Na área de segurança da informação é comum a afirmação de que um incidente não é uma questão de "se", mas apenas de "quando". Nesse sentido, a LGPD estabelece tanto a necessidade de adoção de medidas de prevenção de incidentes, que sejam proporcionais aos riscos (art. 46), como obrigações sobre o que fazer após a ocorrência de um incidente que afete os direitos dos titulares (por exemplo, obrigações de notificação estabelecidas pelo art. 48 da LGPD).

2.1 Política de Segurança da Informação

Em relação à estrutura de governança das empresas, a política de segurança da informação normalmente é o documento principal que estabelece os procedimentos e responsabilidades em relação às práticas de segurança. Este documento busca implementar estratégias de mitigação de risco em relação a incidentes, de forma equilibrada com as demandas de negócio da empresa.

A ISO 27000, por exemplo, estabelece que a política de segurança da informação deve:[5]

a| estar adequada aos objetivos da organização/empresa;

b| incluir objetivos de segurança da informação ou fornecer a estrutura para definir os objetivos de segurança;

c| incluir o compromisso de os colaboradores atenderem aos requisitos aplicáveis relacionados à segurança da informação; e

d| incluir o compromisso com a melhoria contínua do sistema de gestão da segurança da informação.

[5] International Organization for Standardization. ISO/IEC 27000 - Information technology - Security techniques - Information security management systems – Requirements. 2013. p.2.

De forma mais detalhada, o guia *ISF Standard of Good Practice* define que uma política de segurança da informação deve estabelecer:[6]

a| regras de classificação da informação, de forma a indicar sua importância para a organização;

b| a definição dos responsáveis pelas informações e sistemas (quais pessoas/cargos são responsáveis pelos processos de negócios que dependem de dados e sistemas de informação importantes);

c| obrigações de análise de risco regulares;

d| obrigações de conscientização de colaboradores sobre segurança da informação;

e| as fontes de obrigações aplicadas à empresa (por exemplo, obrigações legais e regulatórias, contratuais como licenças de software etc.); e

f| como reportar violações à política de segurança da informação e deficiências de segurança da empresa.

Além das obrigações técnicas voltadas ao departamento de TI, é recomendável que a política de segurança da informação também **contenha obrigações e boas práticas a serem seguidas por todos os colaboradores da empresa**. Um exemplo desse tipo de orientação pode se referir a temas como cuidados no compartilhamento de dados com pessoas de fora da organização, controles de acesso à informação, uso adequado de e-mail e websites, como notificar o departamento de TI caso o colaborador identifique um incidente, entre outros.

A política de segurança da informação, principalmente em relação ao período anterior à aprovação da LGPD, acaba por ter como enfoque apenas os aspectos técnicos da segurança. A partir da LGPD, contudo, **passa a ser necessário que a política de segurança da informação integre, na estrutura de governança da empresa, os papéis das equipes de privacidade e do Encarregado (Data Protection Officer).**[7]

[6] INFORMATION SECURITY FORUM (ISF). The Standard of Good Practice for Information Security. 2007. p. 85.

[7] Art. 5, VIII, da LGPD: *"encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".*

Assim, tanto o âmbito da prevenção quanto o da resposta a incidentes devem ser analisados não apenas sob uma perspectiva técnica de segurança, mas também considerando os aspectos de privacidade e proteção de dados pessoais. Isso porque, além do dever geral imposto pela LGPD de garantia da segurança da informação (art. 46), deve o agente de tratamento notificar a ANPD e os titulares caso ocorra um incidente. Contudo, a notificação não deve ser feita para todo e qualquer incidente, mas apenas para os que possam *"acarretar risco ou dano relevante aos titulares"* (art. 48). E é justamente essa análise de risco e dano, sob a perspectiva da privacidade e proteção de dados, que exige uma avaliação adicional à puramente técnica de TI, com o apoio do Encarregado e do time de privacidade.

Guia ANPD. Adicionalmente, também vale destacar o *"Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte"*, publicado pela ANPD em outubro de 2021, que contém orientações gerais sobre segurança da informação para essa categoria de agentes.[8] Como medidas administrativas, o Guia destaca:

a| a implementação de política de segurança da informação;

b| a realização de treinamentos regulares; e

c| o gerenciamento de contratos.

O Guia também sugere algumas medidas técnicas a serem adotadas, sendo as principais:

a| utilização de **controles de acesso** aos dados (autenticação multifatorial dos usuários, definição de níveis de acesso, e registro das atividades realizadas com os dados);

b| definição de procedimentos para **compartilhamento e armazenamento** seguro;

c| utilização de **criptografia** nas comunicações (por exemplo, web application firewall, conexões TLS/HTTP etc.)

[8] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Segurança da Informação de Agentes de Tratamento de Pequeno Porte. 04/10/2021. Disponível em: <https://bit.ly/3MMWkhS>. Acesso em: 13/03/2022.

d | adoção e atualização de **software antivírus**; e

e | regras definidas para uso de **serviços de cloud** e **dispositivos móveis**.

Apesar de não aprofundar nas exigências organizacionais e técnicas relativas à segurança - o que faz sentido devido à chance de menor risco para os tratamentos realizados por agentes de pequeno porte - o Guia da ANPD pode ser utilizado como parâmetro para indicar temas considerados importantes pela Autoridade.

2.2 Plano de Resposta a Incidentes

Na ocorrência de um incidente de segurança, é importante saber quais medidas devem ser adotadas. Neste caso, como proceder? Para responder de forma efetiva a esta pergunta, é indispensável a construção de um plano de ação cuja finalidade seja estabelecer previamente procedimentos e atribuições. A este plano de ação dá-se o nome de "plano de resposta a incidentes".

O plano de resposta a incidentes pode estar incluído na política de segurança da informação, ou ser tratado como um documento à parte. Essa é uma questão de mera escolha organizacional, a qual deve priorizar a facilidade de entendimento pelos colaboradores da empresa que irão aplicar esses documentos. Em relação ao seu conteúdo, o plano pode ser dividido em três etapas: preparação, resposta e avaliação.[9]

[9]SOMBRA, Thiago Luís; CASTELLANO, Ana Carolina Heringer. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva. Revista do Advogado, Distrito Federal, v. 39, t. 144, p. 168-173, 2019.

I. Preparação

A etapa de preparação consiste na elaboração de um procedimento de resposta a incidentes, com a definição dos responsáveis. Recomenda-se que seja estabelecido um comitê de gestão de crise, com colaboradores de áreas multidisciplinares que serão os primeiros a responder ao incidente. Os membros do comitê devem entender o funcionamento da organização e estabelecer as frentes de resolução do incidente de segurança.

De forma geral e para além do comitê, cada área da empresa tem responsabilidades quando da ocorrência, ou mera suspeita, de um incidente, estejam elas diretamente envolvidas ou não. A Associação Internacional de Profissionais de Privacidade (IAPP) lista as seguintes funções a serem desempenhadas por cada área da empresa:[10]

ÁREA	FUNÇÃO
Tecnologia da Informação	Auxiliar na resolução das questões técnicas relacionadas ao incidente, na investigação das suas causas, e nas recomendações a serem implementadas a partir do aprendizado gerado.
Jurídico/Encarregado (DPO)	Avaliar as consequências legais e regulatórias em relação à privacidade e proteção de dados, tomando as medidas jurídicas apropriadas. Também coordenam as notificações às autoridades e aos titulares afetados pelo incidente.
Recursos Humanos	Conscientizar colaboradores sobre detecção e resposta a incidentes.
Financeiro	Calcular o impacto financeiro dos mecanismos para contenção e correção de incidentes, e assegurar recursos para minimizar seus impactos e efeitos.
Comunicação	Coordenar a comunicação sobre o incidente com terceiros, titulares e a ANPD, para prestação de esclarecimentos sobre o ocorrido e sobre ações tomadas pela empresa.
Alta Diretoria	Apoiar a adoção de medidas necessárias para prevenir futuros incidentes, alocar recursos financeiros e profissionais para mitigar o evento, e emitir publicamente comunicados sobre detecção e correção do incidente.

[10]DENSMORE, Russell. Privacy Program Management. In: THOMAS, Liisa. Data Breach Incident Plans. 2. Ed. IAPP. 2019. Cap.9

II. Resposta

A segunda etapa do plano, a etapa da resposta, consiste no acionamento do plano diante de uma ameaça ou da ocorrência propriamente dita de um incidente de segurança. Nessa fase serão adotadas as:

(i) medidas técnicas para interrupção e mitigação do incidente; e

(ii) eventuais notificações aos envolvidos.

Adicionalmente, devem ser coletadas e preservadas as evidências sobre o incidente e sobre as medidas tomadas, as quais podem ser usadas pela organização para defesa em eventuais processos administrativos e judiciais. Inclusive, as medidas tomadas pela organização podem vir a minimizar sanções aplicadas à empresa pelas autoridades.

Deve-se verificar quais **terceiros atuam no tratamento dos dados (fornecedores e parceiros)** que foram impactados e que precisem ser notificados. Essa notificação em tempo hábil é importante principalmente para os casos em que os terceiros precisem cooperar com a empresa para responder tecnicamente ao incidente. Para isso, é recomendável a criação de notificações padrão e o estabelecimento de canais para contato.

Em relação à notificação à ANPD e aos titulares afetados, o plano de resposta a incidentes deve conter os:

(i) procedimentos de análise das consequências do incidente, em relação à privacidade e proteção de dados; e

(ii) os meios e procedimentos para a notificação. Como a LGPD estabelece que o Controlador[11] só deve notificar nos casos de risco ou dano relevante aos titulares (art. 48, §1º), é papel do time de privacidade e/ou do Encarregado fazer essa análise, verificando se as notificações são necessárias.

[11] Art. 5º, VI, da LGPD: "controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

A LGPD estabelece um mínimo de informações que devem ser notificadas à ANPD e aos titulares (art. 48, §1º), especificamente:

a| natureza dos dados pessoais afetados;

b| titulares envolvidos;

c| medidas técnicas e de segurança usadas para a proteção das informações;

d| riscos relacionados ao incidente;

e| caso a comunicação não tenha sido imediata, os motivos que levaram à demora; e

f| as medidas que já foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente.

Adicionalmente, a ANPD publicou um **modelo de notificação à Autoridade** que contém as informações mínimas a serem enviadas à Autoridade e a forma de envio, por meio do Sistema Eletrônico de Informações (SEI) do governo federal.[12] A Autoridade sugere que a comunicação à ANPD seja feita em até 2 dias úteis contados da data de conhecimento do incidente.

Em relação à **forma de notificação aos titulares**, nem a LGPD nem a ANPD definem um formato, mas sugerimos que a comunicação se dê por escrito, preferencialmente por meios que garantam um contato direto com o titular, como e-mail, telefone ou aplicativos de mensagem.

III. Avaliação

A fase de avaliação acontece após o incidente e sua remediação. Seu objetivo é verificar como a organização lidou com o incidente, a fim de incorporar o aprendizado obtido nos procedimentos existentes. Por exemplo, pode ser

[12]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Comunicação de incidentes de segurança. 21/07/2021. Disponível em: <https://bit.ly/3CLIMyn>. Acesso em: 13/03/2022.

importante atualizar a política de segurança da informação e/ou plano de resposta a incidentes, revisar contratos com fornecedores e clientes, gerenciar acessos, avaliar sistemas etc.

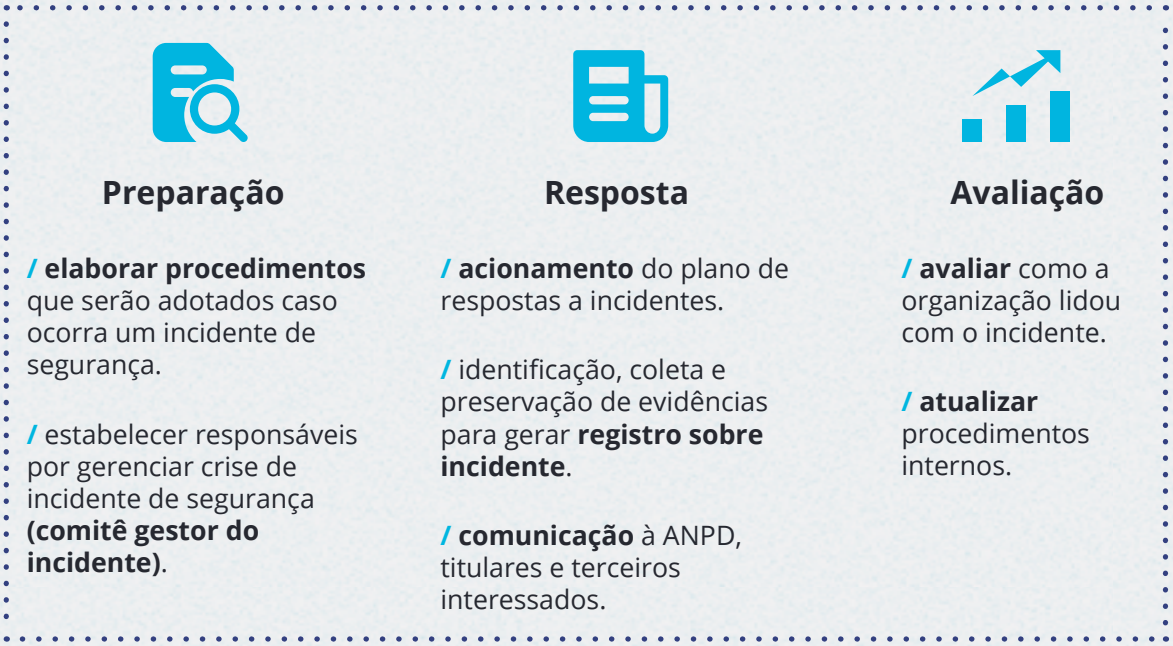


Imagem 2 - Resumo dos elementos do plano de resposta a incidentes

Plano de Continuidade de Negócios

Muitas empresas já possuem um plano de continuidade de negócios (PCN), o qual define procedimentos para manutenção do funcionamento das empresas em casos de adversidades internas e/ou externas. Basicamente, é um plano emergencial que guia a empresa em situações de imprevisto, desde falta de energia elétrica até desastres naturais, e cuja finalidade é reduzir o impacto dessas situações na operação.

É recomendável que o PCN preveja casos relacionados aos principais tipos de incidentes de segurança da informação. Adicionalmente, caso a empresa possua um PCN, este deve estar integrado ao plano de resposta a incidentes e/ou à política de segurança da informação.

2.3 Treinamentos

O treinamento dos colaboradores deve ensinar o funcionamento da estrutura de governança em segurança da informação da empresa, o que envolve:

(i) as medidas de prevenção de incidentes (por exemplo, boas práticas a serem adotadas no compartilhamento de informação); e

(ii) ações a serem tomadas para corrigir e/ou mitigar um incidente em andamento.

O treinamento consiste na educação dos colaboradores, para que tenham uma visão sistêmica de suas responsabilidades e do que deve ser feito. Ainda, a partir de treinamentos e simulações de incidentes podem ser identificadas lacunas técnicas, organizacionais e administrativas da empresa.

Benefícios do treinamento:

a| esclarecimento sobre as funções e responsabilidades de cada um;

b| esclarecimento sobre os procedimentos que devem ser adotados;

c| identificação de eventuais lacunas de segurança;

d| aumento do nível de segurança da empresa, o que reflete em maior confiança dos parceiros e clientes; e

e| diminuição dos riscos de a empresa sofrer incidentes, ou, pelo menos, diminuição da sua gravidade.[13]

[13] DENSMORE, Russell. Privacy Program Management. In: THOMAS, Liisa. Data Breach Incident Plans. 2. Ed. IAPP. 2019. Cap.9

III. Como os treinamentos devem ocorrer e quem deverá realizá-los?

O recomendado é que sejam realizados treinamentos distintos, de forma a se considerar os papéis de cada tipo de colaborador e área na prevenção e resposta a incidentes. Assim, apesar da necessidade de avaliação individual da realidade de cada empresa - considerando sua estrutura organizacional, tratamentos de dados pessoais realizados, tipos de dados etc. - pode-se identificar dois tipos de treinamento:

| **Treinamentos gerais** para colaboradores e eventuais parceiros que realizem tratamento de dados pessoais em nome da empresa, visando garantir que todos tenham conhecimento de conceitos básicos (por exemplo, o que é um incidente de segurança, boas práticas de segurança, para qual área deverá ser realizada a notificação do incidente, entre outros); e

| **Treinamentos específicos**, com base nas responsabilidades atribuídas na política de segurança da informação e/ou no plano de resposta a incidentes, com conteúdo aprofundado para as áreas-chave (TI, time de privacidade, jurídico, comunicação etc.), de forma a reforçar a compreensão das responsabilidades e o aprendizado dos procedimentos, a fim de garantir uma rápida resposta em caso de incidente.

Como elementos de um plano de conscientização, pode-se citar:

a | simulações de incidentes;

b | vídeos;

c | palestras e workshops;

d | cápsulas de conhecimento;

e | seminários; e

f | exercícios.

2.4 Contratação de Seguro

Ainda que as empresas implementem todas as medidas de segurança da informação disponíveis no mercado, elas ainda estão sujeitas a sofrer um incidente de segurança da informação, uma vez que é impossível eliminar todos os riscos e garantir 100% de segurança.[14]

Um incidente de segurança pode acarretar alto custo financeiro[15], o que inclui eventuais multas administrativas e custos relacionados a ações judiciais de reparação de danos. Ainda, além dos custos diretos, pode haver custos indiretos relacionados à interrupção de negócios e perdas de receita, bem como danos reputacionais, que podem vir a representar até 40% dos gastos de um incidente de segurança.[16]

Nesse sentido, atualmente as corretoras de seguro passam a oferecer diversas opções de cobertura, que podem incluir:

a| assessoria imediata para resposta a incidentes, por exemplo: auxílio de consultores em caso de extorsão, assistência de equipes de tecnologia da informação para investigação do incidente, realização de campanhas para mitigação de danos à imagem da empresa etc.;

b| pagamento dos custos referentes à defesa em processos judiciais, bem como eventuais indenizações decorrentes de danos causados a terceiros;

c| cobertura do valor relacionado a multas administrativas;

d| pagamento dos lucros cessantes decorrentes do incidente de segurança da informação;

[14] FORBES. The Future of Cybersecurity Insurance: Policies That Follow the Risk. 2021. Disponível em: <https://bit.ly/3tfXKZl>. Acesso em 21/02/2022.

[15] IBM. Cost of a Data Breach Report. 2021. pp. 7-8. Disponível em: <https://www.ibm.com/security/data-breach>. Acesso em 21/02/2022.

[16] DATA PRIVACY BRASIL. Riscos do Tratamento de Dados & Arquitetura de Segurança da Informação. 2021. Disponível em: <https://bit.ly/3BBO0fs>. Acesso em 21/02/2022.

e| cobertura do valor pago em casos de extorsão cibernética; e

f| pagamento de despesas relacionadas à substituição de ativos digitais e físicos (por exemplo, software e hardware).

Apesar de haver uma vasta gama de opções relacionadas à cobertura contra incidentes de segurança da informação, é necessário entender quais tipos de cobertura fazem sentido para as atividades da empresa. Para isso, alguns critérios devem ser levados em consideração, como os destacados abaixo.

I. Natureza das atividades exercidas

O escopo da cobertura do seguro vai depender, em grande parte, da natureza das atividades da empresa contratante, do volume de dados pessoais tratados por ela e da relevância de recursos tecnológicos no seu negócio. Adicionalmente, o tipo e a frequência de ataques cibernéticos podem variar drasticamente, a depender do setor ao qual a empresa pertence (por exemplo, os setores de energia e saúde), o que pode influenciar nos custos.[17]

II. Obrigações contratuais

Atualmente, antes de contratar fornecedores, prestadores de serviços e/ou parceiros, empresas têm buscado garantias de que esses terceiros estão envidando esforços para a proteção de dados pessoais. A contratação de seguro contra incidentes de segurança da informação pode ser considerada uma dessas garantias. Assim, antes de eleger o escopo da sua cobertura, é aconselhável que a empresa faça um levantamento das suas possíveis obrigações contratuais, para analisar se em alguma delas há exigência de valor mínimo de indenização relacionada a incidentes de segurança.

III. Possibilidade de cumprir com obrigações determinadas pela seguradora

Empresas devem observar cuidadosamente se existem obrigações específicas exigidas pela seguradora para a garantia da cobertura (por exemplo, adoção de medidas mínimas de segurança da informação).

[17]CNN BRASIL. Ataques cibernéticos a empresas brasileiras crescem 220% no 1º semestre de 2021. 2021. Disponível em: <https://bit.ly/34UGHDY>. Acesso em 21/02/2022.

2.5 Fornecedores para Apoio na Resposta a Eventual Incidente

Para lidar de forma adequada com um incidente de segurança, é recomendado que haja uma equipe multidisciplinar para auxiliar a empresa na gestão, apuração e resolução do incidente. Essa equipe é a principal responsável por auxiliar na implementação do plano de resposta a incidentes.

Nesse sentido, o sucesso da resposta ao incidente pode depender de especialistas externos capazes de auxiliar a empresa a apurar e a superar o incidente de forma rápida e eficiente, minimizando, assim, os danos aos titulares, à própria empresa e aos parceiros. Para isso, é preciso que a empresa tenha, em conjunto com seu plano de resposta a incidentes, contatos de fornecedores externos que podem auxiliá-la no enfrentamento da situação de crise.

O conhecimento antecipado de quais fornecedores externos podem ser acionados no caso de um incidente pode ser um diferencial importante, diminuindo o tempo de apuração e resposta ao ocorrido. Assim, listamos abaixo as principais categorias de fornecedores externos que podem auxiliar a empresa durante um incidente de segurança:

a| Escritório de advocacia: auxílio na tomada de decisões em concordância com obrigações legais e regulatórias, prestação de auxílio à elaboração e execução do plano de resposta a incidentes, avaliação dos riscos e danos gerados pelo incidente, elaboração de comunicações a serem enviadas aos titulares e à ANPD.

b| Corretora de criptomoedas: proporcionam ambiente seguro para transações de compra e venda de criptoativos, que podem auxiliar em eventuais pagamentos em sequestros de dados ou pagamentos de recompensa por bugs/falhas de segurança encontrados por terceiros (“bug bounty”).

c| Consultoria em segurança da informação: para apuração das causas do incidente, auxílio na resposta técnica para mitigação e interrupção do incidente, auxílio na coleta de evidências, identificação e monitoramento das informações afetadas, proteção das informações, bloqueio de ameaças, e elaboração de pareceres técnicos.

d| Relações Públicas: planejamento de comunicação estratégica para informar titulares e público externo, incluindo o posicionamento adotado pela empresa e as medidas adotadas para resposta ao incidente.

Esses fornecedores podem auxiliar a empresa na resolução de um incidente de segurança de forma mais eficiente e especializada, sendo, portanto, importante que a empresa tenha conhecimento prévio sobre quais fornecedores ela poderá utilizar na ocorrência ou suspeita de um incidente.

2.6 Metodologias para Gestão de Risco e Outras Boas Práticas

De forma geral, a LGPD impõe aos agentes a obrigação de adotarem *"medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais"* (art. 46), sem definir requisitos técnicos específicos de segurança. A LGPD estabelece apenas que as práticas de segurança da informação a serem adotadas devem ser proporcionais aos riscos oferecidos pela atividade de tratamento de dados pessoais.

A adoção de metodologias e práticas reconhecidas em segurança da informação, além de servir como forma de melhoria da segurança da empresa, pode também auxiliar na atenuação de eventuais sanções aplicadas pela ANPD (artigo 52, § 1º, inciso IX). Ademais, a LGPD indica que os sistemas utilizados para o tratamento de dados pessoais devem razoavelmente alinhar-se a padrões de segurança da informação aceitos pelo mercado (artigo 49).

A metodologia **ISO/IEC 27005:2018** da *International Organization for Standardization*, empregada com consistência pelo mercado, enumera alguns processos para a classificação do risco, os quais incluem, de acordo com o compêndio da ENISA[18]:

(i) o estabelecimento de um contexto;

(ii) a avaliação do risco;

(iii) o tratamento dos riscos;

(iv) a aceitação do risco;

(v) a comunicação e consulta sobre o risco; e

(vi) o monitoramento e a revisão do risco.

Outra metodologia frequentemente referenciada é a **NIST SP 800-37**, do National Institute of Standards and Technology, que indica outros cinco diferentes processos, incluindo:[19]

(i) o preparo de um contexto, funções e prioridades para o gerenciamento do risco;

(ii) a categorização do impacto do risco às operações;

(iii) a seleção, implementação e avaliação de controles adequados para o tratamento do risco;

(iv) a indicação, pelos cargos competentes, de quais riscos de segurança são aceitáveis; e

(v) o monitoramento contínuo das análises de risco e dos impactos aos documentos e sistemas afetados.

Abaixo consta uma lista de metodologias para gestão de risco em segurança da informação:

[18]European Union Agency for Cybersecurity. Compendium of risk management frameworks with potential interoperability. 2022. Disponível em <https://bit.ly/3HM9Tu4>, p. 08.

[19]Ibidem, p. 09-10.

Metodologias de Gerenciamento de Risco[20]

1 | ISO/IEC 27005:2018

2 | NIST SP 800-37 REV. 2

3 | NIST SP 800–30 REV.1

4 | NIST SP 800–39

5 | NIST SP 800–82 REV. 2

6 | BSI STANDARD 200-2

7 | OCTAVE-S

8 | OCTAVE ALLEGRO

9 | OCTAVE FORTE (OCTAVE FOR THE ENTERPRISE)

10 | ISACA RISK IT FRAMEWORK

11 | INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2)

12 | ETSI TS 102 165-1, THREAT VULNERABILITY AND RISK ANALYSIS (TVRA)

13 | MONARC

14 | EBIOS RISK MANAGER

15 | MAGERIT V.3: ANALYSIS AND RISK MANAGEMENT FOR INFORMATION SYSTEMS

16 | EU ITSRM, IT SECURITY RISK MANAGEMENT METHODOLOGY V1.2

17 | MEHARI

18 | ENTERPRISE RISK MANAGEMENT – INTEGRATED FRAMEWORK

19 | AUSTRALIAN ACSC SECURITY MANUAL

20 | ANSI/ISA-62443-3-2-2020

21 | THE OPEN GROUP STANDARD FOR RISK ANALYSIS (O-RA), VERSION 2.0

22 | CORAS

23 | IS RISK ANALYSIS BASED ON A BUSINESS MODEL

[20]Conforme European Union Agency for Cybersecurity. Compendium of risk management frameworks with potential interoperability. 2022. Disponível em <https://bit.ly/3HM9Tu4>.

24| IMO MSC-FAL.1/CIRC.3 GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

25| GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

26| HITRUST

27| ISRAM - INFORMATION SECURITY RISK ANALYSIS METHOD

28| FAIR - FACTOR ANALYSIS OF INFORMATION RISK

29| RISK MANAGEMENT TOOLS

30| GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE

Além do estabelecimento de processos para a classificação de riscos à privacidade e proteção de dados, entre outras boas práticas que podem ser empregadas pelas empresas, vale mencionar, em alguns casos, a contratação de **consultorias especializadas** em segurança da informação e respostas a incidentes de segurança, que conduzirão auditorias prévias à concretização do risco nos sistemas e aplicações identificados ou auxiliarão com o combate e a resposta às ameaças detectadas.

Também é recomendável ao agente de tratamento conduzir **testes de penetração** *(pentests)* às redes e aos sistemas, com certa regularidade, seja por meio de sua própria equipe de TI/SI ou com o apoio de terceiros especializados, desde que os registros e resultados de tais testes sejam devidamente documentados e eventualmente apresentados às autoridades competentes caso a empresa seja acionada nesse sentido.

Voltar para o índice

03 Gestão do Incidente

3.1 Investigação do Incidente

A investigação do incidente de segurança da informação é uma parte crucial da gestão pós incidente, cujo objetivo é o esclarecimento das suas causas, a análise dos danos gerados e a obtenção de aprendizado institucional. Ademais, as informações sobre as causas do incidente e suas consequências são fundamentais para a avaliação da necessidade de notificação á ANPD e aos titulares.

A investigação é uma **medida predominantemente técnica**, que irá envolver tanto o time interno de segurança da informação, como, eventualmente, a contratação de consultorias especializadas em segurança da informação.

Em conjunto com a investigação, é necessário que o time responsável passe a documentar todas as informações, seja para utilização na notificação do incidente ou para eventual defesa em procedimentos administrativos e judiciais. Como ponto de partida, incluímos abaixo uma lista não exaustiva de informações a serem documentadas. É importante que o registro do incidente seja atualizado na medida em que novas informações forem descobertas. Cada atualização deve ser sinalizada como tal e conter log de data e hora referente às novas descobertas ou andamentos.

a | Resumo do incidente (explicação sobre o ocorrido);

b | Causas do incidente (motivações e circunstâncias técnicas);

c | Data de ocorrência;

d | Data da detecção do incidente;

e | Forma de detecção do incidente;

f | Data de término do incidente, se houver;

g | Consequências do incidente;

h | Utilização de consultorias especializadas;

i | Tipos de dados pessoais afetados; e

j | Quais os titulares afetados.

O *National Institute of Standards and Technology do U.S. Department of Commerce* disponibilizou listagem com uma série de procedimentos que podem facilitar a identificação, documentação e preservação de provas relacionadas ao incidente.[21] Indicamos abaixo os procedimentos que entendemos ser de maior utilidade para a produção de provas:

- **Criar perfil de redes e sistemas.** A partir da criação de perfil, é possível registrar as principais características das redes e sistemas da empresa, facilitando a identificação e comprovação de atividades estranhas. Isso pode ser feito por meio de um processo chamado monitoramento da integridade de arquivos, o qual compara a situação atual das redes e sistemas com o perfil criado anteriormente.

- **Criar política de retenção de logs.** Considerando que informações sobre um incidente podem ser registradas em diversos locais, como firewall, IDPS e logs de aplicativos, é importante criar e implementar uma política de retenção de log que especifique por quanto tempo os logs devem ser mantidos. É comum que incidentes perdurem por um longo período em razão da dificuldade em detectá-los. Assim, a manutenção do registro de logs possibilitará que a empresa obtenha as informações necessárias sobre o incidente desde o seu início. A definição do período para manutenção dos logs dependerá de vários fatores, incluindo as políticas de retenção de dados da empresa e o volume dos dados.

- **Correlacionar eventos.** As provas de um incidente podem ser capturadas em vários logs, cada um contendo diferentes tipos de dados (por exemplo, um log de firewall pode ter o endereço IP de origem que foi usado pelo malfeitor, enquanto um log de aplicativo pode conter o seu nome de usuário). Logo, correlacionar eventos por meio da análise de logs pode ser importante para compilar informações úteis sobre o incidente.

- **Manter relógios sincronizados.** Por meio do Network Time Protocol (NTP), empresas podem sincronizar os relógios dos computadores e dispositivos em rede utilizados em suas operações. Isso facilitará a correlação de eventos.

[21] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Security Incident Handling. 2012. pp. 29-30. Disponível em: <https://bit.ly/3BLdiI3>. Acesso em 22/02/2022.

- **Executar analisadores de pacotes para a coleta de dados adicionais.** Caso a empresa detecte que um incidente está ocorrendo, por meio de um analisador de pacotes, ela pode capturar o tráfego de rede e o fluxo de dados que estão sendo transmitidos. A partir daí, é possível coletar informações adicionais sobre o incidente.

- **Buscar ajuda de terceiros.** A depender da magnitude e da complexidade do incidente, é possível que a equipe interna de TI da empresa não seja capaz de determinar a causa e a natureza do incidente. Nesse caso, é aconselhável que a empresa busque consultores e recursos externos (por exemplo, equipe de forense digital).

Finalmente, existem diversos casos em que os dados comprometidos em incidentes de segurança da informação acabam sendo disponibilizados na dark web, que são páginas da internet que escondem os seus endereços IP, dificultando, assim, o seu acesso.[22] A privacidade fornecida pela dark web fez com que o ambiente se tornasse propício para atividades ilegais, como, por exemplo, a venda de dados pessoais indevidamente obtidos. Logo, é importante que empresas façam uma varredura na dark web após a ocorrência de um incidente, a fim de descobrir se os dados foram efetivamente obtidos por um malfeitor.

3.2 Avaliação do Risco e Dano

Após a ocorrência de um incidente, o agente de tratamento deve avaliar suas consequências a fim de verificar:

(i) se é necessário notificar a ANPD e os titulares afetados;

(ii) quais são as medidas que podem ser adotadas para minimizar e/ou reverter os danos e riscos aos titulares e ao próprio agente; e

(iii) quais medidas preventivas podem ser adotadas com base no aprendizado obtido com o incidente.

[22] WIRED. Hacker Lexicon: What Is the Dark Web. 2014. Disponível em: <https://bit.ly/3Hg4s6u>. Acesso em 22/02/2022.

Importante destacar que consideramos ser útil na avaliação a diferenciação entre um **dano** efetivamente gerado pelo incidente (por exemplo, perda de confidencialidade da informação) e os **riscos** acarretados, os quais podem ou não se materializar em dano (por exemplo, aumento das chances de o titular sofrer uma fraude).

Risco vs. Dano

A título comparativo, é interessante citar o debate jurídico que vem ocorrendo nos tribunais dos Estados Unidos em relação aos conceitos de "risco" e "dano".[23] Alguns tribunais têm entendido que um dano relacionado a um incidente só ocorre se for comprovado que os dados pessoais afetados foram utilizados de maneira indevida (por exemplo, roubo de identidade ou fraude). Em outros casos, porém, alguns tribunais têm entendido que o simples fato de o incidente ter aumentado os riscos (probabilidade) de uso indevido seria o suficiente para configurar dano ao titular.

Assim, vale ressaltar que debate semelhante pode vir a ocorrer no Brasil, na medida em que os tribunais comecem a julgar cada vez mais casos envolvendo incidentes de segurança da informação.

Também vale esclarecer que este subtópico se refere apenas à avaliação das consequências aos titulares afetados pelo incidente em relação à privacidade e proteção de dados, pois é a partir dessa avaliação que se aplica parte das obrigações da LGPD (por exemplo, notificação do incidente).

Abaixo são explicados exemplos de metodologias e elementos para auxiliar na análise de um incidente de segurança da informação envolvendo dados pessoais.

I. ANPD

Até a data de publicação deste Guia, a ANPD não publicou orientação ou metodologia específica para análise das consequências de um incidente de segu-

[23]SOLOVE, Daniel J.; CITRON, Danielle Keats. Risk and Anxiety: A Theory of Data-Breach Harms.Texas Law Review, nº 737. 2018. Disponível em: <https://bit.ly/3t8ZfJZ>. Acesso em: 13/03/2022.

rança da informação. Contudo, verifica-se que alguns elementos de análise podem ser inferidos do modelo de notificação de incidentes à ANPD[24], sendo os principais:

a| natureza dos dados pessoais (por exemplo, dados sensíveis, financeiros, e de geolocalização etc.);

b| quantidade de titulares;

c| categoria dos titulares (por exemplo, consumidores, crianças, adolescentes etc.);

d| medidas adotadas para reverter ou mitigar os efeitos do prejuízo do incidente; e

e| análise das prováveis consequências do incidente.

Assim, o modelo de notificação de incidentes da ANPD apenas oferece alguns parâmetros para que os agentes atingidos por um incidente possam analisar a gravidade do incidente, para fins de notificação. Um ponto de atenção é que a ANPD faz a diferenciação das consequências de um incidente entre o risco gerado e o dano sofrido pelos titulares, contudo, não oferece maiores detalhes sobre essa diferenciação.

II. ENISA

A Agência Europeia para a Segurança das Redes e da Informação (ENISA) desenvolveu, em parceria com a Autoridade de Proteção de Dados da Alemanha e da Grécia, uma metodologia quantitativa para análise da gravidade de incidentes de segurança da informação envolvendo dados pessoais.[25]

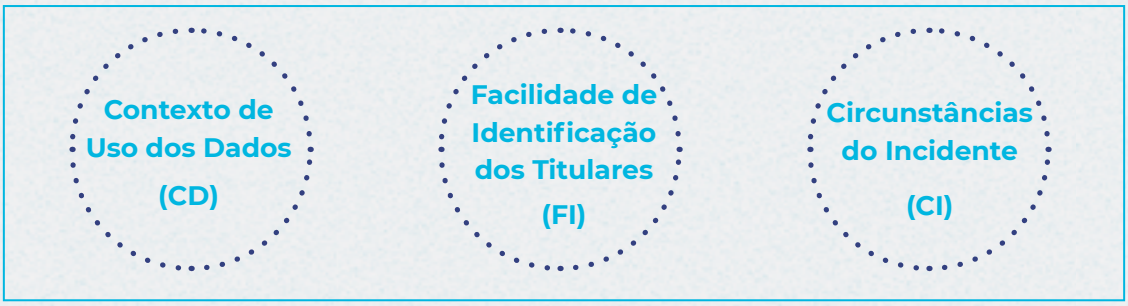
A ENISA entende que a avaliação da gravidade de um incidente de segurança refere-se à "estimativa da magnitude do impacto potencial sobre os indivíduos derivado da violação dos dados"[26]. Como potenciais impactos, podemos

[24]AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Formulário de comunicação de incidente de sDigite a equação aqui. egurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD). 21 de julho de 2021. Disponível em: <https://bit.ly/3HyL4le>. Acesso em: 03/03/2022.

[25]EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. Recommendations for a methodology of the assessment. of severity of personal data breaches. Versão 1. Dezembro, 2013. Disponível em: <https://bit.ly/3pBWQVY>. Acesso em: 03/03/2022.

[26]Ibid, p.2. Tradução nossa.

citar, como exemplo, roubo de identidade, fraude, dano físico e dano moral (por exemplo, dano à reputação). A metodologia apresenta três elementos principais de análise:



Os três elementos são relacionados quantitativamente para formar uma nota de gravidade do incidente, pela seguinte fórmula:[27]

Gravidade = (CD x FI) + CI

Abaixo serão analisados, de forma resumida, a composição de cada um dos três elementos.

i. Contexto de Uso dos Dados (CD)

Este item é o elemento principal da análise, avaliando a criticidade dos dados afetados pelo incidente. A nota do CD é feita com base nos seguintes elementos:

• Passo 1 - Classificação dos tipos de dados pessoais: comuns, comportamentais, sensíveis e financeiros – importante notar que a ENISA considera essas categorias como não exaustivas, podendo haver outras.

• Passo 2 - Fatores contextuais: volume dos dados, características específicas do controlador e/ou dos titulares, se os dados estão publicamente disponíveis etc.

[27] Ibid, p.3.

ii. Facilidade de Identificação dos Titulares (FI)

O FI busca verificar o quão fácil seria a associação dos dados afetados pelo incidente ao respectivo titular. A facilidade de identificação pode ser classificada como: **(i)** insignificante, **(ii)** limitada, **(iii)** significativa e **(iv)** máxima. Este item funciona no cálculo como um fator de correção do CD, servindo para ajustar (para mais ou para menos) o grau de criticidade dos dados afetados pelo incidente.

iii. Circunstâncias do Incidente (CI)

Por fim, este item serve no cálculo como elemento majorante ou minorante da gravidade do incidente, com base na ocorrência de determinados fatores. Considera, portanto, se houve a ocorrência dos seguintes fatos:

(i) perda de confidencialidade;

(ii) perda de integridade;

(iii) perda de disponibilidade; e

(iv) se o incidente teve caráter acidental, humano, técnico ou intencional.

Para verificação de como cada um dos elementos é pontuado no cálculo da gravidade, deve ser consultado os anexos da recomendação da ENISA: "Recommendations for a methodology of the assessment of severity of personal data breaches".[28]

3.3 Aprendizado Pós Incidente

A implementação de medidas eficazes para a gestão e resposta eficazes a incidentes de segurança, por mais bem elaboradas que sejam, encontram espaço para melhorias, sendo a ocorrência de um incidente uma oportunidade de aprendizados. Após a remediação dos efeitos de um incidente de segurança, a realização de uma avaliação interna possibilita a incorporação das lições aprendidas na prática com o incidente. Esse aprendizado pode ser utilizado

[28] Ibid.

no aprimoramento dos processos na prevenção, detecção e resposta a incidentes similares no futuro.

A efetivação do aprendizado pós-incidente pode ser feita por meio da coleta de informações, como em reuniões com responsáveis pelos setores envolvidos[29] na resolução do incidente, extraídas dos relatórios de acompanhamentos[30] etc. A coleta de tais informações pode ter como objetivo a resposta de questões centrais[31] [32], como:

a| Quais partes do processo de resposta funcionaram? Quais partes não funcionaram?

b| Foi necessário executar procedimentos não documentados? Em caso afirmativo, eles foram executados com sucesso e documentados?

c| Foram encontrados imprevistos? Como eles poderiam ter sido evitados?

d| Qual a diferença entre os custos reais e os custos orçados?

e| Quais informações podem corrigir incidentes similares?

Após o registro do incidente, a organização terá um conjunto de informações que devem ser incorporadas aos procedimentos internos, através, por exemplo, da:

(i) revisão da política de segurança da informação e/ou do plano de resposta a incidentes;

(ii) revisão de contratos com fornecedores;

(iii) reavaliação de procedimentos de acesso e compartilhamento de dados;

(iv) revisão das diretrizes de notificação; e

(iv) avaliação de sistemas e ferramentas de segurança.

As respostas a essas questões também podem servir como fontes para a elaboração de treinamentos baseados não somente em situações hipotéticas, mas em crises já superadas pela organização, possibilitando uma capacitação mais robusta dos colaboradores.

[29]Computer Security Incident Handling Guide. National Institure of Standarts and Technology. p.38. Disponível em: <https://bit.ly/3JaocKu>. Acesso em 29/11/2021.

[30]Idem, p.39

[31]DENSMORE, Russell. Privacy Program Management. In: THOMAS, Liisa. Data Breach Incident Plans. 2ª ed. IAPP

Voltar para o índice

04 Conclusão

De forma resumida, a LGPD estabelece apenas uma **obrigação geral de proteção da segurança dos dados pessoais** (art. 46), deixando em aberto a forma como os agentes de tratamento irão selecionar e adotar as medidas técnicas e organizacionais. A ANPD ainda não publicou orientações robustas sobre o tema, sendo importante ressaltar, contudo, os elementos listados no:

(i) modelo de comunicação de incidentes de segurança à ANPD; e

(ii) *"Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte"*.

Assim, é recomendável que os agentes de tratamento busquem estruturar seu programa de governança e segurança da informação **com base em boas práticas e metodologias reconhecidas pelo mercado** (por exemplo, ISO 27000 e a metodologia da ENISA para a avaliação de incidentes). A adoção de políticas e procedimentos robustos é fundamental tanto para se evitar incidentes como para mitigar e solucionar incidentes que venham a ocorrer.

Ademais, a verificação da necessidade de **notificação dos titulares e da ANPD** exige uma análise do *"risco ou dano relevante aos titulares"* (art. 48) que deve ser feita de forma adequada, podendo ser mais robusta nos casos em que o agente utilize metodologias reconhecidas de avaliação de risco.

b/luz

deixa com a gente

Para saber mais, acesse nosso site ou
nos acompanhe nas redes sociais.

baptistaluz.com.br