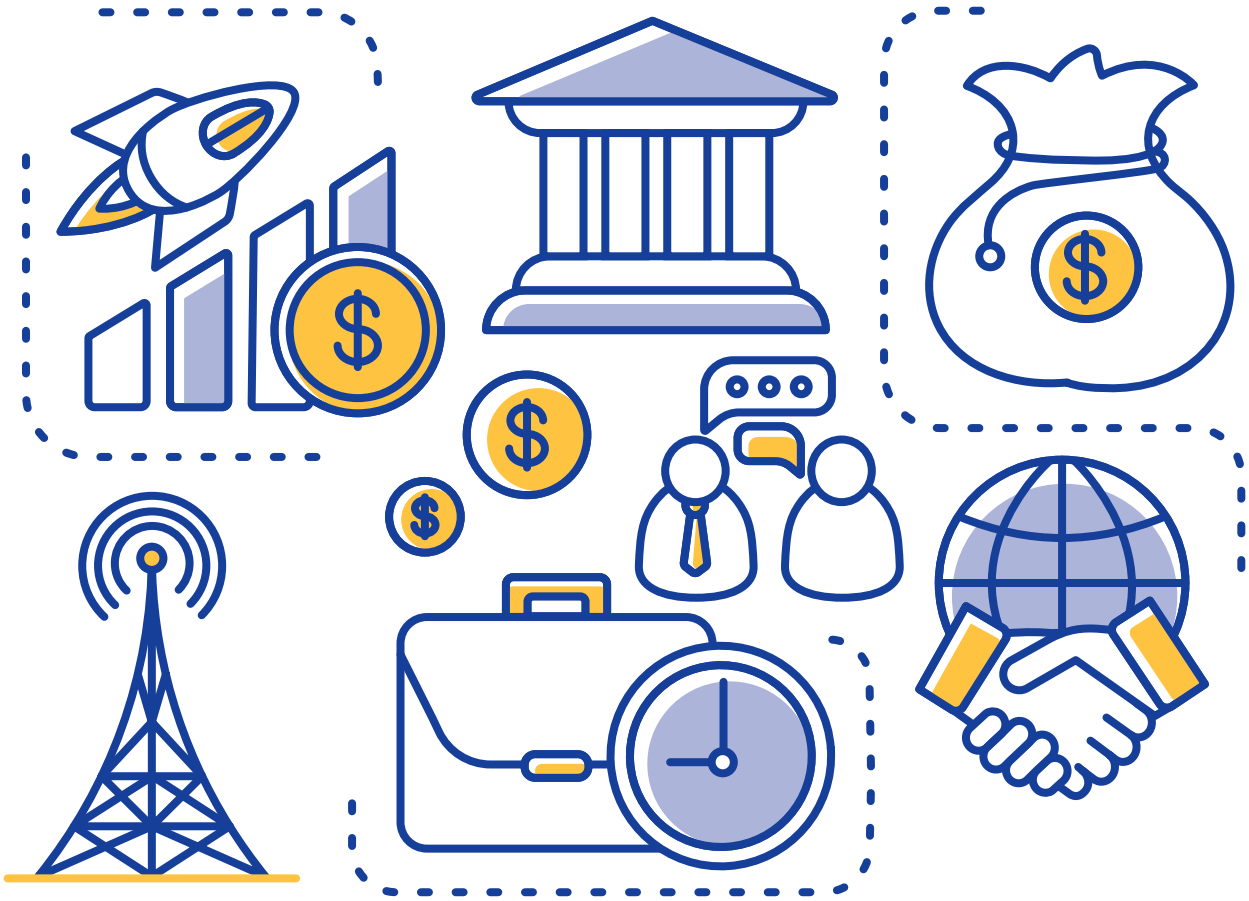


SEGURANÇA DA INFORMAÇÃO:

SETORES REGULADOS

@opiceblum

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

ÍNDICE

Diretiva NIS 2016/1148 da União Europeia

Setores

- Energia
- Saúde
- Aviação Civil
- Financeiro
- Mercado de Valores
- Telecomunicações
- Seguros Privados

Proteção de Dados Pessoais

- Lei Geral de Proteção de Dados (LGPD)
- *General Data Protection Regulation* (GDPR)

INTRODUÇÃO

Atualmente, sistemas informacionais desempenham papel vital na sociedade, com fiabilidade e segurança essenciais para a realização de atividades econômicas, promoção de serviços e o funcionamento do mercado.

Amplitude, frequência e impacto de incidentes de segurança nesses sistemas têm aumentado cada vez mais, o que ameaça gravemente seu funcionamento e os negócios que deles dependem. Esses sistemas têm se tornado, ainda, alvo frequente de ações danosas, que podem danificar ou interromper sua operação.

Incidentes de segurança da informação podem impedir o exercício de atividades econômicas, gerar perdas financeiras, minar a confiança dos usuários e impedir que serviços essenciais sejam prestados à população.

Desse modo, a segurança desses sistemas tem sido cada vez mais objeto de debate, tanto pelas próprias organizações que os empregam, quanto por órgãos responsáveis por sua fiscalização. As agências reguladoras têm direcionado seu foco aos requisitos necessários para garantir a segurança e o bom desempenho de redes e sistemas de informação, bem como às medidas tomadas em caso de incidentes, tendência observada no Brasil e na Europa.

Na presente cartilha, serão apresentadas as principais regras vigentes no âmbito de setores regulados brasileiros e europeus, que têm como objetivo regular a segurança da informação, em especial no que diz respeito a incidentes e deveres de notificação às autoridades.

Para saber mais sobre o tema, acesse nossa cartilha "**Como identificar e reagir a incidentes de segurança**" e nosso guia "**Incidentes de segurança da informação – dever de comunicação**".

Boa leitura!

Diretiva NIS 2016/1148 da União Europeia

Como parte da **Estratégia de Segurança Cibernética da União Europeia**, a Comissão Europeia propôs a **Diretiva de Segurança de Redes e Sistemas de Informação** (*NIS Directive EU* 2016/1148), primeira legislação sobre o tema aplicada a todo o Bloco. Após sua adoção em 2016, os Estados-membros passaram a transpor seu conteúdo a legislações nacionais específicas.

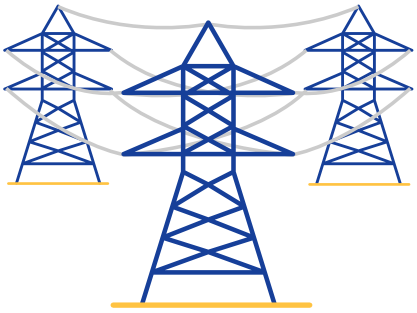
A Diretiva estabelece, entre outros, requisitos de segurança e de notificação para operadores de serviços essenciais e para prestadores de serviços digitais. Como operadores de serviços essenciais entendem-se as entidades públicas ou privadas atuantes nos seguintes setores: **energia**, **transportes**, **bancário**, **mercado financeiro**, **saúde** e de **infraestruturas digitais** (pontos de troca de tráfego, prestadores de serviços de DNS e TLD). Os prestadores de serviços digitais, por sua vez, incluem entidades fornecedoras de mercados em linha, motores de pesquisa em linha e serviços de computação em nuvem.

A fim de determinar a importância do impacto de um incidente, são levados em consideração:

- Número de usuários afetados pela perturbação do serviço essencial
- Duração do incidente
- Distribuição geográfica, no que se refere à zona afetada pelo incidente

Setores

Energia:



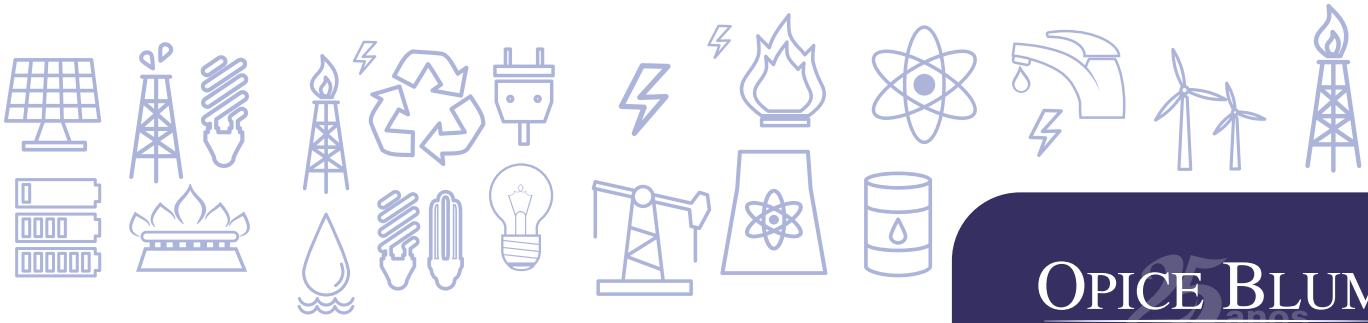
A **Resolução Normativa nº 964, de 14 de dezembro de 2021, da Agência Nacional de Energia Elétrica (ANEEL)**, em vigor desde 1º de julho de 2022, estabelece as diretrizes e o conteúdo mínimo das políticas de segurança cibernética dos agentes do setor de energia elétrica.

Em seu artigo 6º, a norma estabelece que os agentes devem notificar a equipe de coordenação setorial responsável pelos incidentes cibernéticos de maior impacto que afetem de maneira substancial a segurança das instalações, a operação ou os serviços aos usuários ou de dados.

Essa notificação deverá incluir análise da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso. Ela deverá ser realizada assim que o agente tiver ciência do incidente e de sua dimensão.

Finalmente, estabelece-se que a notificação do incidente cibernético de maior impacto não exclui o atendimento de outras obrigações de comunicação previstas em leis, normas e regulamentos.

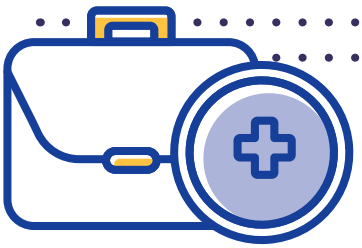
No cenário europeu, segundo a Diretiva NIS 2016/1148, para o setor de energia elétrica, além dos critérios intersetoriais levados em consideração, será necessário observar a quantidade ou a percentagem de energia nacional gerada.



Além dessa norma, a União Europeia conta com outra diretivas que tratam especificamente sobre setor de energia, a exemplo:

- Diretiva 2019/944 do Parlamento Europeu e do Conselho;
- Regulamento 2019/943 do parlamento europeu e do conselho: estabelecem princípios gerais sobre a segurança cibernética e a proteção de dados aplicáveis aos medidores inteligentes e às redes de transmissão e distribuição;
- Recomendação 2019/553 da Comissão: define as principais questões relacionadas à segurança cibernética no setor da energia, nomeadamente os requisitos em tempo real, os efeitos em cascata e a combinação de tecnologias clássicas e de ponta. As orientações estão focadas na análise de risco e no grau de prontidão em relação a sistemas, *softwares, hardwares* e sistemas de monitoramento automatizados;
- Regulamento 2019/941 do Parlamento Europeu e do Conselho: focado na prevenção de crises, que estabelece normas para a cooperação entre os Estados-membros, tendo em vista prevenção, preparação e gestão de crises de eletricidade, em um espírito de solidariedade e de transparência, e no pleno respeito aos requisitos de um mercado interno de eletricidade competitivo.

Saúde:



Instituído pela Agência Nacional de Saúde Suplementar, o **TISS** (sigla referente à Troca de Informação de Saúde Suplementar) é utilizado para estabelecer o fluxo de informações entre os prestadores de serviços, as operadoras privadas e a ANS, bem como para garantir o faturamento desses prestadores. O documento é estruturado em todos os campos que devem ser preenchidos, o que reflete na padronização dos dados que serão enviados à ANS e no menor índice de intercorrências.

O padrão TISS está organizado em cinco componentes:

Organizacional: estabelece o conjunto de regras operacionais.

Representação de Conceitos em Saúde: estabelece o conjunto de termos para identificar eventos e itens assistenciais na saúde suplementar, consolidados na Terminologia Unificada da Saúde Suplementar - TUSS.

Conteúdo e estrutura: estabelece a arquitetura dos dados utilizados nas mensagens eletrônicas e no plano de contingência, para coleta e disponibilidade dos dados de atenção à saúde.

Comunicação: estabelece meios e métodos de comunicação das mensagens eletrônicas definidas no componente de conteúdo e estrutura. Adota a linguagem de marcação de dados *XML - Extensible Markup Language*.

Segurança e Privacidade: estabelece os requisitos de proteção para assegurar o direito individual ao sigilo, à privacidade e à confidencialidade dos dados de atenção à saúde. Tem como base o sigilo profissional e segue a legislação.

O padrão TISS é obrigatório por lei, tendo como regulamentação a Resolução Normativa nº 305/2012. Entre as especificações, estão vedação da alteração do documento pelas operadoras de saúde, assim como obrigação de respeitar o padrão utilizado pela ANS e a utilização de arquivos XML.

A Diretiva NIS 2016/1148 estabelece que, para o setor de Saúde, independentemente dos critérios levados para identificar e mensurar um incidente, deverá ser observado o número de pacientes sob cuidados do prestador em cada ano.

Aviação Civil:

A Agência Nacional de Aviação Civil (ANAC), por meio da **Instrução Normativa nº 128, de 6 de novembro de 2018**, aprovou a Política de Segurança da Informação (POSI/ANAC), que objetiva dotar a Agência de instrumentos jurídicos, normativos e organizacionais de capacitação científica, tecnológica e administrativa, para assegurar confidencialidade, integridade e autenticidade, além do não repúdio e da disponibilidade dos dados e das informações tratadas, classificadas e sensíveis.

A POSI tem por objetivo promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação; estabelecer diretrizes para a elaboração de normas complementares e procedimentos internos necessários à efetiva implementação da segurança da informação; e promover as ações necessárias à implementação e manutenção da segurança da informação.

Por meio da **Portaria nº 5805, de 30 de agosto de 2021**, a ANAC instituiu o Comitê de Segurança da Informação e de Proteção de Dados Pessoais, cujas atribuições envolvem, entre outras: emitir orientações gerais às unidades organizacionais quanto à implementação das ações de Segurança da Informação e de Proteção de Dados Pessoais, aprovar normas complementares relativas à Segurança da Informação e à Proteção de Dados e acompanhar investigações e avaliações dos danos decorrentes de quebras de segurança.

A ANAC, por meio do *Brazilian Aviation Security Team* (BASeT), lançou o "**Manual de Conscientização em Segurança Cibernética na Aviação Civil**" com o objetivo de auxiliar diversas organizações e empresas da aviação civil a verificar a segurança dos processos internos que utilizam tecnologia de informação e avaliar a necessidade de incremento de segurança.

As informações contidas no manual podem servir de base para a realização de avaliação de risco em segurança cibernética por operadores da aviação, que encontra previsão em regulamentos, **como o Regulamento Brasileiro da Aviação Civil (RBAC) nº 107 para operadores de aeródromo** e o **RBAC nº 108 para operadores aéreos**.

No que diz respeito a incidentes cibernéticos, o Manual menciona que, a depender da natureza do incidente, a comunicação com as autoridades apropriadas, autoridade da aviação civil, fabricantes de equipamentos e fornecedores de serviços será importante para habilitar a informação que será compartilhada com outros usuários.

Para a Aviação Civil, incluindo os aeroportos e as transportadoras aéreas, o transporte ferroviário e os portos marítimos, a Diretiva NIS 2016/1148 prevê que, para a completa mensuração dos riscos e danos de um incidente, devem ser analisados a percentagem de volume de tráfego nacional e o número de passageiros ou de operações de movimentação de carga anuais.

Financeiro:

A **Resolução CMN nº 4.893/2021** dispõe que as instituições autorizadas a funcionar pelo BACEN devem observar os seguintes critérios:

- Implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados;
- Estabelecer plano de ação e de resposta a incidentes objetivando a implementação da política de segurança cibernética;
- Elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes;

- Assegurar suas políticas, estratégias e estruturas para gerenciamento de riscos previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços;

- Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, as instituições autorizadas a funcionar pelo BACEN devem avaliar se os fornecedores possuem capacidade técnica-administrativa para proteção dos dados;

- Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever a adoção de medidas de segurança para transmissão e armazenamento dos dados, entre outros requisitos;

- Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade de negócios:

    - tratamento previsto para mitigar os efeitos dos incidentes relevantes e da interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem;

    - prazo estipulado para reinício ou normalização das atividades ou dos serviços relevantes interrompidos; e

    - comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configuram situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades.

Além disso, podemos citar a **Circular Susep nº 638/2021**, que prevê os requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPC), sociedades de capitalização e resseguradores locais ("supervisionadas"), contra ameaças e ataques cibernéticos. A norma impõe às supervisionadas o dever de gestão do risco cibernético, que deve estar em conformidade com seu Sistema de Controles Internos (SCI) e com a Estrutura de Gestão de Riscos (EGR).

No setor financeiro, conforme as diretrizes da Diretiva 2016/1148 da União Europeia, além dos elementos intersetoriais, será necessário mensurar a sua importância sistêmica do mercado com base nos ativos totais ou na razão entre ativos totais/PIB.

Mercado de Valores:

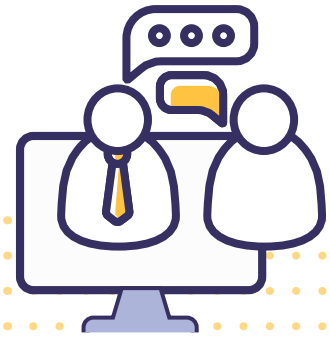
A **Resolução CVM 35** estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários, revogando, entre outras normas, a Instrução CVM nº 612, de 21 de agosto de 2019. Em seu artigo 46, a norma prevê que o intermediário deve comunicar, tempestivamente, aos seus órgãos de administração e à SMI a ocorrência de incidentes de segurança cibernética relevantes.

A comunicação deverá incluir:

- Descrição do incidente, incluindo indicação do dado ou informação sensível afetada;
- Avaliação sobre o número de clientes potencialmente afetados;
- Medidas já adotadas pelo intermediário ou as que pretende adotar;
- Tempo consumido na solução do evento ou prazo esperado para que isso ocorra;
- Qualquer outra informação considerada importante.

Aqui, a Diretiva 2016/1148 da UE prevê que a Autoridade Europeia dos Valores Mobiliários e dos Mercados desempenha também papel de supervisão direta de determinadas entidades, a exemplo das agências de notação de risco e os repositórios de transações, que devem ser observadas no momento de análise do dano proveniente de um incidente.

Telecomunicações:



Resolução nº 740/2020 da Agência Nacional de Telecomunicações

A **Resolução nº 740/2020**, que aprovou o Regulamento de Segurança Cibernética aplicada ao Setor de Telecomunicações, trata, em seus artigos 9 e 17, das medidas a serem adotadas em caso de ocorrência de incidente de segurança.

Segundo o artigo 9º, a prestadora deverá notificar à Agência e comunicar às demais prestadoras e aos usuários, conforme o caso e sem prejuízo de outras obrigações legais de comunicação, os incidentes relevantes que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários.

O artigo 17, por sua vez, estabelece que a notificação do incidente relevante deve incluir:

- Análise da causa e do impacto
- Ações de mitigação adotadas, conforme o caso

Cabe ao GT-Ciber dispor sobre os aspectos de forma e procedimento para a notificação de que trata o artigo 17, observando o disposto no artigo 24 do Regulamento. De acordo com o **Despacho Decisório nº 49/2021/COQL/SCO**, o dever de comunicação aos usuários (art. 9º do R-Ciber) será considerado atendido "com a notificação ao titular de dados para cumprimento da Lei Geral de Proteção de Dados (LGPD)".

A notificação à Autoridade Nacional de Proteção de Dados (ANPD) não supre a necessidade de notificação da Anatel; e sempre que houver notificação de consumidor como titular de dados para fins de atendimento à LGPD, a Anatel deverá ser notificada.

Quanto à forma de realização da notificação, ela deverá ser feita via SEI, com a criação de área específica para tratamento dos processos.

O prazo para notificação preliminar é de 2 dias úteis, contados da data do conhecimento do incidente. Há, ainda, prazo adicional de 60 dias para atendimento ao artigo 17, § 1º, o qual determina que a notificação à Agência deverá incluir análise da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso.

Diretiva 2009/140/EC do Parlamento Europeu e Conselho

A **Diretiva 2009/140/EC** trata do quadro regulamentar comum para redes e serviços de comunicações eletrônicas no âmbito da União Europeia. Em seu artigo 13a, que lida especificamente com segurança e integridade das redes, é estabelecido que os Estados-membros devem assegurar que as empresas adotem medidas técnicas e organizacionais adequadas para gerir adequadamente os riscos que comunicações eletrônicas representam para a segurança das redes e dos serviços.

Essas medidas devem assegurar um nível de segurança adequado, prevenindo e minimizando o impacto de incidentes de segurança aos usuários e às redes interconectadas.

Os Estados-membros devem assegurar que empresas notifiquem a autoridade reguladora nacional competente no momento da ocorrência de uma violação de segurança ou perda de integridade do sistema.

Dessa forma, a entidade reguladora nacional deverá informar às entidades reguladoras de outros Estados-membros e à Agência Europeia para a Segurança das Redes e da Informação (ENISA). Também deverá ser informado ao público e exigido que as empresas façam essa comunicação sempre que a violação colocar em risco os interesses da sociedade.

As entidades reguladoras nacionais deverão anualmente apresentar à Comissão e à ENISA um relatório de síntese sobre as notificações recebidas e as medidas tomadas em conformidade.

Seguros Privados:

Deliberação 171/2015 da Superintendência de Seguros Privados

De acordo com a **Deliberação 171/2015**, nos contratos de serviços relacionados ao provimento, gerenciamento e suporte de infraestrutura computacional de TI, deverá constar cláusula que exija a existência de estrutura de tratamento de incidentes de segurança computacional por parte do prestador (art. 17, *caput*).

Em referência a esses contratos, cabe à Etir (Equipes de Tratamento de Incidentes de Redes) supervisionar o tratamento de incidentes de segurança computacional para o fiel cumprimento das suas atribuições (art. 17, parágrafo único). Ainda, a Etir tem autonomia para tomar ações emergenciais em resposta aos incidentes de segurança computacional (art. 18).

Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados e as orientações da Autoridade Nacional de Proteção de Dados

A ANPD (Autoridade Nacional de Proteção de Dados) recomenda que, em caso de incidente de segurança envolvendo dado pessoal, o agente de tratamento deva avaliar o risco, considerando:

- Natureza, categoria e quantidade de titulares afetados;
- Categoria e quantidade de dados afetados; e
- Consequências concretas e prováveis.

O agente de tratamento deverá comunicar ao Encarregado pela Proteção de Dados Pessoais (art. 5º, VIII da LGPD); e, em se tratando de operador, também comunicar o ocorrido ao controlador.

A ANPD e os titulares de dados também deverão ser comunicados em caso de risco ou dano relevante aos titulares (art. 48 da LGPD). Desse modo, será necessário comunicar o incidente ao titular dos dados pessoais sempre que o controlador avaliar internamente que ele possa acarretar risco ou dano relevante, considerando, sob a perspectiva da LGPD:

A probabilidade de risco ou dano relevante para os titulares, que será maior sempre que o incidente envolver: dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes; potencial de ocasionar danos materiais ou morais, como discriminação; violação do direito à imagem e à reputação; fraudes financeiras; e roubo de identidade.

O volume de dados envolvido; o quantitativo de indivíduos afetados; a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente; e a facilidade de identificação dos titulares por terceiros não autorizados.

O prazo para a comunicação, segundo a ANPD, embora pendente de regulamentação, é de 2 dias úteis, a partir da ciência do incidente.

Caberá ao agente de tratamento elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, a fim de cumprir o princípio da responsabilização e da prestação de contas (art. 6º, X, da LGPD).

Quanto às informações que devem estar contidas na comunicação pelo agente de tratamento, além do previsto no § 1º do artigo 48 da LGPD, a ANPD recomenda que haja:

Identificação e dados de contato de entidade ou pessoa responsável pelo tratamento; Encarregado de Proteção de Dados Pessoais; ou outra pessoa de contato;

Indicação se a notificação é completa ou parcial. Nesse último caso, destacar se a comunicação é preliminar ou complementar; e

Informações sobre o incidente de segurança de dados pessoais, incluindo:

- Data e hora da detecção;
- Data e hora do incidente e sua duração;
- Circunstâncias em que a violação de segurança de dados pessoais ocorreu, como perda, roubo, cópia, vazamento, entre outros;
- Descrição dos dados pessoais e das informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;
- Resumo do incidente, com indicação da localização física e meio de armazenamento;
- Possíveis consequências e efeitos negativos sobre os titulares afetados;
- Medidas de segurança, técnicas e administrativas, preventivas tomadas pelo controlador;
- Resumo das medidas implementadas para controlar os possíveis danos;
- Possíveis problemas de natureza transfronteiriça; e
- Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir danos.

É importante ressaltar que os controladores devem ser cautelosos, realizando a comunicação de forma clara e concisa, mesmo nos casos de dúvida sobre a relevância dos riscos e danos.

General Data Protection Regulation (GDPR)

O artigo 33 do GDPR trata do dever de notificação de violação de dados pessoais à Autoridade Supervisora, que deve ocorrer sem demora injustificada e, sempre que possível, até 72 horas após o agente ter tomado conhecimento da sua ocorrência. Em caso de atraso, a notificação deve vir acompanhada dos motivos que o ocasionaram.

A notificação deverá ser feita sempre que a violação de dados pessoais for suscetível de resultar em risco para direitos e liberdades dos titulares afetados, devendo conter, pelo menos: descrição da natureza da violação dos dados pessoais (incluindo informações sobre dados pessoais afetados e suas categorias, bem como número aproximado de titulares afetados e categorias); informações de contato do Encarregado ou outro ponto de contato na organização; possíveis consequências resultantes da violação; medidas adotadas e propostas pelo agente para reparar a violação ou atenuar seus efeitos.

CRÉDITOS

SÓCIOS

José Roberto Opice Blum
Renato Opice Blum
Marcos Gomes da Silva Bruno
Rony Vainzof
Camilla Jimene
Caio César Carvalho Lima
Danielle Serafino
Juliano S. de Albuquerque Maranhão
Ricardo Campos
Henrique Fabretti Moraes

CONTEÚDO JURÍDICO

Adriana Cardoso de Moraes Cansian
Caio César Carvalho Lima
Florence Terada
Giovana Figueiredo Peluso Lopes
Yasmin Brandão

REVISÃO

Rony Vainzof
Caio César Carvalho Lima
Yasmin Brandão

COORDENAÇÃO EDITORIAL

Yasmin Brandão

ARTE E DIAGRAMAÇÃO

Paola Cosentino

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF