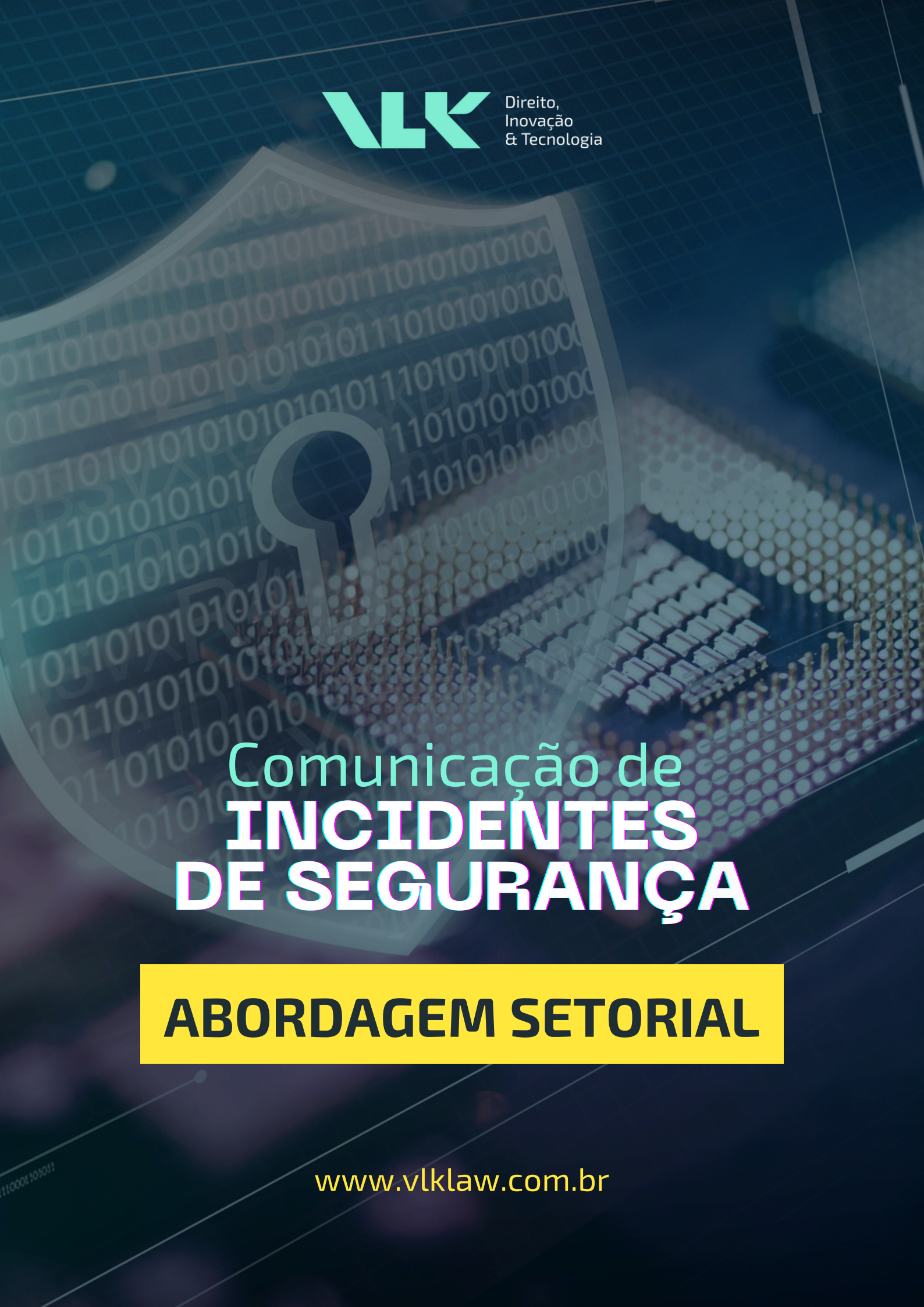

VLK
Direito,
Inovação
& Tecnologia
Comunicação de
INCIDENTES
DE SEGURANÇA
ABORDAGEM SETORIAL
www.vlklaw.com.br

APRESENTAÇÃO

Incidentes de segurança da informação são uma realidade cada vez mais presente e desafiadora para setores altamente regulados como financeiro, saúde, telecomunicações, seguros e energia. A resposta adequada a esses eventos não se limita à contenção dos danos internos; em muitos casos, exige comunicação formal aos órgãos reguladores, dentro de prazos e critérios bem definidos.

Este material foi desenvolvido para fornecer guia preciso sobre quando e como comunicar incidentes aos reguladores setoriais. Aqui, você encontrará informações essenciais sobre o que configura incidente relevante, quais são as exigências normativas para cada setor e quais prazos devem ser cumpridos para mitigar riscos legais e sanções.

Nosso objetivo é simplificar a complexidade regulatória, oferecendo panorama claro das obrigações de comunicação e das melhores práticas para garantir conformidade e transparência. Este documento complementa o E-Book sobre Comunicação de Incidentes de Segurança, lançado em junho de 2024 pelo VLK Advogados e que apresenta infográficos interativos; perguntas e respostas; e a visão da Autoridade Nacional de Proteção de dados sobre o tema, de acordo com suas Notas Técnicas.

Com abordagem prática e orientada para a realidade dos negócios, este Guia ajudará sua organização a agir com segurança e previsibilidade no tratamento de incidentes, protegendo dados, reputação e a continuidade dos negócios.

Bons estudos!

VLK Advogados

ÍNDICE

Direito,
Inovação
& Tecnologia

1) SETOR FINANCEIRO

Entes Reguladores

Banco Central do Brasil (BCB), incluindo o Conselho Monetário Nacional (CMN), e Comissão de Valores Mobiliários (CVM).

1. Resolução n° 4893 (CMN)

Resolução CMN n° 4.893, de 26/02/2021, atualizada em fevereiro de 2024, aborda os requisitos mínimos da Política de Segurança Cibernética e Contratação de Serviços em Nuvem pelas instituições autorizadas a funcionar pelo Banco Central.

PRINCIPAIS ASPECTOS

O inciso III do art. 20 da Resolução estabelece que, entre os procedimentos para gerenciamento de riscos a serem adotados pelas instituições reguladas, está o dever de comunicação tempestiva ao BCB sobre a ocorrência de incidentes relevantes para as atividades da instituição, bem como sobre interrupções de serviços essenciais que configurem uma situação de crise para a instituição financeira. Além disso, determina a obrigação de informar as providências adotadas para a retomada das atividades.

2. Resolução n° 1/2020 (BCB)

Resolução BCB n° 1, de 12.08.2020 ("Regulamento do Pix").

Instrução Normativa BCB n° 412/2023 ("Procedimentos operacionais para a comunicação aos titulares de dados pessoais em caso de ocorrência de incidente de segurança").

PRINCIPAIS ASPECTOS

Os participantes do Arranjo Pix que forneçam contas aos Titulares deverão comunicá-los da ocorrência de incidentes envolvendo os seus dados, ainda que não seja a Instituição responsável pelo incidente e mesmo que o incidente de segurança não acarrete risco ou dano relevante aos titulares, conforme expressamente previsto no inciso VIII do art. 32 da Resolução do BCB, em sua redação atualizada pela Resolução BCB nº 402/2024.

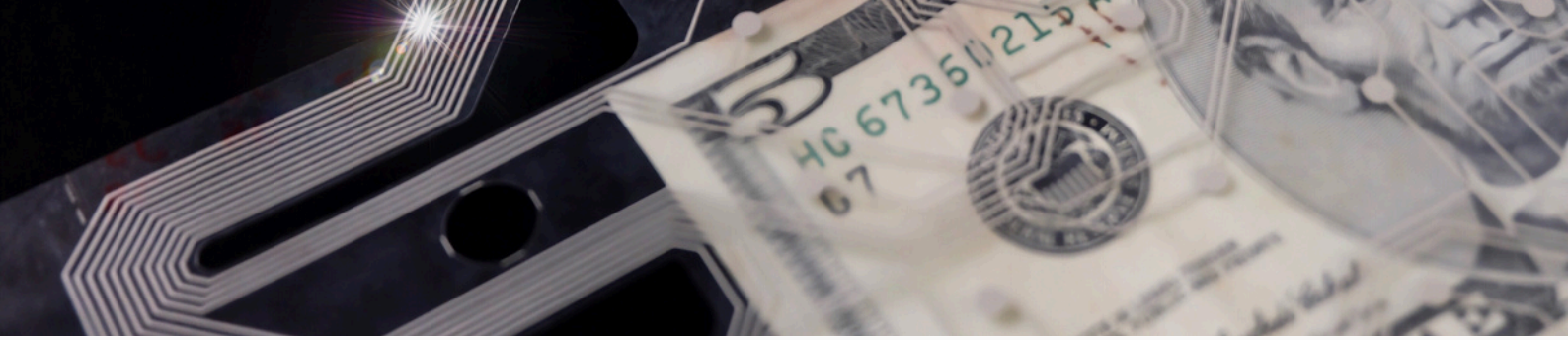
Os procedimentos operacionais relativos à comunicação, estes foram estabelecidos pela Instrução Normativa BCB n° 412/2024, a qual estabelece que:
(i) o Banco Central comunicará as instituições que devem realizar as comunicações por intermédio do Sistema de Correio Eletrônico do Banco Central;
(ii) a comunicação deve ser realizada, ainda que a Chave Pix não esteja mais vinculada a uma conta transacional;
(iii) competirá ao Banco Central definir o prazo de comunicação;
(**iv**) ela deverá utilizar linguagem clara, ser individual e abranger, pelo menos: (a) as informações sobre o incidente; (b) a descrição dos dados pessoais potencialmente afetados e da sua natureza; e (c) os riscos relacionados ao incidente; e
(**v**) as comunicações devem ser armazenadas, já que podem ser requeridas pelo Banco Central a qualquer tempo.

3. Instruções nºs 505 e 612 (CVM)

A Instrução CVM nº 505, de 27.09.2011, estabelece normas e procedimentos a serem observados nas operações realizadas com valores mobiliários, no mercado regulado e ela foi alterada em 2019, com a edição da Instrução CVM nº 612, de 21.08.2019, que incluiu diversos Capítulos com obrigações relacionadas ao tema, como o de Segurança da Informação (Capítulo VII-B) e de Plano de Continuidade dos Negócios (Capítulo VIII-A).

PRINCIPAIS ASPECTOS

Direcionadas aos "intermediários", definidos como as instituições habilitadas a atuarem como integrante do sistema de distribuição, por conta própria e de terceiros, na negociação de valores mobiliários em mercados regulamentados de valores mobiliários, a referuda Instrução da CVM determina o desenvolvimento de Política de Segurança da Informação, com tratamento e controle de dados de clientes, segurança cibernética, e diretrizes para a avaliação "da relevância" dos incidentes de segurança, incluindo as situações em que clientes afetados devem ser comunicados.



Segundo a Instrução, deve ser considerado "relevante" o incidente de segurança cibernético que afete processos críticos de negócios, ou dados ou informações sensíveis, e tenha impacto significativo sobre os clientes.

A Instrução ainda exige o desenvolvimento e implementação de regras, procedimentos e controles internos adequados visando garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade dos dados e informações sensíveis, contemplando as diretrizes para a identificação e classificação dos dados e informações sensíveis, bem como os procedimentos adotados para garantir o registro da ocorrência de incidentes relevantes, suas causas e impactos. Ademais, detalha que dentre as regras, procedimentos e controles é fundamental existir:

(I) a proteção das informações de cadastro e de operações realizadas pelo cliente contra acesso ou destruição não autorizados, vazamento ou adulteração;

(II) a concessão e administração de acessos individualizados a sistemas, bases de dados e redes; e

(III) segregação de dados e controle de acesso, de forma a prevenir o risco de acesso não autorizado, de adulteração ou de mau uso das informações. .

Por fim, determina que intermediário deve manter em sua página na rede mundial de computadores orientações para seus clientes sobre suas principais práticas de segurança das informações, além de estabelecer regras próprias para Segurança Cibernética (art. 35-H)

No que toca à comunicação de incidente, a Instrução CVM estabelece que o intermediário deve comunicar, tempestivamente, aos seus órgãos de administração e à SMI (Superintendência de Relações com o Mercado de Intermediários) a ocorrência de incidentes de segurança cibernética relevantes.

Na comunicação de incidentes, segundo o art. 35-I, são exigidas as seguintes informações do intermediário:

(I) a descrição do incidente, incluindo indicação do dado ou informação sensível afetada;

(II) avaliação sobre o número de clientes potencialmente afetados;

(III) medidas já adotadas pelo intermediário ou as que pretende adotar;

(IV) tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e V – qualquer outra informação considerada importante.

Já no relatório que deve ser encaminhado à SMI, a Instrução determina seu conteúdo mínimo, qual seja:

(I) descrição do incidente e das medidas tomadas, informando o impacto gerado pelo incidente sobre a operação da instituição e seus reflexos sobre os dados dos clientes; e

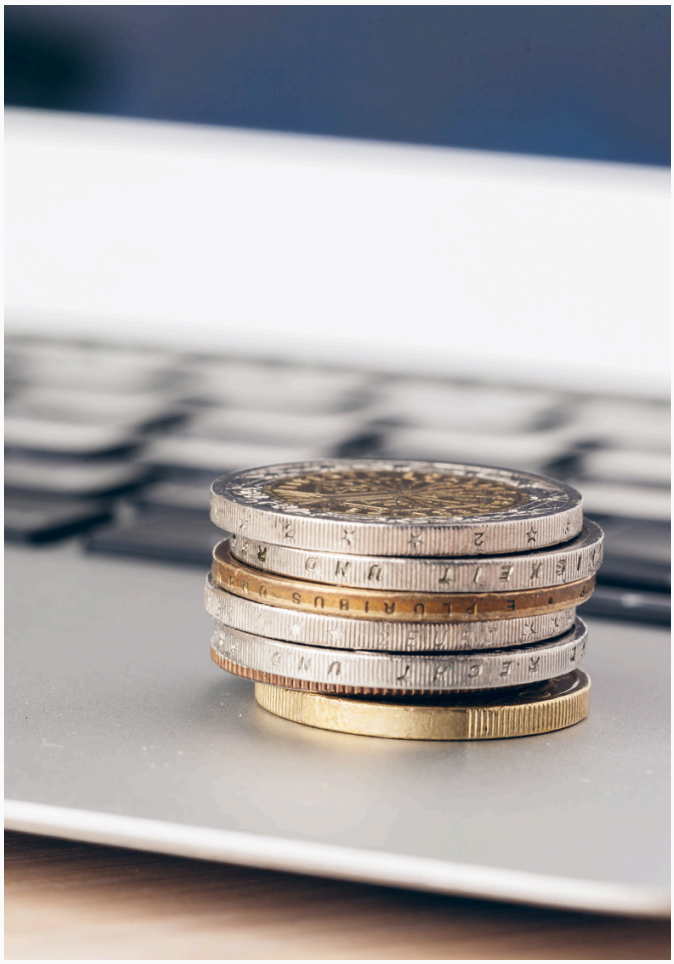
(II) os aperfeiçoamentos de controles identificados com o objetivo de prevenir, monitorar e detectar a ocorrência de incidentes de segurança cibernética, se for o caso, além de cópias a) das comunicações realizadas com seus clientes, se houver; e b) dos relatórios internos de investigação produzidos pelo intermediário ou por terceiros sobre a análise do incidente e as conclusões dos exames efetuados.

4. Lei das S/A

Lei das Sociedades por Ações (Art. 157 § 4º da Lei nº 6.404/76)

PRINCIPAIS PONTOS

Determina a necessidade de que os administradores de companhias abertas comuniquem imediatamente à bolsa de valores e divulguem pela imprensa fato relevante ocorrido nos seus negócios, que possa influir, de modo ponderável, na decisão dos investidores do mercado de vender ou comprar valores mobiliários emitidos pela companhia. (art. 157 § 4º da Lei nº 6.404/76). A CVM regulamentou o dispositivo legal pela Resolução CVM nº 44, de 23.08.21.



Apesar de não mencionar expressamente "incidente de segurança" como fato potencialmente relevante, traz como exemplos situações que podem caracterizá-lo, como "início, retomada ou paralisação da fabricação ou comercialização de produto ou da prestação de serviço". Portanto, caso o incidente de segurança tenha o poder de influir, desta maneira, na decisão de investidores, tal obrigação de comunicação deve ser cumprida.

Além disso, companhias globais precisam observar disposições assemelhadas nos demais países em que também estejam listadas, sendo cumulativas as obrigações de comunicação, em regra.

2) SETOR DE SAÚDE

Ente Regulador

Agência Nacional de Vigilância Sanitária (Anvisa) e ANS (não possui disposições regulatórias específicas sobre o tema).

1. Portaria nº 1.184/2023 (Anvisa)

A Portaria nº 1.184/2023 da ANVISA prevê que sejam estabelecidas disposições específicas para a comunicação de incidentes de segurança da informação, especialmente relacionados aos **dispositivos médicos** e à **proteção de dados pessoais**, respectivamente.

PRINCIPAIS ASPECTOS

Os artigos 29 a 31 da Portaria preveem a criação de procedimentos e de plano de resposta a incidentes de segurança, exigindo que os fornecedores de serviços de Tecnologia da Informação e Comunicação demonstrem garantias de medidas de segurança e comuniquem imediatamente qualquer risco ou incidente que possa impactar a proteção dos dados pessoais.

O Artigo 31 determina que a ANVISA estabeleça normas próprias para o gerenciamento de incidentes com dados pessoais, alinhadas com outras políticas de segurança da informação e privacidade, **as quais ainda não foram estabelecidas.**

2. Guia 33 (Anvisa)

O Guia nº 33/2020 publicado pela Anvisa fornece informações para a **"Validação de Sistemas Computadorizados"** e é aplicável aos programas de computador utilizados nas áreas, equipamentos e demais atividades relevantes às Boas Práticas de Fabricação de Insumos e Medicamentos.

PRINCIPAIS ASPECTOS

A **Seção 11.5** do Guia destaca a importância do gerenciamento de incidentes, crucial para garantir respostas rápidas e eficazes, minimizando potenciais interrupções dos serviços e danos aos titulares, com comunicações claras para escalonamento apropriado e notificação às partes relevantes, incluindo autoridades regulatórias quando necessário.

Além disso, a **Seção 11.6** aborda as Ações Corretivas e Preventivas ("CAPA"), com enfoque na implementação de medidas para corrigir não conformidades já ocorridas e prevenir a recorrência dos incidentes de segurança.

A documentação meticulosa de todas as ações e avaliações de eficácia é essencial para manter a conformidade contínua e aprimorar a robustez dos sistemas computadorizados.

3. Guia 38 (Anvisa)

O Guia nº 38/2020, publicado pela Anvisa, traça os "Princípios e práticas de cibersegurança em dispositivos médicos", destacando a importância da colaboração entre fabricantes, prestadores de serviços de saúde, usuários e a própria Anvisa para garantir a segurança dos dispositivos médicos ao longo de seu ciclo de vida.

PRINCIPAIS ASPECTOS

A **Seção 6.5** do Guia aborda a resposta a incidentes de cibersegurança, especificando a necessidade de os fabricantes desenvolverem e manterem processos robustos para avaliar, responder e comunicar incidentes significativos, em colaboração com a Anvisa e outros prestadores de serviços de saúde.

3) SETOR DE TELECOMUNICAÇÕES

Ente Regulador

Agência Nacional de Telecomunicações (Anatel)

1. Normas

Resolução nº 740/2020, da Anatel, a qual aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações.

Resolução nº 767/2024, que alterou a Resolução nº 740/2020.

Despacho Decisório 49/2021/COQL/SCO.

PRINCIPAIS ASPECTOS

O Regulamento de Segurança Cibernética prevê, além do dever de estabelecer a necessidade de Política de Segurança Cibernética que aborde o procedimento de resposta a incidentes (art. 14), determina as situações em que a comunicação de incidentes de segurança à Anatel é obrigatória, englobando as siações em que:

O Incidente for de comunicação obrigatória à ANPD (art. 2°-C); e

For Incidente relevante, aqui entendido aqueles que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários, hipótese em que os usuários também devem ser notificados. Nessas hipóteses, as comunicações devem incluir análise da causa e do impacto, bem como ações de mitigação adotadas (art. 9° c/c art. 17).

A forma e o procedimento de comunicações devem ser definidos pelo GT-Ciber da Anatel (art. 17, §3°), o qual por meio do Despacho Decisório 49/2021/COQL/SCO, estabeleceu que as comunicações realizadas para a Anisa devem ser feitas pelo SEI, em até 2 dias úteis, ainda que de forma preliminar, podendo ser complementadas em até 60 dias. Ainda, o Despacho Decisório lista situações exemplificativas consideradas como incidentes relevantes:

(i) Vazamentos de dados (dados corporativos ou de clientes);

(ii) Ransomwares bem-sucedidos; comprometimentos decorrentes de Ameaças Persistentes Avançadas (Advanced Persistent Threat - APT);

(iii) Ataques de Negação de Serviço, considerando os seguintes parâmetros de tráfego e de quantidade de pacotes por segundo: igual ou superior a 50Gbps ou a 20Mbps; problemas de roteamento (sequestro de prefixos, vazamento de rotas e/ou erros de configuração) que venham a ocasionar impacto na entrega de serviços aos clientes das prestadoras, órgãos ou entidades que operam na Internet; e

(iv) Indisponibilidade de serviço causada por incidente de segurança cibernética.

Outro ponto relevante constante do Regulamento é a obrigação de avaliação prévia de fornecedores em relação a conformidade com as regras do Regulamento e a condução de auditorias independentes periódicas. O processo deve ser documento e apresentado à Anatel mediante solicitação. A Resolução nº 767/2024 aprofundou a obrigação, requerendo a inclusão da análise de serviços de computação em nuvem, bem como dos impactos operacionais e financeiros da dependência desses serviços.

Por fim, as prestadoras devem compartilhar entre si informações sobre incidentes relevantes de forma sigilosa e não discriminatória, podendo optar pelo anonimato. Este compartilhamento, cujos detalhes também são estabelecidos pelo GT-Ciber, visam incentivar a participação de todas as prestadoras e buscar coordenação com outras entidades relevantes (art. 18).

Além do Regulamento, a Anatel publicou, em outubro de 2023, Guia Orientativo de Segurança Cibernética para Prestadoras de Serviços de Telecomunicações, no qual são apresentadas medidas de orientação para a proteção das redes, sistemas e dados diante das ameaças cibernéticas sofridas pelas empresas de telecomunicações.

Especificamente a respeito de incidentes, o Guia traz recomendações valiosas, como: razões para se criar plano de resposta a incidentes, designação de pessoal para gerenciar tratamento de incidentes e manutenção de informações de contato para os relatos de incidentes.

4) SETOR DE SEGUROS

Ente Regulador

Superintendência de Seguros Privados (Susep)

1. Normas

Circular SUSEP nº 638/2021, que dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais.

PRINCIPAIS ASPECTOS

As Supervisionadas têm a obrigatoriedade de possuir e manter atualizados processos, procedimentos e controles para, de maneira proativa: a) identificar e reduzir vulnerabilidades e b) detectar, responder e se recuperar de incidentes – o que deverá ser formalizado no Plano de Continuidade de Negócios (PCN) da companhia (artigo 5º).

As Supervisionadas devem implementar Plano de Ação e de Resposta a Incidentes (conforme artigo 6° e ss), abrangendo, pelo menos:

- As ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;
- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e
- A área responsável pelo registro e controle dos efeitos de incidentes relevantes.

As Supervisionadas devem realizar a comunicação de Incidentes relevantes para a Susep em até 5 (cinco) dias úteis (art. 8°), incluindo:

- A extensão do dano causado;
- As ações em curso para regularização completa da situação; e
- Os respectivos responsáveis e prazos, se aplicável.

O QUE SÃO INCIDENTES RELEVANTES?

Eventos adversos, decorrentes ou não de atividade maliciosa, que, conforme parâmetros definidos pela supervisionada, comprometam substancialmente:
a) a confidencialidade, integridade ou disponibilidade de dados relevantes; ou
b) serviços relevantes de processamento ou armazenamento de dados (art. 2°, IV).

E DADOS RELEVANTES?

São dados pessoais, conforme definido na legislação em vigor, dados relativos a clientes ou a processos críticos de negócio, bem como quaisquer outros dados ou informações consideradas sensíveis de acordo com as diretrizes estabelecidas pela supervisionada (art. 2°, VI).

O Regulamento prevê o dever das reguladas em comunicar incidentes às partes afetadas, incluindo clientes (art. 5°, VII). Não existem, no entanto, qualificação para incidentes comunicáveis, e prazo previsto para a realização dessa comunicação, razão pela qual, a princípio, tem sido aplicado, na prática, o prazo de 5 (cinco) dias úteis, que é válido para a comunicação de incidentes relevantes à Susep.

As Supervisionadas têm, ainda, a obrigatoriedade de documentar em relatório anual a efetividade da prevenção e tratamento de incidentes feitos pela companhia durante o referido ciclo.

O RELATÓRIO DEVE CONTER, NO MÍNIMO:

a) a descrição dos incidentes relevantes detectados, com detalhamento das respectivas causas, efeitos e respostas adotadas;

b) os dados estatísticos referentes à totalidade dos incidentes detectados, contemplando sua quantidade e principais causas e efeitos;

c) os resultados dos testes relativos aos cenários previstos no Plano de Continuidade de Negócios (PCN); e

d) a descrição das principais vulnerabilidades identificadas e das ações adotadas pela companhia para seu tratamento.

Todas as versões do relatório anual e demais documentos que comprovem o atendimento ao disposto na Circular 638 **devem ser armazenados pela companhia pelo prazo mínimo de 05 (cinco) anos**, conforme Circular nº 605/2020.

4) SETOR DE ENERGIA

Ente Regulador

Agência Nacional de Energia Elétrica (ANEEL)

1. Normas

Resolução ANEEL nº 24/2021
Resolução ANEEL n° 964/2021

PRINCIPAIS ASPECTOS

Conforme artigo 4° da Resolução 964, é dever do agente de tratamento adotar, como parte de sua Política de Cibersegurança, mecanismos e objetivos de segurança cibernética para prevenir, detectar, responder e reduzir a vulnerabilidade a incidentes, e se recuperar deles, bem como os parâmetros a serem utilizados na avaliação da relevância dos incidentes para fins de comunicação à equipe de coordenação setorial.

A regulada deve, ainda, realizar "o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes de maior impacto para suas atividades, abrangendo inclusive informações recebidas de empresas prestadoras de serviços a terceiros".

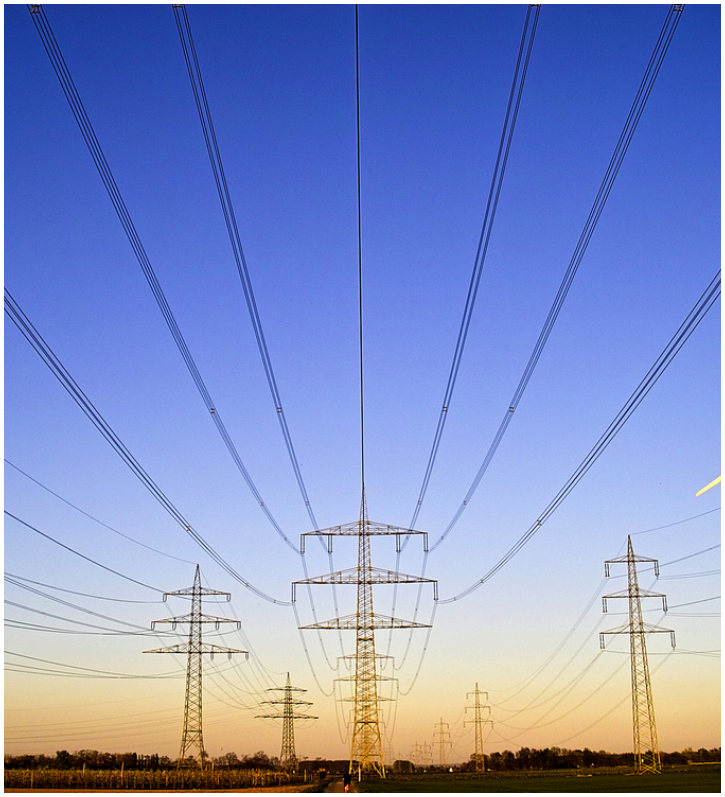
O Regulamento prevê a obrigação de comunicação para a ANEEL de Incidentes de maior impacto (art. 6°) da Resolução 964.

O QUE SÃO INCIDENTES?

São descritos como "a ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso" (art. 2°, I)

QUAIS INCIDENTES SÃO CONSIDERADOS COMO DE MAIOR IMPACTO?

Aqueles assim estabelecidos com base na classificação de severidade que consta do processo de gestão de riscos de segurança da informação do agente (art. 2°, II)



Por fim, como pontuado acima, agentes devem manter registros e enviar para a Aneel ou para a equipe de coordenação setorial designada as seguintes informações sempre que solicitadas:

- Os resultados dos modelos de maturidade aplicados em formato definido pela agência (link), o que inclui a(o): identificação do empreendimento; descrição da ocorrência; avaliação do evento quanto à extensão; impacto – alcance e comprometimento da infraestrutura, perda e integridade da informação; identificação do grau de ameaça do evento relacionado ao grau de vulnerabilidade; relevância do evento de segurança e classificação da vulnerabilidade; avaliação do evento quanto à complexidade de normalização – nível de esforço requerido para normalização; e classificação do evento quanto a frequência da ocorrência.

- Os riscos cibernéticos identificados, com a respectiva forma de tratamento; e

- Os dados das equipes de prevenção, tratamento e resposta a incidentes cibernéticos.

SOBRE NÓS

O VLK Advogados entende o Direito como instrumento para impulsionar a inovação, o sucesso dos negócios e uma sociedade mais próspera e justa.

Participamos ativamente da construção de marcos regulatórios e de centenas de projetos inovadores, o que nos permite antecipar tendências e gerar segurança jurídica para viabilizar negócios nas seguintes áreas:

- Governança Ética e Proteção de Dados
- Inteligência Artificial
- Segurança Cibernética e Resposta a Incidentes
- Economia Criativa, *Legal Marketing* e Propriedade Intelectual
- *Legal Design e Visual Law*
- *Advocacy* e Regulação Estratégica de Tecnologia
- Contencioso Estratégico

contato@vlklaw.com.br

VLK ADV

WWW.VLKLAW.COM.BR