VLK ADV

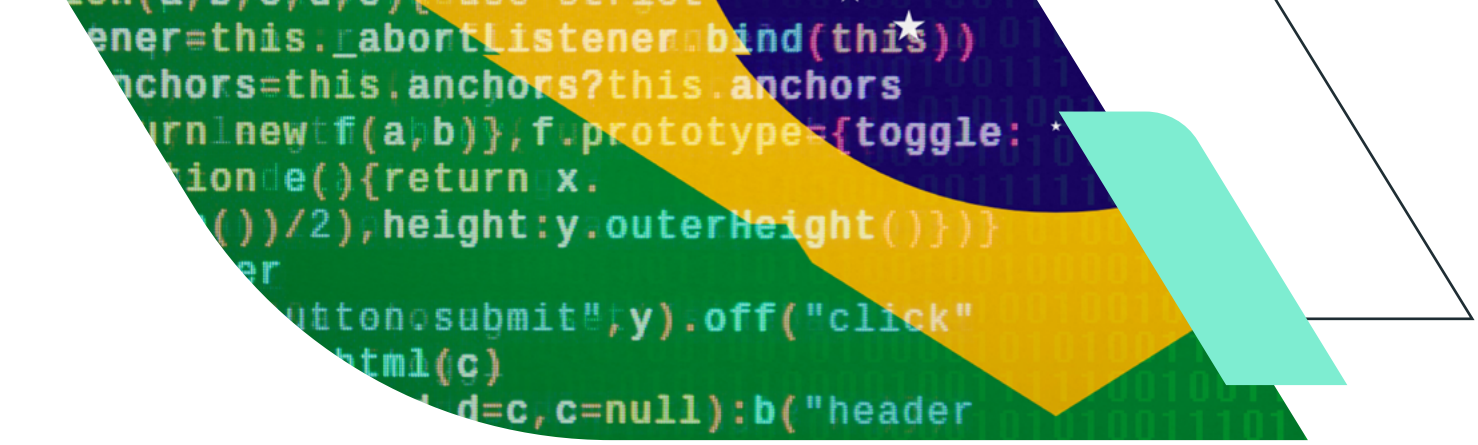
CIBERSEGURANÇA NO BRASIL

CENÁRIO REGULATÓRIO & LEGAL

MAIO 2025

WWW.VLKLAW.COM.BR

INDEX



1. Contextualização do Panorama Brasileiro

Incidentes cibernéticos despontam como preocupação crítica de curto e longo prazo, segundo relatórios mais recentes do Fórum Econômico Mundial. A pauta vai muito além de fraudes e vazamentos de dados: ataques cibernéticos têm potencial para paralisar empresas, instituições e até países inteiros.

O impacto financeiro é alarmante. O custo direto e indireto dos ciberincidentes representa 14% do PIB global por ano (Fórum Econômico Mundial, 2024). No Brasil, esse valor pode chegar a 18% do PIB — o equivalente a R$ 2,3 trilhões, segundo o INCC. Em média, cada incidente custa US$ 4,8 milhões (IBM, 2024). Quando uma empresa de capital aberto sofre um ataque bem-sucedido, independentemente de sua performance anterior, o valor de suas ações tende a cair, em média, 7,5% (Harvard Business Review, 2023).

Diante desse cenário, diversas estratégias vêm sendo apontadas como caminhos para a mitigação de riscos. Entre elas, destacam-se:

- A coordenação nacional de cibersegurança, pois a fragmentação entre diferentes stakeholders leva a respostas lentas e ineficazes diante do volume e da complexidade das ameaças;
- A harmonização regulatória, com a criação de um marco legal claro, equilibrado e baseado em risco, alinhado às melhores práticas internacionais e sem impor custos operacionais proibitivos; e

- A implementação de um programa nacional de conscientização em cibersegurança, voltado a empresas e cidadãos, que também integre o tema aos currículos educacionais, desde o ensino básico até o superior.

No cenário internacional, a movimentação já começou há décadas. A Convenção de Budapeste sobre crimes cibernéticos foi adotada em 2001. A partir da segunda década dos anos 2000, a União Europeia aprovou a diretiva NIS, obrigando os 27 países do bloco a criarem legislações e estruturas nacionais de cibersegurança. Mais recentemente, a UE aprovou a NIS2, elevando ainda mais o nível de exigência. Países como China, Rússia, Japão e Coreia do Sul também desenvolveram leis e órgãos específicos.

No Brasil, apenas em 2023 o país promulgou sua adesão à Convenção de Budapeste. As exigências existentes são, em geral, setoriais e não harmonizadas. Leis como o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Propriedade Industrial e a LGPD, por exemplo, contêm dispositivos relacionados ao tema, assim como regulações específicas para setores como o financeiro, telecomunicações, seguros e saúde. No entanto, falta um corpo normativo comum, além de outros setores sequer contarem com exigências mínimas em cibersegurança.

A ausência de um órgão regulador nacional e intersetorial compromete a implementação de normas transversais, recomendadas pelas boas práticas internacionais. Essa lacuna pode ajudar a explicar por que o Brasil figura entre os países mais atacados do mundo. Sem regras claras, a cibersegurança é frequentemente negligenciada — e os prejuízos só se evidenciam quando já é tarde demais.

Lembrando-se que 98% dos ataques cibernéticos poderiam ser evitados com medidas básicas de higiene digital, como uso de antimalware, atualização de sistemas, autenticação multifator, controle de acessos e governança de credenciais (Microsoft Digital Defense Report, 2022). Ou seja, um órgão central pautando a conscientização de empresas e pessoas, já seria suficiente para evitar boa parte dos incidentes.

Embora a criação de uma estrutura nacional de governança em cibersegurança represente um investimento relevante — e que deve ser analisado com cautela à luz do cenário fiscal atual — os números indicam que, se bem desenhada e executada com foco em eficiência e coordenação, essa medida pode gerar impactos econômicos positivos. Estima-se que a prevenção de apenas 10% dos prejuízos causados por ataques cibernéticos já resultaria em uma economia anual entre R$ 150 e R$ 230 bilhões. Mesmo considerando um custo total estimado em R$ 500 milhões anuais a partir do quinto ano, o potencial de retorno seria muito expressivo, com ganhos da ordem de 300 vezes superiores ao investimento. Sob a ótica governamental, a arrecadação tributária derivada dessa economia superaria os R$ 50 bilhões — o que representaria um retorno fiscal superior a 100 vezes o valor investido. Ainda assim, é essencial que qualquer proposta avance com base em diálogo intersetorial, transparência e racionalização de recursos.

Em outras palavras, cibersegurança deixou de ser uma questão meramente técnica. É uma escolha estratégica e essencial — de líderes, conselhos e, acima de tudo, das nações.

Introdução extraída do artigo:
"Cibersegurança: O Custo de Não Fazer"

2. Normas Gerais

A) LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD – Lei 13.709/18)

Nos termos da LGPD, o tratamento de dados pessoais deve observar a boa-fé e ser pautado por princípios (Art. 6º), como:

- **Segurança:** com a adoção de medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, bem como contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão
- **Prevenção:** mediante a implementação de ações que evitem a ocorrência de danos em decorrência do tratamento;
- **Responsabilização e prestação de contas:** exigindo que o agente demonstre a adoção de medidas eficazes que comprovem o cumprimento das normas de proteção de dados.

O tratamento será considerado **irregular** quando não observar a legislação ou deixar de garantir o nível de segurança que o titular razoavelmente pode esperar, considerando o modo como é realizado, os riscos envolvidos e as técnicas disponíveis à época (Art. 44).

Os agentes de tratamento **devem adotar medidas de segurança, técnicas e administrativas aptas a 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 (Art. 46).

Os **agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação** em relação aos dados pessoais, mesmo após o seu término (Art. 47).

Além disso, e**m caso de incidente de segurança com risco ou dano relevante**, o controlador tem o **dever de comunicar tanto a ANPD quanto o titular afetado** (Art. 48).

B) MARCO CIVIL DA INTERNET (Lei 12.965/14) E SEU DECRETO REGULAMENTADOR (Decreto 8.771/16)

O **Marco Civil** da Internet estabelece, entre seus princípios, a **preservação da estabilidade, segurança e funcionalidade da rede**, por meio de medidas técnicas alinhadas aos padrões internacionais e do estímulo a boas práticas (art. 3º, V).

Além disso, impõe deveres de guarda de registros:

- O **administrador de sistema autônomo** responsável pela conexão deve manter os **registros de conexão** pelo prazo de **1 ano**, sob sigilo e em **ambiente controlado e seguro** (art. 13).
- Os **provedores de aplicações de internet**, quando organizados profissionalmente e com fins econômicos, devem manter os **registros de acesso às aplicações** por **6 meses,** também sob **sigilo** e em **ambiente seguro** (art. 15).

O **Decreto nº 8.771/2016**, por sua vez, regulamenta os **padrões de segurança e sigilo** na guarda, armazenamento e tratamento dos dados pessoais e comunicações privadas, impondo que os provedores adotem medidas como (Art. 13):

- **Controle estrito de acesso** aos dados, com definição clara das responsabilidades e privilégios dos usuários autorizados;
- **Autenticação robusta**, preferencialmente com múltiplos fatores, para individualizar os responsáveis pelos acessos;
- **Inventário detalhado dos acessos**, incluindo momento, duração, identidade do responsável e arquivo acessado;
- **Soluções de proteção à inviolabilidade dos dados**, como encriptação ou medidas de segurança equivalentes.

C) CÓDIGO DE DEFESA DO CONSUMIDOR

Nos termos do **Código de Defesa do Consumidor**, é considerada prática abusiva a colocação no mercado de **produtos ou serviços em desacordo com normas técnicas estabelecidas por órgãos oficiais competentes** ou, na ausência destas, **pela Associação Brasileira de Normas Técnicas – ABNT** (art. 39, VIII).

Isso implica que **empresas que negligenciam a observância de normas técnicas reconhecidas para cibersegurança**, como a **ABNT NBR ISO/IEC 27001** e a **ABNT NBR ISO/IEC 27701, podem ser responsabilizadas por práticas inadequadas ou inseguras**, inclusive no âmbito da defesa do consumidor.

3. Normas Setoriais

A) SETOR DE TELECOMUNICAÇÕES

No setor de telecomunicações, a **Agência Nacional de Telecomunicações (Anatel)** é a entidade responsável por definir diretrizes de **segurança cibernética** aplicáveis às prestadoras de serviços.

O tema é disciplinado principalmente pela **Resolução nº 740/2020**, alterada pela **Resolução nº 767/2024**, que institui o **Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações**. Dentre suas principais exigências, destaca-se a obrigatoriedade de:

- **Estabelecimento de Política de Segurança Cibernética**, com procedimentos de **resposta a incidentes** (art. 14);
- **Comunicação obrigatória à Anatel** de incidentes de segurança considerados relevantes, tais como:
  - Aqueles também reportáveis à ANPD (art. 2º-C);
  - Incidentes que afetem substancialmente a segurança das redes ou dos dados dos usuários (art. 9º e 17), com necessidade de notificação aos usuários e inclusão de análise da causa, impacto e ações de mitigação.

A forma de comunicação deve seguir diretrizes do **GT-Ciber da Anatel**, conforme estabelecido no **Despacho Decisório 49/2021/COQL/SCO**: o incidente deve ser reportado pelo SEI **em até 2 dias úteis**, ainda que de forma preliminar, com complementação em até 60 dias. São exemplos de incidentes relevantes:

- Vazamentos de dados corporativos ou de clientes;
- Ransomwares bem-sucedidos e ameaças persistentes avançadas (APT);
- Ataques de negação de serviço (DDoS) com tráfego igual ou superior a 50Gbps ou 20Mpps;
- Problemas de roteamento com impacto na entrega de serviços;
- Indisponibilidade de serviço causada por incidente cibernético.

O regulamento também impõe **obrigações de avaliação prévia de fornecedores**, inclusive de serviços em nuvem, quanto à conformidade com as regras, exigindo **auditorias independentes periódicas** e documentação do processo, a ser apresentada à Anatel mediante solicitação.

Há ainda a exigência de **compartilhamento de informações sobre incidentes relevantes** entre prestadoras, de forma sigilosa e não discriminatória, inclusive com opção de anonimato, para fins de coordenação com outras entidades (art. 18).

Complementarmente, a Anatel publicou, em outubro de 2023, um **Guia Orientativo de Segurança Cibernética**, com recomendações práticas, como a criação de planos de resposta a incidentes, designação de responsáveis pela gestão desses eventos e manutenção de canais de contato específicos para comunicação de incidentes.

B) SETOR FINANCEIRO

No setor financeiro, as diretrizes sobre segurança cibernética e resposta a incidentes são estabelecidas por **entes reguladores como o Banco Central do Brasil (BCB), o Conselho Monetário Nacional (CMN) e a Comissão de Valores Mobiliários (CVM).**

A **Resolução CMN nº 4.893/2021**, atualizada em 2024, estabelece diretrizes para a política de segurança cibernética e requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem por instituições financeiras, prevendo as seguintes obrigações:

Política de Segurança Cibernética

- Deve ser elaborada, implementada e compatível com o porte, perfil de risco e complexidade da instituição.
- Precisa conter objetivos, controles e procedimentos específicos.
- Revisada anualmente e aprovada pela alta administração.

Plano de Ação e Resposta a Incidentes

- Estabelecer ações preventivas e reativas, com área responsável por registrar efeitos dos incidentes.
- Elaborar relatório anual, incluindo incidentes, testes e efetividade

Comunicação de Incidentes ao BCB

- Incidentes relevantes e interrupções de serviços essenciais devem ser comunicados **tempestivamente**.
- Devem ser informadas também as providências adotadas para a retomada das atividades.

Contratação de Serviços de Nuvem e Processamento de Dados

- Avaliação prévia da empresa contratada e aderência à regulação.
- Responsabilidade integral da instituição pelos serviços contratados.
- Comunicação ao BCB após contratação/alteração de serviços relevantes.
- Exigências adicionais para serviços prestados no exterior.

Designação de Diretor Responsável

- A instituição deve nomear **diretor responsável** pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

No âmbito do **Pix**, a **Resolução BCB nº 1/2020,** a **Resolução BCB nº 402/2024** e a **Instrução Normativa BCB nº 412/2024**, determinam que os participantes que oferecem contas aos titulares **devem comunicá-los diretamente sobre incidentes com seus dados pessoais**, mesmo quando não forem os responsáveis diretos pelo incidente, e ainda que não haja risco ou dano relevante.

A comunicação deve seguir os seguintes critérios operacionais:

- Ser realizada conforme prazo definido pelo BCB, via sistema oficial de correio eletrônico;
- Incluir linguagem clara, individualizada, e conter informações sobre o

incidente, os dados afetados e os riscos envolvidos;
- Ser arquivada, estando disponível ao BCB a qualquer tempo.

Já no mercado de capitais, a **Instrução CVM nº 505/2011**, com as alterações da **Instrução CVM nº 612/2019**, impõe obrigações aos intermediários de valores mobiliários quanto à **segurança da informação e continuidade de negócios**. A norma exige a adoção de **Política de Segurança da Informação**, abrangendo:

- Tratamento e controle de dados de clientes;
- Avaliação da **relevância de incidentes de segurança**;
- Comunicação aos clientes afetados, quando o incidente envolver **processos críticos de negócio** ou **dados sensíveis**, com **impacto significativo**.

C) SETOR DE ENERGIA

No setor de energia elétrica, a **Agência Nacional de Energia Elétrica (ANEEL)** estabelece, por meio das **Resoluções nº 24/2021** e **nº 964/2021**, obrigações específicas relacionadas à **segurança cibernética**.

De acordo com o **art. 4º da Resolução nº 964/2021**, os agentes regulados devem adotar mecanismos de prevenção, detecção, resposta e recuperação de incidentes como parte integrante de sua **Política de Cibersegurança.** Essa política também deve prever critérios para avaliar a relevância dos incidentes e orientar a comunicação à equipe de coordenação setorial designada.

É obrigatória a **comunicação à ANEEL dos incidentes considerados de maior impacto** (art. 6º), os quais devem ser registrados, analisados em termos de causa e impacto, e acompanhados de medidas de controle de efeitos — incluindo dados fornecidos por **prestadores de serviços terceirizados**.

A norma define **incidente cibernético** como qualquer evento que comprometa, real ou potencialmente, a **disponibilidade, integridade, confidencialidade ou autenticidade de sistemas** de informação ou dos dados neles tratados, inclusive **tentativas de exploração de vulnerabilidades** que configurem violação de normas ou políticas internas (art. 2º, I).

Já os incidentes de maior impacto são aqueles classificados com **alta severidade**, conforme a matriz de risco de cada agente (art. 2º, II).
Adicionalmente, os agentes devem manter registros detalhados e fornecer à ANEEL, mediante solicitação, informações como:

- Resultados dos modelos de maturidade aplicados, incluindo extensão e impacto dos eventos, grau de ameaça, relevância, vulnerabilidade, esforço de normalização e frequência;
- Riscos cibernéticos identificados e respectivas formas de tratamento;
- Dados das equipes responsáveis pela prevenção, tratamento e resposta a incidentes cibernéticos.

D) SETOR DE SAÚDE

No setor da saúde, a **Agência Nacional de Vigilância Sanitária (Anvisa)** é o principal ente regulador com disposições voltadas à segurança da informação, especialmente no que se refere a **dispositivos médicos e proteção de dados pessoais**. A **Agência Nacional de Saúde Suplementar (ANS)**, por sua vez, **ainda não possui regulação específica sobre o tema**.

A **Portaria Anvisa nº 1.184/2023** determina, entre os **arts. 29 a 31**, que fornecedores de serviços de tecnologia da informação

e comunicação adotem **procedimentos e plano de resposta a incidentes de segurança**, devendo comprovar a existência de **garantias de segurança** e **comunicar imediatamente** qualquer risco ou incidente que possa afetar dados pessoais. A norma também prevê que a Anvisa deverá editar r**egulamentação própria para o gerenciamento de incidentes envolvendo dados pessoais**, ainda pendente de publicação.

O **Guia nº 33/2020** da Anvisa, voltado à **validação de sistemas computadorizados** aplicados nas Boas Práticas de Fabricação, trata da **gestão de incidentes** (Seção 11.5), ressaltando a importância de respostas rápidas, notificações claras às autoridades competentes e comunicação escalonada em caso de impacto relevante. Na **Seção 11.6**, são abordadas as **ações corretivas e preventivas (CAPA)**, com foco na **documentação rigorosa** das medidas adotadas e na **avaliação da eficácia**, assegurando melhoria contínua e robustez dos sistemas.

Já o **Guia nº 38/2020**, que trata dos **princípios e práticas de cibersegurança em dispositivos médicos**, estabelece diretrizes para que os f**abricantes desenvolvam processos sólidos para avaliação, resposta e comunicação de incidentes cibernéticos**, em colaboração com a Anvisa e os prestadores de serviços de saúde, ao longo de todo o ciclo de vida dos dispositivos (Seção 6.5).

E) SETOR DE SEGUROS

No setor de seguros, a **Superintendência de Seguros Privados (Susep)** regulamenta as exigências de **segurança cibernética** por meio da **Circular SUSEP nº 638/2021**, aplicável a seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais.

A norma determina que as supervisionadas mantenham **processos, procedimentos e controles atualizados** para **identificar e reduzir vulnerabilidades**, bem como **detectar, responder e se recuperar de incidentes cibernéticos**, o que deve estar formalizado no **Plano de Continuidade de Negócios (PCN)** da companhia (art. 5º)

É obrigatória a implementação de um **Plano de Ação e de Resposta a Incidentes**, contendo:

- Ações de adaptação da estrutura organizacional às diretrizes da política de segurança cibernética;
- Procedimentos, controles e tecnologias para prevenção e resposta a incidentes;
- Designação da área responsável pelo registro e acompanhamento dos efeitos de incidentes relevantes (arts. 6º e seguintes).

Incidentes relevantes são definidos como eventos adversos — maliciosos ou não — que comprometam substancialmente a **confidencialidade, integridade ou disponibilidade de dados ou serviços relevantes** (art. 2º, IV). Já **dados relevantes** abrangem dados pessoais (conforme a LGPD), informações de clientes, processos críticos e quaisquer outros definidos como sensíveis pelas próprias supervisionadas (art. 2º, VI).

A comunicação desses incidentes à **Susep deve ocorrer em até 5 dias úteis** (art. 8º) e deve conter:

- A extensão do dano;
- As ações em curso para correção;
- Os responsáveis e prazos, quando aplicável.

Além da Susep, há também o **dever de notificação às partes afetadas**, incluindo os **clientes,** embora a norma não estipule prazo específico nem defina claramente os tipos de incidentes que exigem tal comunicação (art. 5º, VII). Na prática, tem-se adotado o mesmo **prazo de 5 dias úteis** previsto para o envio à Susep.

Por fim, as supervisionadas devem elaborar **relatório anual** sobre a **efetividade das ações de prevenção e resposta a incidentes**, com base nas ocorrências e medidas adotadas no período.

4. Serviços Essenciais e Infraestruturas Críticas

As **infraestruturas críticas** e os **serviços essenciais** representam áreas estratégicas para a **segurança nacional**, o funcionamento da sociedade e a continuidade de atividades econômicas vitais. A regulação sobre o tema encontra-se nos seguintes marcos normativos no Brasil:

A **Política Nacional de Segurança de Infraestruturas Críticas**, instituída pelo **Decreto nº 9.573/2018**, atribui ao **Gabinete de Segurança Institucional da Presidência da República (GSI/PR)** a competência para acompanhar os temas relacionados às infraestruturas críticas no âmbito da administração pública federal (art. 2º).

Complementarmente, a **Estratégia Nacional de Segurança de Infraestruturas Críticas**, prevista no **Decreto nº 10.569/2020**, reforça o papel estratégico de setores como **comunicações, energia, transportes, finanças e águas**, cuja interrupção ou destruição pode gerar impactos sociais, econômicos, políticos ou à própria **segurança e soberania nacionais**. A estratégia destaca a atuação do GSI na **identificação e análise de riscos**, em cooperação com entes públicos e privados.

Já a **Lei nº 7.783/1989** define os **serviços e atividades essenciais**, que devem ser mantidos mesmo em contextos de greve, dada sua importância para o atendimento das **necessidades inadiáveis da comunidade.** O rol inclui, entre outros:

- Abastecimento de água, energia elétrica, combustíveis e gás;
- Assistência médica e hospitalar;
- Distribuição de medicamentos e alimentos;
- Telecomunicações e transporte coletivo;
- Processamento de dados ligados a serviços essenciais;
- Controle de tráfego aéreo, atividades bancárias e portuárias;
- Atividades médico-periciais e funerárias.

A legislação determina que **sindicatos e empregadores mantenham equipes mínimas em operação durante paralisações,** de forma a evitar prejuízos irreversíveis e garantir a continuidade dos serviços essenciais (arts. 9º e 11).

5. Crimes Cibernéticos

A legislação penal brasileira prevê sanções específicas para crimes cometidos no ambiente digital, com foco na **proteção de dispositivos informáticos, dados e sistemas** contra invasões e fraudes.

INVASÃO DE DISPOSITIVO INFORMÁTICO (ART. 154-A DO CÓDIGO PENAL)

É crime **invadir dispositivo informático de uso alheio**, com ou sem conexão à rede, com a finalidade de **obter, adulterar, destruir dados ou instalar vulnerabilidades**, sem autorização do usuário.

- **Pena:** reclusão de **1 a 4 anos**, e multa.
- Incorre na mesma pena quem **produz, vende ou distribui programas ou dispositivos** com o intuito de permitir essa prática.
- A pena é aumentada de **1/3 a 2/3** se a invasão causar **prejuízo econômico.**
- Se a invasão resultar na obtenção de **comunicações privadas, segredos comerciais ou industriais, informações sigilosas ou controle remoto do dispositivo**, a pena é de **2 a 5 anos**, e multa.
- Haverá **agravamento de 1/3 a 2/3** se os dados obtidos forem **divulgados, comercializados ou transmitidos** a terceiros.

FRAUDE ELETRÔNICA (ART. 171, §2º-A E §2º-B DO CÓDIGO PENAL)

Trata-se da prática de **fraude para obtenção de vantagem ilícita**, com uso de **redes sociais, ligações, e-mails ou outros meios digitais** que induzam a vítima ou terceiros a erro.

- **Pena:** reclusão de **4 a 8 anos**, e multa.
- A pena é aumentada de 1/3 a 2/3 se o crime for praticado com **uso de servidores no exterior.**

FURTO DIGITAL (ART. 155, §4º-B DO CÓDIGO PENAL)

Caracteriza-se pelo **furto mediante fraude**, cometido por meio de **dispositivos eletrônicos ou informáticos**, ainda que sem violação de mecanismos de segurança ou com uso de **software malicioso.**

- **Pena:** reclusão de **4 a 8 anos**, e multa.

6. Rede Federal de Gestão de Incidentes Cibernéticos

(DECRETO Nº 10.748, DE 16 DE JULHO DE 2021)

O **Decreto nº 10.748/2021** institui a **Rede Federal de Gestão de Incidentes Cibernéticos**, com base no Decreto nº 9.637/2018, com o objetivo de **fortalecer a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional** no enfrentamento de riscos cibernéticos (art. 1º e 2º).

A finalidade da Rede é **elevar o nível de resiliência em segurança cibernética** dos ativos de informação da administração pública federal, por meio de ações integradas de **prevenção, tratamento e resposta a incidentes cibernéticos.**

Dentre seus **principais objetivos**, destacam-se (art. 3º):

- **Divulgação de medidas preventivas e reativas** relacionadas à segurança cibernética;
- **Compartilhamento de alertas** sobre ameaças e vulnerabilidades;
- **Disseminação de informações** sobre ataques cibernéticos;
- **Promoção da cooperação institucional** entre os participantes da Rede;
- **Agilidade na resposta a incidentes**, garantindo eficiência no enfrentamento de eventos cibernéticos relevantes.

7. Decisões Judiciais Relevantes

O Superior Tribunal de Justiça (STJ) tem analisado casos relevantes sobre vazamento de dados e responsabilidade das empresas, interpretando a LGPD:

- Em 2023, a Segunda Turma entendeu que, **embora o vazamento de dados seja uma falha indesejável, ele não gera, por si só, o direito à indenização por danos morais**. Para tanto, o titular deve comprovar o efetivo prejuízo causado pela exposição, pois os dados vazados eram comuns e frequentemente fornecidos em cadastros e sites de consulta. Porém, poderia ser diferente o entendimento se o caso envolvesse dados sensíveis, como os de saúde, origem racial ou étnica, convicção religiosa ou biométrico, por exemplo.
- Seguindo a premissa acima, em 2025, a Terceira Turma do STJ reconheceu que, em contrato de seguro de vida, **o vazamento de dados pessoais sensíveis do segurado gera responsabilidade objetiva da seguradora e caracteriza dano moral presumido**, sendo destacado que dados sensíveis exigem maior proteção e que seu vazamento pode comprometer aspectos da vida do segurado, como honra, imagem e segurança pessoal.

- Em 2024, a mesma Terceira Turma do STJ entendeu que instituição financeira responde pelo defeito na prestação do serviço consistente **no tratamento indevido de dados bancários, quando essas informações são utilizadas por estelionatários para aplicar golpes contra consumidores.**
- Em outro caso decorrente de ataque hacker, a Terceira Turma do STJ, em 2024, reforçou que o fato de **a invasão ter sido causada por terceiros não afasta a responsabilidade da empresa, pois a organização precisa demonstrar que adotou boas práticas de segurança**, incluindo governança de dados, ferramentas de supervisão e políticas de mitigação de riscos. Se não conseguir provar sua diligência (responsabilidade proativa), poderá ser responsabilizada.

8. Política Nacional de Cibersegurança e Comitê Nacional De Cibersegurança

(DECRETO Nº 11.856/2023)

O Decreto nº 11.856/2023 instituiu a Política Nacional de Cibersegurança (PNCiber), com a finalidade de orientar a atuação do Estado brasileiro no tema. A política se estrutura a partir de princípios fundamentais, como:

- Soberania nacional e priorização dos interesses do País;
- Prevenção de incidentes e ataques cibernéticos, sobretudo contra infraestruturas críticas e serviços essenciais;
- Reforço à resiliência de organizações públicas e privadas;
- Promoção da educação e do desenvolvimento tecnológico em cibersegurança;
- Cooperação entre entes públicos e privados;
- Fomento à cooperação técnica internacional.

A PNCiber estabelece também objetivos estratégicos, entre os quais se destacam:

- Desenvolvimento de produtos, serviços e tecnologias nacionais voltados à cibersegurança;
- Garantia da confidencialidade, integridade, autenticidade e disponibilidade das informações digitais;
- Proteção reforçada a grupos vulneráveis no ciberespaço, como crianças, adolescentes e idosos;
- Combate aos crimes cibernéticos e ações maliciosas;
- Estímulo à adoção de medidas de proteção, gestão de riscos e resiliência organizacional;
- Fortalecimento da educação e capacitação técnico-profissional em segurança cibernética;
- Incentivo à pesquisa científica, à inovação e à articulação entre diferentes níveis de governo, poderes, setor privado e sociedade;
- Criação de mecanismos regulatórios e de controle para aprimorar a segurança nacional no ambiente digital;
- Estruturação de ações coordenadas para a cooperação internacional

Como **instrumentos de implementação**, a política será operacionalizada por meio de:

- Estratégia Nacional de Cibersegurança;
- Plano Nacional de Cibersegurança.

Para acompanhar e promover sua execução, o decreto cria o **Comitê Nacional de Cibersegurança (CNCiber)**. Suas atribuições incluem:

- Propor atualizações à PNCiber e seus instrumentos;
- Avaliar e sugerir medidas para ampliar a segurança cibernética nacional;

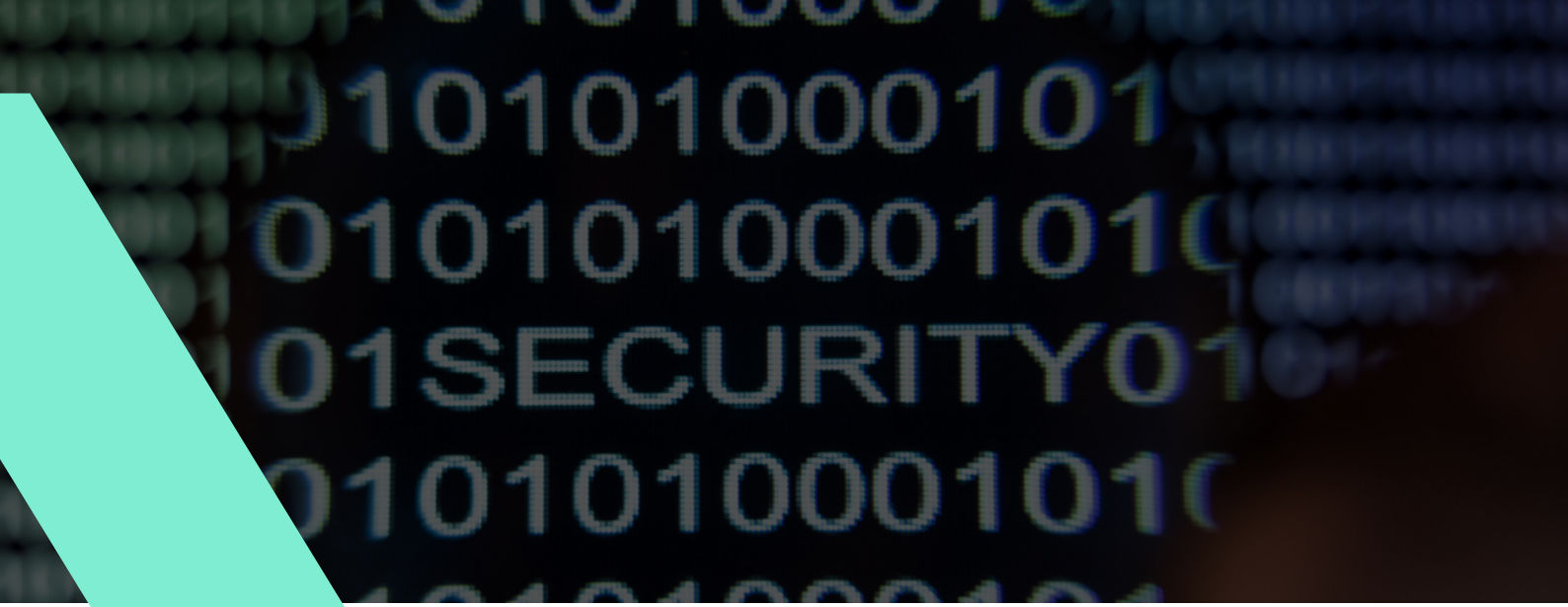
- Formular propostas para aprimorar a prevenção, detecção e resposta a incidentes;
- Propor ações de formação em cibersegurança e estratégias de colaboração internacional;
- Atuar como instância de interlocução com a sociedade e entes federativos.

O CNCiber é um colegiado presidido pelo representante do Gabinete de Segurança Institucional da Presidência da República, e composto por 14 representantes de órgãos da administração pública federal, por 1 representante do Comitê Gestor da Internet no Brasil e por 9 representantes de entidades da sociedade civil, sendo entre elas 3 entidades com atuação relacionada à segurança cibernética ou à garantia de direitos fundamentais no ambiente digital, 3 instituições científicas, tecnológicas e de inovação relacionadas à área de segurança cibernética e 3 entidades representativas do setor empresarial relacionado à área de segurança cibernética.

9. Próximos Passos no Brasil

O Brasil está caminhando com a consolidação de sua governança em cibersegurança, incluindo as seguintes avaliações e medidas para esse ano de 2025:

- **Proposta de Estratégia Nacional de Cibersegurança;**
- **Proposta de criação de um Órgão de Governança da Atividade de Cibersegurança no Brasil**;
- Cibereducação e Ciberhigiene –conscientização e boas práticas para **pessoas físicas e empresas**, com foco em prevenção de riscos.
- **Referenciais mínimos de segurança cibernética** – desenvolvimento de **recomendações práticas para operadores de Serviços Essenciais e Infraestruturas Críticas**, estabelecendo parâmetros mínimos de proteção.
- **Diretrizes para ISACs (Information Sharing and Analysis Centers)** – elaboração de **guia** para a criação e funcionamento de centros de compartilhamento e análise de incidentes, com base na **Portaria nº 148 do GSI**, visando integração à **Rede Governamental de Gestão de Incidentes Cibernéticos (REGIC).**
- **Plano Nacional de Cibersegurança** – construção do plano operacional que dará suporte à futura **Estratégia Nacional,** consolidando diretrizes, metas e ações coordenadas.



10. Conclusão

A **cibersegurança é pilar fundamental para a transformação digital**, a competitividade das empresas brasileiras e, por consequência, a estabilidade econômica e social do país, motivo pelo qual é importante que o Brasil:

- Estabeleça Marco Legal equilibrado, flexível e eficiente, alinhado com as melhores práticas internacionais, restringindo maior carga normativa às infraestruturas críticas e serviços essenciais para a economia brasileira;
- Crie entidade central de coordenação nacional de cibersegurança, com função de organizar e coordenar as ações regulatórias e políticas públicas relacionadas ao tema, bem como evitar sobreposição de competências;
- Fomente à conscientização, educação e capacitação em cibersegurança;
- Inserirá as PMES na esteira de governança da cibersegurança;
- Incentive à pesquisa, desenvolvimento e inovação em cibersegurança;
- Estimule e crie segurança jurídica para o compartilhamento de dados, inteligência e estabelecimento de uma rede nacional de resposta a incidentes cibernéticos;
- Fortaleça suas relações internacionais para colaborar em iniciativas globais de cibersegurança.

Direito,
Inovação
& Tecnologia

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

COMUNICACAO@VLKLAW.COM.BR

AUTORES

RONY VAINZOF

rony@vlklaw.com.br

ALEXANDRA KRASTINS

alexandra.lopes@vlklaw.com.br

CAIO LIMA

caio@vlklaw.com.br

Direito,
Inovação
& Tecnologia

O e-book: "Cibersegurança no Brasil:
Panorama Legal e Regulatório" de Maio de 2025