Cibersegurança no Território Brasileiro: Impacto da LGPD e normas de Segurança da Informação na Defesa Nacional

KIMOSHIRO

THE BOTTOM LINE IS, CYBERSECURITY IS SURVIVAL

Abian M. Laginestra - Caio Gabriel Oliveira
Ingrid Braren - Joyce Freitas

Cibersegurança no Território Brasileiro: Impacto da LGPD e normas de Segurança da Informação na Defesa Nacional

DEDICATÓRIA

Dedico esta obra a todos os profissionais e apoiadores da cibersegurança. Aos corajosos e corajosas que mergulham neste profundo e denso universo da Segurança da Informação. Nosso caminho está apenas começando!

SUMÁRIO

AGRADECIMENTOS

Esse trabalho sintetiza a dedicação de pessoas aguerridas e talentosas, em busca de uma sociedade digital mais segura e com melhor governança de dados.

Agradeço ao meu time querido da Kimoshiro: Anderson Furtado, Vitor Motta, Caio Oliveira e Joyce Freitas.

Agradeço à minha filha Valentina pelos inúmeros "Papai está trabalhando!". Em sua pouca idade, tanto entendimento.

Agradeço aos queridos amigos e amigas Alex Pinheiro, Marcia Freitas e Cristiane Magalhães pelo grande apoio.

Agradeço a Claudia Solange Ballao por essa jornada incrível.

INTRODUÇÃO

A revolução digital acelerou a transformação da sociedade e o acesso à Internet facilitou a oferta de serviços em todas as áreas. Ao mesmo tempo em que ganhamos agilidade e eficiência no nosso dia a dia, passamos a expor nossos dados pessoais na rede mundial de computadores.

Serviços básicos passaram a ser disponibilizados com muito mais rapidez devido ao uso dos meios virtuais, como comprar uma passagem aérea online, emitir a segunda via da conta de luz ou contratar serviços de streaming para a TV.

Entretanto, para isso, precisamos preencher formulários contendo nossos dados pessoais - número da identidade, CPF, nome completo, e-mail etc. Dependendo do site, inserimos informações sensíveis como orientação sexual, etnia, biometria, posicionamento político ou filosófico ou religioso, dados de crianças e adolescentes, entre outros.

Mas o que acontece com essas informações? Onde elas ficam armazenadas?

Ao mesmo tempo em que a informatização de serviços trouxe

benefícios, também nos tornou mais vulneráveis. Vazamentos de dados podem criar grandes transtornos na nossa vida. Os dados expostos podem ser usados por cibercriminosos para abrir contas bancárias, solicitar empréstimos, clonar cartões e mais uma miríade de ações criminosas que têm potencial para causar danos financeiros, emocionais, comerciais e profissionais.

Empresas privadas têm sido vítimas de ataques com pedidos de resgates de grande vulto que afetam seus processos de negócios e viabilidade operacional. Grandes ataques foram registrados contra diversas empresas brasileiras em 2021.

No plano governamental, a informatização dos serviços estatais também se tornou alvo de criminosos que ameaçam explorar vulnerabilidades de infraestruturas críticas que podem ocasionar o caos em um país. Ataques a setores essenciais como energético, distribuição de água, exploração de petróleo, transporte, comunicação, controle alfandegário, instalações e equipamentos militares e nucleares, além de ataques a ministérios, tribunais, influências no sistema eleitoral, entre outros, podem afetar todas os entes da administração pública, seja na esfera federal, estadual ou municipal.

Diante desse cenário ameaçador, a cibersegurança tem sido uma preocupação cada vez maior tanto das empresas privadas como dos governos de várias partes do mundo.

O governo brasileiro, atento a esta realidade, tem produzido

diversas legislações a respeito da proteção de dados, tendo por bússola o princípio constitucional do art. 5º, X da Constituição Federal de 1988.

Entre as muitas legislações que regulam o tema, o foco deste trabalho será apresentar as novas produções legais de maio até agosto de 2021, com base na Lei Geral de Proteção de Dados (Lei nº13.709/2018) e na Constituição Federal.

Capítulo 1 - Cenário da Segurança da Informação no Brasil

Antes da abordagem legal, é preciso ampliar a compreensão do tema Segurança da Informação.

A digitalização quase total dos modelos de negócios tornou a economia global mais eficiente e dinâmica, e também mais vulnerável a ataques cibernéticos. A variedade e a complexidade das ameaças colocam em risco a imprescindível confiança no mundo digital, fator chave para as atividades online.

Por outro lado, a Segurança da Informação tem como característica a velocidade e o acompanhamento da inovação tecnológica, constituindo um desafio para a adoção de medidas eficazes na proteção das infraestruturas críticas nacionais.

Esse cenário levou a crescentes investimentos conjuntos entre governos e setores produtivos. Em consequência, estima-se que, em 2020, o mercado de segurança cibernética mundial seja avaliado em US$ 151.000.000.000,00 (151 bilhões de dólares)[1]. A título de

[1] GLOBAL DIGITAL POPULATION AS OF JULY 2019 (IN MILLIONS). STATISTA. Disponível em: <https://www.statista.com/statistics/617136/digital-population-worldwide/>.

comparação, vê-se que, atualmente, o mercado brasileiro de segurança cibernética movimenta perto de US$ 2.000.000.000,00 (2 bilhões de dólares) por ano com a venda de softwares, hardwares e serviços.

A Organização das Nações Unidas alerta que o mundo pode perder 6 trilhões de dólares este ano, na área de proteção de dados pessoais e financeiros, em decorrência de crimes cibernéticos[2].

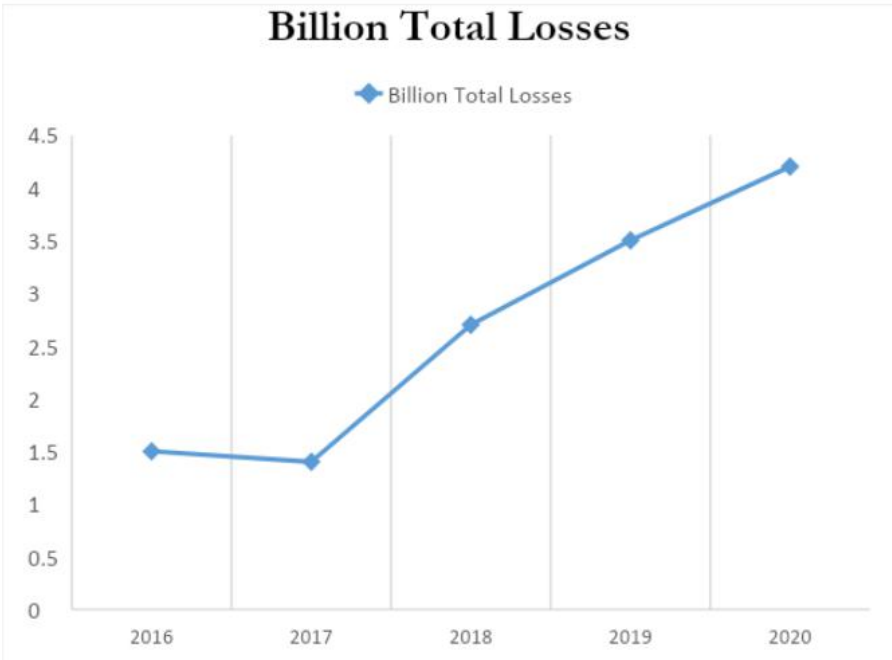
Em termos financeiros, o *Federal Bureau Investigation* (FBI) relatou que, só em 2020, as perdas financeiras foram de 4,2 bilhões de dólares[3].

Acesso em set. de 2021.

[2] CORREIO BRAZILIENSE. Disponível em: <https://www.correiobraziliense.com.br/tecnologia/2021/07/4935247-brasil-sobe-53-posicoes-no-ranking-mundial-de-ciberseguranca-da-onu.html>. Acesso em set. 2021.

[3] Ver IC3 2020 Internet Crime Report em <https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf>.


Total Complaints
Total Complaints
900000
800000
700000
600000
500000
400000
300000
200000
100000
0
2016
2017
2018
2019
2020


Billion Total Losses
Billion Total Losses
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
2016
2017
2018
2019
2020

Você sabia?
No ano de 2020, o FBI constatou perdas financeiras de US$ 4,2 bilhões por crimes cibernéticos.
Em 2021, a ONU estima perdas de até US$ 6 trilhões relacionados à área de proteção de dados.

O gráfico acima, extraído do relatório do IC3[4], demonstra que nos últimos cinco anos as perdas decorrentes de crimes cibernéticos somam US$ 13,3 bilhões.

O Relatório de 2019 do Fundo Monetário Internacional[5] destacou que, em todas as economias, a diretriz é a implementação de ações que fortaleçam a resiliência, ao mesmo tempo em que elege, como necessária, a busca por maior cooperação multilateral para gerenciar os riscos em segurança cibernética.

O risco para a economia brasileira, gerado pela intrusão em computadores e pela disseminação de códigos maliciosos praticados pelo crime organizado, já é uma realidade.

Atualmente, são mais de 4.500 serviços disponibilizados de forma centralizada no portal Gov.br e mais de cem milhões de brasileiros cadastrados no Portal Único. É uma enorme base pública de dados pessoais.

---

[4] A imagem inclui dados anuais e agregados de perdas dos anos de 2016 a 2020. Durante este período, o IC3 recebeu um total de 2.211.396 reclamações, reportando perdas de 13,3 bilhões de dólares.

[5] WORLD ECONOMIC OUTLOOK REPORTS. INTERNATIONAL MONETARY FUND. Disponível em <https://www.imf.org/en/Publications/WEO/Issues/2019/03/28/world-economic-outlook-april-2019>. Acesso em set. de 2021.

Entretanto, quando se fala em ranking de educação digital em cibersegurança, o Brasil está na 42ª colocação entre os 50 países avaliados para o estudo global *Cyber Risk Literacy and Education Index*, da consultoria Oliver Wyman[6].

Mas, no plano da normatização para garantir a Segurança da Informação, o Brasil saltou do 71ª lugar para a 18ª posição no Índice Global da Segurança Cibernética 2020 - ranking realizado pela União Internacional de Telecomunicações (UIT), agência da Organização das Nações Unidas (ONU) especializada em tecnologia da informação e comunicação[7].

O índice mede as ações de 194 nações para enfrentar riscos cibernéticos, e a pontuação, de 0 a 100, é obtida a partir de avaliação de cinco aspectos: jurídico, técnico, cooperativo, organizacional e de capacitação.

O novo posicionamento brasileiro expressa uma sensível melhora do país e reflete as medidas que vêm sendo tomadas com a publicação de normativas, diretrizes e consensos sobre a governança de Segurança da Informação, especialmente na administração pública federal.

[6] Disponível em <https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html>. Acesso em 20 set. 2021.

[7] Disponível em: <Brasil ganha 53 posições em ranking global de cibersegurança (febraban.org.br)>. Acesso em 17 set. 2021.

Capítulo 2 - Política Nacional de Segurança da Informação (PNSI)

Para fomentar a criação de uma cultura de Segurança da Informação no Brasil, o Governo Federal editou o Decreto nº 9.637/2018: a Política Nacional de Segurança da Informação - PNSI, alterada pelo Decreto nº 10.641/2021.

Ela tratou dos princípios, objetivos, instrumentos, atribuições e competências de Segurança da Informação para os órgãos e entidades da Administração Pública Federal sob o prisma da governança.

Os princípios que regem a Segurança da Informação no Brasil são:

I. Soberania nacional;

II. Respeito e promoção dos direitos humanos, da liberdade de expressão, proteção dos dados pessoais, da privacidade e o acesso à informação;

III. Promoção da visão sistêmica da Segurança da Informação;

IV. Responsabilidade brasileira na coordenação de esforços, no estabelecimento de políticas, diretrizes e estratégias voltadas à Segurança da Informação;

V. Educação para o fomento da cultura de Segurança da Informação;

VI. Integração e cooperação entre o Poder Público, o setor empresarial, a sociedade e as instituições acadêmicas;

VII. Cooperação internacional.

Interessante notar a preocupação com a formação sistêmica da Segurança da Informação, demonstrando que se trata de uma transversal, que perpassa várias áreas de conhecimento, desde os princípios fundamentais da pessoa humana, já consagrados na Constituição Federal na forma da proteção à privacidade de dados e liberdade de expressão, a cooperação no cenário internacional, que é uma área ligada à política externa do Brasil, até a educação e a integração entre diferentes setores.

De fato, o Brasil tem dado seguimento às diretrizes apontadas na Política Nacional de Segurança da Informação. Vemos isso em

tratados internacionais, como a Convenção Europeia sobre Crimes Cibernéticos, a instituição de uma Estratégia Nacional de Segurança Cibernética e outros instrumentos legais, como será visto nos capítulos a seguir.

A PNSI traz alguns objetivos inovadores relacionados à Segurança da Informação, como o fomento às atividades de pesquisa, de desenvolvimento tecnológico e inovação, o fortalecimento da cultura, a proteção das informações das infraestruturas críticas e dos dados pessoais sob a guarda das entidades públicas.

Diante disso, o Decreto nº 9.637, de 2018, indicou, em seu art. 6º, que a Estratégia Nacional de Segurança da Informação seja construída em módulos: segurança cibernética, defesa cibernética, segurança das infraestruturas críticas, segurança da informação sigilosa e proteção contra vazamento de dados.

A Segurança Cibernética - Seg Ciber foi identificada como a área mais crítica. Por isso, o Gabinete de Segurança Institucional da Presidência da República elegeu, em janeiro de 2019, a Estratégia Nacional de Segurança Cibernética - E-Ciber como o primeiro módulo da Estratégia Nacional de Segurança da Informação a ser elaborado.

A PNSI determinou que o Gabinete de Segurança Institucional da Presidência da República - GSI/PR - é o responsável pela aprovação de estratégias, normas, recomendações e planos no tema relacionado à

Segurança da Informação. Vemos, de fato, uma atuação presente do GSI/PR.

A PNSI ainda prevê que os órgãos da Administração Pública Federal são responsáveis por elaborar políticas internas para implementar e promover ações de capacitação em Segurança da Informação. Neste sentido, vemos produções como o Manual de Segurança Cibernética da ANAC e a Circular SUSEP 638/2021. que serão abordadas adiante.

A publicação da PNSI colocou em prática o direito à privacidade e à proteção dos dados. Ela demonstra a preocupação do Brasil em assegurar que os três pilares da Segurança da Informação - confidencialidade, integridade e autenticidade - sejam preservados.

Preocupa-se também com a disseminação de uma cultura nacional, apta a assegurar o direito dos cidadãos brasileiros e tornar o Brasil cada vez mais seguro no aspecto da proteção dos meios cibernéticos. As leis a seguir confirmam essa ideia.

Capítulo 3 - Estratégia Nacional de Segurança Cibernética (E-Ciber)

A criação de um arcabouço jurídico que reúna todos os atores estatais e não estatais sob a égide da segurança cibernética, com adoção de normas de governança em todas as esferas, poderá contribuir para o alinhamento estratégico, doutrinário e operacional nas ações de defesa cibernética.

Por isso, verificou-se a necessidade de um direcionamento central de onde emanam as principais diretrizes, servindo como local de consulta e direcionamento estratégico de Segurança da Informação.

O GSI e a ANPD têm coordenado esse esforço, propondo medidas e regulamentos com a participação de representantes de todos os setores da sociedade. Faz-se exceção, apenas, aos aspectos relacionados à defesa e à guerra cibernéticas, que estão a cargo do Ministério da Defesa.

A Estratégia Nacional de Segurança Cibernética (E-Ciber), assinada pelo Presidente da República em fevereiro de 2020, com validade no quadriênio 2020-2023, é uma orientação do Governo Federal sobre as principais ações por ele pretendidas na área de segurança cibernética, em termos nacionais e internacionais.

Em 2015, o Governo Federal deu publicidade à Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal, com validade até 2018, como um importante instrumento de apoio ao planejamento dos órgãos e entidades do Governo, cujo objetivo foi de melhorar a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais. Esse documento impulsionou as discussões sobre o tema no âmbito da Administração Pública Federal, assim como em outros setores da sociedade.

A E-Ciber foi regulamentada pelo Decreto nº 10.222/2020. Depois de 31 reuniões e 7 meses de estudos e debates, ela foi elaborada sob a coordenação do Gabinete de Segurança Institucional da Presidência da República, com a participação de mais de 40 órgãos e entidades do governo, instituições privadas e setor acadêmico.

A E-Ciber busca fazer um alinhamento normativo, estratégico e operacional, facilitando a mensuração dos níveis de maturidade da sociedade em segurança cibernética, dando uma percepção mais clara sobre a importância da Segurança da Informação como tema de relevância nacional.

Por meio de metodologia *bottom up* e com base nas conclusões dos subgrupos de trabalho, em avaliação comparativa - *benchmarking* - sobre estratégias adotadas em outros países, alinhado ao conteúdo

da Política Nacional de Segurança da Informação, chegou-se ao diagnóstico da segurança cibernética global e do Brasil.

Em seguida, foram estabelecidos os objetivos estratégicos nacionais e as respectivas ações estratégicas, segundo sete eixos de atuação que demonstram à sociedade brasileira os pontos considerados relevantes para o país na área da segurança cibernética.

Um ponto crítico relacionado ao aumento da preocupação com a Segurança da Informação se refere à proteção cibernética das empresas representantes das infraestruturas críticas: Telecomunicações, Transportes, Energia, Água e setor Financeiro. Embora a Saúde não tenha constado na listagem oficial, é considerada parte desse rol.

Partiu-se da premissa de que, se essas companhias tiverem seus serviços interrompidos ou destruídos, haverá um sério impacto social, econômico, político e à segurança nacional.

Por isso, essas empresas precisam ter uma abordagem consistente e evolutiva em segurança cibernética para identificar e avaliar vulnerabilidades, com um gerenciamento de ameaças eficaz. Com essa ideia, elas devem observar as cinco funções previstas na estrutura de segurança cibernética do *National Institute of Standards and Technology* - NIST: Identificar, Proteger, Detectar, Responder e Restaurar.

A avaliação é que os principais tipos de ameaças contra essas organizações são ataques de *phishing*, negação de serviço em larga escala,

vazamentos de informações privadas, espionagem, terrorismo cibernético e a interrupção de serviços.

O desafio é a necessidade de equilíbrio entre segurança, privacidade e o não confinamento de recursos para garantia do fomento ao ambiente de inovação.

É mencionado em muitas estratégias nacionais de segurança cibernética que ataques às infraestruturas críticas estão entre as maiores ameaças à segurança nacional - considerando-se que grande parte das economias nacionais está, de modo crescente, dependente de sistemas de informação de setores essenciais, baseados em controles automatizados.

Portanto, a proteção de infraestruturas críticas contra ameaças cibernéticas em evolução requer uma abordagem ampla, com o acompanhamento da avaliação de riscos, planejamento, coordenação e desenvolvimento de ações de segurança cibernética para definir normativas e requisitos metodológicos para a implementação das ações de segurança cibernética.

No decorrer da elaboração da estratégia brasileira, foi observado que:

- não há, no Brasil, um arcabouço autóctone e abrangente de segurança cibernética que contribua para o fortalecimento da resiliência cibernética nacional;

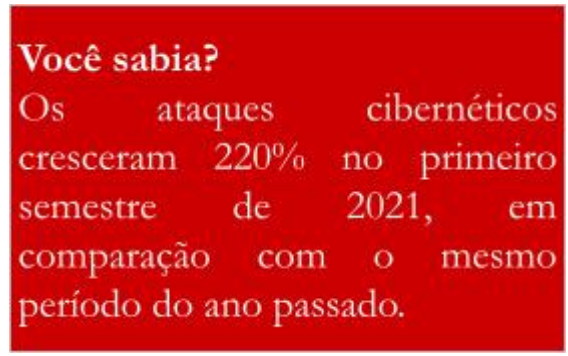
- códigos, normas, padrões e orientações em vigor evoluíram com o desenvolvimento de projetos, de ferramentas e de práticas relacionadas à segurança cibernética, mas não foram absorvidos de modo adequado pelas entidades públicas e privadas;
- os recursos de segurança cibernética evoluíram;
- é necessário aumentar a articulação entre os representantes das infraestruturas críticas;
- é importante estabelecer modelos que permitam compreender o risco cibernético para a prestação de serviços e avaliar o custo de uma ocorrência; e
- é necessário incentivar essas organizações críticas a criarem uma cultura de segurança cibernética.

A necessidade de estabelecer e consolidar parcerias estratégicas no ambiente cibernético tornou-se mais evidente ao se constatar que grande parte das infraestruturas críticas estão sob responsabilidade do setor privado, o que reforça a necessidade de propósitos comuns, em segurança cibernética, entre Governo, empresas privadas, academia e a sociedade em geral.

Segundo o Relatório da "*Internet Organised Crime Threat Assessment* - IOCTA"[8], de 2018, da Agência da União Europeia para a Cooperação

[8] Internet Organised Crime Threat Assessment (IOCTA) 2018. European Union Agency for Law Enforcement Cooperation, Europol. Disponível em: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018>. Acesso em 20 set. 2021.

Policial - Europol, "a falta de legislação adequada sobre crimes cibernéticos fez com que o Brasil fosse o alvo número um e a principal fonte de ataques online na América Latina; 54% dos ataques cibernéticos reportados no Brasil supostamente são originários de dentro do país". O documento prossegue afirmando que, "de modo semelhante aos EUA, o Brasil é um dos principais hospedeiros de sites de *phishing*, com alguns relatos colocando o Brasil como uma das dez maiores fontes mundiais de ataques cibernéticos".



Verifica-se, ainda, que o número de ataques cibernéticos cresceu 220% no primeiro semestre de 2021, comparado ao mesmo período de 2020[9]. Os dados foram analisados pelo grupo MZ, com base em informações levantadas junto à CVM (Comissão de Valores Mobiliários). O setor energético foi o que sofreu mais ataques, com seis notificações, seguido pela Saúde, com cinco intimações.

[9] Disponível em: <https://www.cnnbrasil.com.br/business/ataques-ciberneticos-a-empresas-brasileiras-crescem-220-no-1-semestre-de-2021/>. Acesso em 17 set. 2021

Um ataque cibernético de grande envergadura, caso não seja adequadamente tratado, pode afetar profundamente a reputação da organização, ocasionar perda de receitas, levar a prejuízos operacionais com a paralisação dos serviços, resultar em perda de informações e ainda levar à aplicação de sanções legais e administrativas.

Dessa forma, é importante que as organizações, públicas ou privadas, estabeleçam políticas e procedimentos de segurança cibernética que sejam periodicamente revisados, atendam à evolução tecnológica, ao aperfeiçoamento de processos e à necessidade de capacitação contínua e estruturada para todos os colaboradores, por meio de programas de capacitação e de treinamento.

Dentro dessa perspectiva, ressaltam-se três vertentes importantes: a medição da eficácia e da eficiência dos centros de tratamento e resposta aos incidentes computacionais; a elaboração de indicadores para medir o desempenho do país em segurança cibernética; e o estabelecimento de rotina de verificações de conformidade em segurança cibernética dentro dos órgãos públicos e das entidades privadas, por eles conduzidas, de modo que seja possível estabelecer a correta relação entre os aspectos técnicos de tecnologia da informação - como análise de vulnerabilidades, relatórios técnicos de ameaças e relação de soluções em tecnologia - e os aspectos de negócio, como continuidade dos serviços prestados, riscos à imagem e processos de tomada de decisão.

A verificação de conformidade deve ser vista como um processo natural, baseada em programas estabelecidos pelas próprias entidades públicas e privadas, e que visa ao aprimoramento contínuo dos sistemas voltados à segurança cibernética. Por isso, deve ser objeto de constante atenção.

Diante de todas essas considerações, o E-Ciber tratou, em termos de proteção e segurança, de alguns eixos temáticos. São eles:

I. Governança da Segurança Cibernética Nacional: aborda os aspectos relativos a mecanismos e medidas passíveis de adoção em prol da governança cibernética, a metodologia de gestão de riscos, a confiança e segurança no uso do certificado digital, a implantação de modelo centralizado de coordenação da segurança cibernética nacional e o monitoramento do cenário cibernético;

II. Prevenção e mitigação de ameaças cibernéticas: versa sobre a gestão de incidentes computacionais, que envolve detecção, triagem, análise e resposta a esses incidentes;

III. Proteção Estratégica: objetiva analisar os aspectos relativos à proteção cibernética do Governo e à proteção cibernética das infraestruturas críticas, cujo nível de proteção deve ser adequado e proporcional à sua relevância, de forma a reduzir a vulnerabilidade

das organizações governamentais e proporcionar níveis adequados de segurança e de resiliência contra ataques cibernéticos.

Para alcançar todas estas metas, o Governo Federal tem investido na proteção legal, como se verá a seguir.

Capítulo 4 - A Legislação Brasileira

A privacidade é um direito fundamental previsto no art. 12 da Declaração Universal dos Direitos Humanos de 1948 e na Constituição Federal do Brasil no artigo 5º, X e XII.

As Leis nºs 12.737/2012 e 12.965/2014, conhecidas respectivamente como Lei Carolina Dieckmann e o Marco Civil da Internet, foram dois baluartes para a regulamentação da Segurança da Informação no âmbito tecnológico no Brasil.

No entanto, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), inovou ao exigir a implementação da Segurança da Informação no tratamento de dados de todas as organizações, sejam elas públicas ou privadas, sob pena de responsabilidade e multas que podem chegar a R$ 2.000.000,00 (dois milhões de reais).

A LGPD dispõe de forma bastante ampla sobre operações de tratamento de dados, sejam elas realizadas em meios digitais, físicos ou quaisquer outros, visando garantir sobretudo a privacidade e a autodeterminação informacional dos titulares destes dados, frente às atividades dos chamados controladores e operadores. Entende-se por tratamento atos como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento,

arquivamento, armazenamento, eliminação etc. Em outras palavras, se uma empresa armazena dados de compras de clientes, ou mesmo coleta dados dos seus próprios funcionários para arquivamento no setor de recursos humanos, ela deverá realizar tais operações de tratamento seguindo as regras previstas na LGPD.

Normalmente, acredita-se que apenas o consentimento do titular dos dados pessoais permite a realização de operações de tratamento. Todavia, existem várias outras hipóteses previstas pela lei. A necessidade de cumprir obrigações legais ou contratuais, a execução de políticas públicas, o exercício regular de direitos, a proteção da vida e da saúde e até mesmo o legítimo interesse do controlador dos dados também podem justificar operações de tratamento de dados.

Neste último caso, que diz respeito aos legítimos interesses do controlador dos dados, encontramos um grande foco de incertezas, haja vista tratar-se de algo que no Direito se costuma chamar de "conceito jurídico indeterminado". Tais conceitos jurídicos dependem em grande medida da interpretação de autoridades para ganhar maior densidade e sentido como norma de conduta.

Por se tratar de uma lei que entrou em vigor há pouco tempo, ainda não existe precisão sobre os contornos que as autoridades competentes darão ao legítimo interesse do controlador, mas alguns parâmetros podem ser antecipados com base na experiência jurídica, internacional e nacional, no que tange à proteção da privacidade e

outros direitos fundamentais. No meio jurídico diz-se que a aplicação do legítimo interesse como base legal para tratamento de dados depende da realização de um raciocínio de balanceamento que deve ponderar os seguintes fatores: a) a adequação entre as finalidades legítimas do controlador e as operações de tratamento realizadas; b) o tratamento do mínimo de dados necessários para atingir os fins legítimos do controlador dos dados; c) as expectativas razoáveis que o titular poderia criar em relação à utilização de seus dados pessoais; d) a consideração de que o tratamento será feito não só para atender aos interesses do controlador, mas também aos interesses e direitos fundamentais do titular dos dados tratados.

Para tornar tudo mais concreto, imaginemos uma situação na qual uma empresa atuante no setor de comércio eletrônico faz a coleta de dados dos clientes que realizam compras em sua plataforma digital. O tratamento posterior destes dados com a finalidade de realizar marketing direto e enviar ofertas personalizadas, com base no perfil de compra dos usuários, pode ser realizado com fundamento no legítimo interesse do controlador dos dados. Nesse caso, podemos ver que a prática está de acordo com os interesses legítimos do comerciante, bem como expectativas, direitos e interesses dos consumidores. Por outro lado, se uma farmácia compartilha os dados do seu programa de fidelidade com uma operadora de plano de saúde, com o fim majorar o prêmio pago por alguns de seus clientes, podemos vislumbrar uma

aplicação equivocada da ideia de legítimo interesse como fundamento para tratamento de dados pessoais.

Ademais, vale destacar que, por se tratar de hipótese que permite o tratamento dos dados pessoais em situação de maior incerteza de aplicação, a própria LGPD exige maior precaução e transparência, sendo necessário cuidado com o registro das operações de tratamento e a documentação das justificativas de aplicação dessa base legal de tratamento.

Além dessas leis de amplo aspecto, temos acompanhado a publicação de vários instrumentos normativos de competência do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República e outras agências regulamentadoras vinculadas à Administração Pública Federal.

Capítulo 5 - A Atuação da Agência Nacional de Proteção de Dados (ANPD)

Dando continuidade ao processo legislativo sobre Segurança da Informação, no dia 28 de maio de 2021 a ANPD abriu consulta pública sobre as regras de fiscalização que serão seguidas pela Agência. A consulta esteve disponível por 30 dias na plataforma Participa + Brasil.

Essa consulta expressa o posicionamento do Poder Público para abrir o debate de implementação das normas da LGPD, possibilitando a participação de estudantes, acadêmicos, profissionais da área e sociedade civil.

O texto proposto estabelece o mecanismo de fiscalização que a Autoridade pretende adotar, com previsão de ações de monitoramento, orientação, prevenção e aplicação de sanção, seguindo a lógica da regulação responsiva.

Conforme a minuta, as atividades de monitoramento da forma como as empresas tratam dados pessoais começarão em janeiro de 2022.

A ANPD editará dois mapas de monitoramento por ano, que vão definir os temas prioritários para fiscalização a cada semestre. Isso fornece alguma previsibilidade para as empresas que, a esta altura, já devem estar adequadas à legislação.

O ciclo de monitoramento considerará todas as reclamações, denúncias, representações e notificações de incidentes, bem como outras fontes de insumos recebidos pela ANPD que sejam relacionados às violações de dados pessoais ou da privacidade.

Para aumentar a colaboração na implementação da cultura de proteção e privacidade de dados no Brasil, a ANPD assinou Acordo de Cooperação Técnica (ACT) com a Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública (Senacon/MJSP), em 22 de março de 2021.

O objetivo é realizar um trabalho conjunto destinado à proteção de dados dos consumidores para dar maior agilidade nas investigações de incidentes de segurança.

Para isso, a Senacon/MJSP passará a compartilhar informações coletadas sobre as reclamações de consumidores e relacionadas à proteção de dados pessoais. Com esse intuito, formalizou um Núcleo dentro do Conselho Nacional de Defesa do Consumidor.

A ANPD, por sua vez, fixará as interpretações necessárias à aplicação da Lei Geral de Proteção de Dados nos casos concretos.

O convênio acima demonstra o aumento cada vez maior de ferramentas para concretizar a Segurança da Informação como uma realidade.

Capítulo 6 - Acordo de Cooperação entre a ANPD e o NIC.BR

No dia 20 de julho de 2021 foi assinado um Acordo de Cooperação entre a ANPD e o Núcleo de Informação e Coordenação do Ponto BR – NIC.br.

Esse acordo tem como premissas: o intercâmbio de informações; realização de ações de interesse comum no que diz respeito à proteção de dados pessoais e à Segurança da Informação; mútua cooperação técnico-científica voltada para o desenvolvimento de ações e produção de materiais de capacitação e conscientização no tema; além da previsão de apoio institucional entre as entidades e a produção conjunta e coordenada de estudos, análises e pesquisas sobre proteção de dados pessoais, Segurança da Informação, privacidade nas redes e tecnologia. O Acordo de Cooperação também tem como anuente o Coordenador do Comitê Gestor da Internet no Brasil – CGI.br, Marcio Migon.

A cooperação trará benefícios não apenas para os partícipes, mas principalmente para a sociedade, incluindo agentes regulados e titulares de dados pessoais.

Alguns dos benefícios esperados são a divulgação e esclarecimento dos procedimentos a serem tomados por controladores

em caso de incidentes envolvendo dados pessoais, a difusão dos conhecimentos quanto à Segurança da Informação e de consciência situacional no ambiente cibernético brasileiro, e a educação do cidadão quanto a como proteger suas informações na Internet.

A ANPD e o NIC.br já iniciaram algumas das atividades previstas no Acordo. Dentre elas, pode ser destacado o lançamento de dois fascículos da Cartilha de Segurança para Internet: um sobre a proteção de dados e outro sobre os cuidados em relação a vazamento de dados pessoais.

O Acordo de Cooperação com o NIC.br é o terceiro a ser celebrado pela ANPD neste ano. É mais um fruto das ações previstas no Planejamento Estratégico da Autoridade, que tem como um de seus objetivos a promoção do diálogo com entidades governamentais e não-governamentais, com o intuito de construir parcerias estratégicas para a promoção de estudos, atuação em conjunto e incorporação das melhores práticas no tema de proteção de dados pessoais.

Capítulo 7 - Plano Estratégico Institucional 2020-2025

Ainda no mês de julho deste ano, o Governo Federal atualizou os dados relativos ao Plano Estratégico Institucional 2020-2025. Ele dispõe sobre a elaboração, avaliação e revisão do planejamento estratégico institucional dos órgãos e das entidades da Administração Pública Federal integrantes do Sistema de Organização e Inovação Institucional do Governo Federal – SIORG.

Nas reuniões do Comitê de Governança, Riscos e Controle do GSI (ocorridas em março, junho, setembro e dezembro de 2021), houve a apresentação dos indicadores parciais obtidos até então, buscando-se verificar tendências quanto ao cumprimento das metas anteriormente, possibilitando correções de rumo, a fim de que as mesmas venham a ser atingidas.

Os pontos apresentados no relatório são:

I. O aperfeiçoamento dos mecanismos de governança e gestão corporativa que envolve o número de reuniões anuais do Comitê de Governança, Riscos e Controle, do Grupo de Trabalho de

Planejamento Estratégico e Gestão Estratégica e porcentagem de Planos de Ação do PPIF tem sido executado no prazo estabelecido;

II. Tem havido promoção da inovação dos serviços e processos com foco na simplificação e na transformação digital, com a taxa de migração dos aplicativos próprios;

III. Registra a intensificação dos mecanismos de proteção da Presidência da República e de outras instituições do Estado.

Apresenta, ainda, os seguintes dados:

I. Índice de incidentes cibernéticos resolvidos em 2021. Meta anual: 92% de solução dos incidentes cibernéticos recebidos e detectados por ano.
II. Monitoramento até 31/05: 78,32% (2.323 incidentes resolvidos de um total de 2.970 incidentes detectados, medição em março).

III. Taxa de missões de segurança de instalações com sucesso: 100% de missões com sucesso.

IV. Monitoramento de janeiro até 31/05: janeiro: 100% (124 missões); fevereiro: 100% (112 missões); março: 100% (124 missões); abril: 100% (120 missões); maio: 100% (124 missões).

Quando avalia a potência das ações de assuntos estratégicos de Defesa e Segurança Nacional em prol do interesse do Estado e sociedade brasileiros, traz os seguintes números:

I. Meta 2021: Acompanhar 96% dos desdobramentos das propostas produzidas no âmbito do Comitê de Desenvolvimento do Programa Espacial Brasileiro.

II. Monitoramento até 31/05: janeiro: 100% (1 acompanhamento); fevereiro: 100% (1 acompanhamento); março: 100% (1 acompanhamento); abril: 100% (1 acompanhamento); maio: 100% (1 acompanhamento).

No quesito aprimoramento da gestão da inteligência de Estado (ABIN):

I. Monitoramento até 31/05: janeiro: 100% (6 pesquisas respondidas); fevereiro: 100% (42 pesquisas respondidas); março: 100% (15 pesquisas respondidas); abril: 98,84% (85 satisfeitos de

um total de 86 pesquisas respondidas); maio: 95,65% (22 satisfeitos de um total de 23 pesquisas respondidas).

Os níveis apresentados até 31 de maio são bastante satisfatórios. Demonstram o empenho do Brasil na implementação da Segurança da Informação, que precisa ser constantemente aprimorada, a fim de se manter sempre vigilante e atualizada.

Capítulo 8 - Instrução Normativa nº1 de 27 de Maio de 2020

Essa instrução trata da Estrutura de Gestão da Segurança da Informação no âmbito da Administração Pública Federal. Sua finalidade é orientativa, para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional, reconhecidos pilares da Segurança da Informação.

A norma elenca que, dentro do conceito de Segurança da Informação, está abrangida a segurança cibernética; a defesa cibernética; a segurança física; a proteção de dados organizacionais; e as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Passa, então, a tratar da Estratégia Nacional de Segurança Cibernética, que traça os objetivos estratégicos da Segurança da Informação. Eles devem orientar o planejamento da gestão de Segurança da Informação na administração federal.

Os objetivos estratégicos do E-Ciber são: tornar o Brasil mais próspero e confiável no ambiente digital; aumentar a resiliência brasileira às ameaças cibernéticas; e fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

Para concretizar essas metas, divide as ações em:

I. fortalecimento das ações de governança cibernética;

II. estabelecimento de um modelo centralizado de governança no âmbito nacional;

III. promoção de um ambiente participativo, colaborativo, confiável e seguro entre o setor público, setor privado e sociedade;

IV. elevação do nível de proteção do Governo;

V. aumento do nível de proteção das infraestruturas críticas nacionais;

VI. aprimoramento das leis relativas à segurança cibernética;

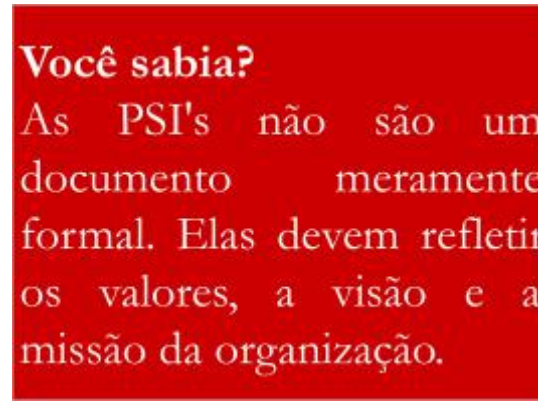
VII. incentivo à concepção de soluções inovadoras em segurança cibernética;

VIII. ampliação da parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade;

IX. elevação do nível de maturidade da sociedade em segurança cibernética;

X. ampliação da cooperação internacional entre o Brasil e outros agentes internacionais no campo da segurança cibernética.

É interessante notar que a IN nº 1/2020 tornou obrigatório que todos os órgãos e entidades federais tenham uma Política de Segurança da Informação, implementada e formalizada pela Alta Administração da instituição. Essas PSIs devem conter as diretrizes, responsabilidades, competências e subsídios para plena execução dentro da organização.



As PSIs não são documentos meramente formais. Elas devem ser incorporadas na cultura organizacional. É um instrumento vivo, que deve acompanhar as mudanças e auxiliar no constante aprimoramento da cultura de segurança. Elas devem ser divulgadas de forma ampla e acessível para os servidores, usuários e prestadores de serviço.

As PSIs são um reflexo da visão, da missão e dos valores da organização. Mas existe uma estrutura básica que a IN nº 1/2020 elenca. São necessários:

I. determinação do escopo, conceitos e definições a serem utilizadas na PSI;

II. informação dos princípios que regem a Segurança da Informação no órgão ou na entidade;

III. diretrizes gerais sobre o tratamento dos dados dentro da organização;

IV. previsão de regras de segurança física e do ambiente;

V. plano de gestão de incidentes;

VI. indicação da gestão de ativos;

VII. gerenciamento do uso dos recursos operacionais e de comunicações como e-mail, acesso à Internet, mídias sociais, computação em nuvem, dentre outros;

VIII. estabelecimento dos controles de acesso;

IX. gestão de riscos;

X. gestão de continuidade;

XI. previsão de auditorias e conformidade;

XII. atribuições e responsabilidades dos envolvidos na estrutura de gestão de Segurança da Informação;

XIII. estabelecimento de penalidades para os casos de violação da PSI ou quebra de segurança;

XIV. política de atualização da PSI, que não deve exceder quatro anos.

A IN nº 1/2020 ressalta que a Alta Administração precisa estar comprometida com as diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão da Segurança da Informação.

Outra obrigatoriedade trazida pela normativa em estudo é a obrigatoriedade da instituição de um Comitê de Segurança da Informação, coordenado pelo Gestor de Segurança da Informação,

nomeado pela Alta Administração da entidade, que tem atribuições específicas:

I. responsável pelas ações de capacitação e profissionalização dos recursos humanos sobre Segurança da Informação;

II. implementar uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

III. coordenar e executar as ações de Segurança da Informação;

IV. consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de Segurança da Informação no âmbito interno;

V. aplicar ações corretivas e administrativas quando houver casos de violação da Segurança da Informação.

A IN nº 1/2020 expressa a preocupação brasileira com a Segurança da Informação. As exigências de adequação espelham o comprometimento com esse tema e seguem o regramento da LGPD.

Capítulo 9 - Decreto 10.741/21: Rede Federal de Gestão de Incidentes Cibernéticos

A Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) foi instituída em 19 de julho de 2021. É uma ação prevista na Política Nacional de Segurança da Informação, cuja finalidade é manter e aprimorar a coordenação entre órgãos e entidades da Administração Pública Federal para prevenção, tratamento e resposta a incidentes cibernéticos.

Mas de que maneira essa coordenação acontece?

Segundo o Decreto, as informações sobre incidentes cibernéticos, configurações e características técnicas de ativos de informação de cada órgão ou entidade da Administração Pública Federal são imprescindíveis para a segurança da sociedade e do Estado.

Com o compartilhamento, torna-se mais fácil o mapeamento dos incidentes e as razões pelas quais ocorreram, permitindo correções e adoção de meios de mitigação de riscos, evitando que os mesmos problemas se repitam em outras organizações públicas. Isso eleva o nível de resiliência e maturidade, com evidentes ganhos para todos os envolvidos.

Para isso, ela tem como objetivos:

I. divulgação das medidas de prevenção, tratamento e resposta a incidentes cibernéticos;

II. compartilhamento de alertas sobre ameaças e vulnerabilidades cibernéticas;

III. divulgação das informações sobre ataques cibernéticos;

IV. promoção da cooperação entre os seus participantes; e

V. promoção da celeridade na resposta a incidentes cibernéticos.

Os órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional são obrigados a participar da Rede Federal de Gestão de Incidentes Cibernéticos. A participação das empresas públicas, das sociedades de economia mista federais e das suas subsidiárias é opcional, voluntária e ocorre por meio de um termo de adesão. No entanto, o Banco Central do Brasil e a Comissão Nacional de Energia Nuclear, em razão da sua relevância estratégica, são compelidos a participar do ReGIC e têm a atribuição específica de

identificar as infraestruturas críticas de suas áreas de atuação e operar para a adequação à proteção da Segurança da Informação.

A Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia também tem participação na ReGIC, na condição de órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp do Poder Executivo Federal.

Por se tratar de infraestruturas críticas, de grande importância para o Brasil, o ReGIC manterá articulação com o Ministério da Defesa e das Forças Singulares, e será operado pelo Comando de Defesa Cibernética, na condição de órgão central do Sistema Militar de Defesa Cibernética.

Capítulo 10 - Instrução Normativa GSI/PR Nº3, de 28 de Maio de 2021

A Instrução Normativa nº 3/2021 é um documento com diversos indicativos técnicos sobre a efetivação, na administração pública, dos princípios da Segurança da Informação.

No que concerne aos processos de gestão de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, a IN GSI/PR nº 3/2021 estabelece que, a partir da sua publicação, será obrigatório:

I. o mapeamento dos ativos de informação;

II. a gestão de riscos de Segurança da Informação;

III. a gestão de continuidade de negócios;

IV. a gestão de mudanças nos aspectos de Segurança da Informação; e

V. a avaliação de conformidade (*compliance*) dos processos que envolvem a Segurança da Informação.

Como o processo de mapeamento de ativos busca estruturar e manter um registro de ativos de informação para subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à Segurança da Informação, ele deve considerar:

I. os objetivos estratégicos da organização;

II. os processos internos da organização;

III. os requisitos legais; e

IV. a estrutura do órgão ou da entidade.

De acordo com a normativa, o agente responsável pela gestão dos ativos de informação deverá identificar e classificar os ativos de informação por nível de criticidade; identificar potenciais ameaças; identificar vulnerabilidades dos ativos; consolidar informações da análise do nível de Segurança da Informação de cada ativo de informação ou de grupos de ativos de informação em um relatório; autorizar a atualização do relatório; e avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

Desta forma, o agente deverá buscar direcionar e controlar o risco de Segurança da Informação, de forma a adequá-lo para níveis que

sejam classificados como aceitáveis.

O processo de gestão de riscos deverá ser documentado e planejado, constituído por um relatório de identificação, análise e avaliação dos riscos e um relatório de tratamento de riscos.

O processo de gestão de continuidade de negócios deve ser baseado nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão e em diretrizes institucionais sobre gestão de continuidade de negócio. Com essa ideia, a Instrução Normativa em análise estabelece que as diretrizes institucionais devem ser formalizadas, contemplando, no mínimo, os aspectos:

I. consonância com a missão do órgão ou da entidade, considerando sua estrutura, natureza do negócio e sua complexidade;

II. compromissos claros com relação às obrigações legais e regulamentares;

III. identificação de autoridades do órgão ou da entidade e delegações necessárias, incluindo os responsáveis por continuidade de negócios na instituição;

IV. critérios para o tipo e a escala dos incidentes a serem tratados;

V. referências às normas, aos regulamentos ou às políticas; e

VI. compromisso de realizar e manter a continuidade do negócio da instituição.

Segundo o artigo 23, o Plano de Continuidade de Negócios deve conter requisitos mínimos: objetivo; as atividades críticas de negócio a serem contempladas no plano; os requisitos para ativação do plano e o tempo máximo aceitável de permanência da falha; o responsável pela ativação do plano, com seus respectivos dados de contato; e o responsável por aplicar as medidas de contingência definidas.

O GSI exige, a partir dessa norma, o manejo de Segurança da Informação. A ISO 27001/2013, no item 4.4, trata do assunto:

> 4.4 Sistema de gestão da segurança da informação: a organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação, de acordo com os requisitos desta Norma.

Essa gestão deverá garantir o planejamento, a organização, a direção e o controle das melhores práticas de segurança, visando a

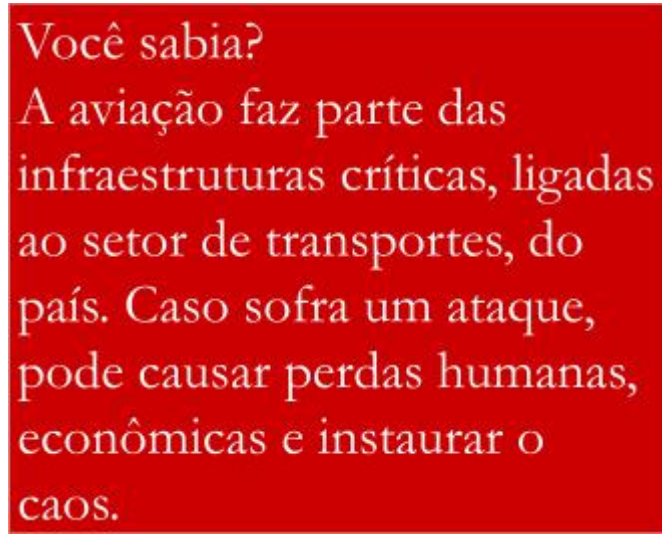
confidencialidade, autenticidade e integridade da informação. E o Estado, sem dúvida, deve primar pelo exemplo, instituindo, no seu âmbito de competência, o gerenciamento eficaz da Segurança da Informação.

Capítulo 11 - Manual de Conscientização sobre Cibersegurança - ANAC

A Agência Nacional de Aviação Civil - ANAC é um dos sistemas de infraestrutura crítica nacional. Recentemente, a Agência lançou um manual sobre cibersegurança para promover a conscientização sobre Segurança da Informação, aplicado a todos os indivíduos que participam do sistema de aviação civil brasileiro.

O manual possui também o intuito de auxiliar os responsáveis pela AVSEC (*Aviation Security*) da aviação civil na promoção e divulgação da importância do zelo pela segurança dos ativos de Tecnologia da Informação e da Comunicação.

Considera que a informação é um ativo de ampla relevância em qualquer tipo de organização. No caso de aeroportos e empresas aéreas,



essa constatação não poderia ser diferente: esse tipo de ativo possui uma dupla sensibilidade, pois a informação permite que o serviço seja prestado ao usuário final ao mesmo tempo em que gera uma série de vulnerabilidades que podem comprometer a segurança das organizações, ou seja, é extremamente importante, tanto do ponto de vista operacional quanto do ponto de vista da segurança.

O artefato leva em conta que a segurança cibernética ganha especial relevância quando aplicada às instalações críticas, pois, se os serviços forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional.

A aviação faz parte desses sistemas críticos, na vertente do setor de transportes. Nos aeroportos estão concentrados alguns dos principais sistemas de infraestrutura crítica de grande impacto, como telecomunicações, energia e água. Todos estes setores estão relacionados na constituição e operações aéreas, fazendo parte da sua infraestrutura crítica que requer um alto nível de segurança cibernética. Além disso, em geral, todos estes setores fazem uso da Tecnologia da Informação e Comunicação (TIC) instalada no aeroporto.

O manual publicado especifica que todas as organizações envolvidas no setor de aviação civil, sejam elas públicas ou privadas, devem realizar a conscientização em cibersegurança. Para que isso ocorra, exige que cada uma delas aponte:

I. Um setor responsável pela segurança cibernética;

II. A instituição de responsabilidades de todos os profissionais com relação à segurança, garantida através da assinatura de termo de compromisso ou responsabilidade – Política de Uso;

III. A responsabilidade dos gestores e coordenadores em supervisionar suas equipes, divulgar e disseminar medidas preventivas, desenvolvendo uma cultura de Segurança da Informação.

Portanto, o desenvolvimento da gestão de Segurança da Informação deve ser contínuo e periódico, com ações de conscientização que permitam que todos os usuários compreendam as consequências que um ataque pode causar.

O manual publicado pela ANAC visa destacar aspectos dos maiores riscos e desafios relacionados a ataques direcionados para organizações da aviação civil, sobretudo em aeroportos.

Os sistemas de segurança de TIC aplicam-se a pessoas, procedimentos, dados, software e hardware que são usados para reunir e analisar informações analógicas e digitais usadas no gerenciamento das atividades da aviação civil.

O uso de sistemas de conexão em rede, acesso a serviços de voo pela web, entretenimento a bordo, armazenamento e

compartilhamento de dados em nuvem, conectividade de dispositivos móveis e serviços de sistemas de navegação aérea são alguns exemplos do uso dessas novas tecnologias na aviação civil.

Já existem lugares onde um passageiro pode adquirir seu bilhete de passagem e ir da sua origem ao seu destino de forma 100% digital, sem necessidade de interagir com pessoas. Assim, dadas as facilidades e os benefícios obtidos, a aviação civil está cada vez mais dependente da disponibilidade de sistemas de Tecnologia da Informação e Comunicação, bem como da integridade e confidencialidade dos dados.

Se informações confidenciais caírem em mãos de entidades não autorizadas, esta violação de segurança poderá afetar a aviação civil de forma significativa, interferindo nas operações aéreas e podendo levar, inclusive, a perdas de vidas.

Ao mesmo tempo, atrelado ao crescimento das facilidades proporcionadas por estas tecnologias da era cibernética, surgem também novas ameaças e riscos ao ambiente do transporte aéreo. Tal fato exigiu que temas como risco cibernético, ameaça, incidente, ataque e segurança cibernética estejam presentes na agenda dos Estados da comunidade internacional de aviação civil.

O manual recomenda que os sistemas de TIC sejam protegidos com o desenvolvimento e adoção de políticas de segurança, indicando quais funções e processos são críticos a fim de protegê-los, garantindo a confidencialidade, disponibilidade e integridade dos sistemas e seus

dados.

Da mesma forma, indica a necessidade de treinamento dos recursos humanos em ações de conscientização, inclusive do pessoal de manutenção e tripulação das aeronaves. Eles devem compreender como os sistemas podem ser atacados, incluindo noções de engenharia social; medidas de precaução que podem ser adotadas para impedir ou minimizar o ataque e suas consequências; quais possíveis recursos são alterados ou têm sua operação afetada; e procedimentos de contingência no caso de suspeita de um ciberataque.

Para a proteção das redes de computadores, recomenda-se a segmentação física ou lógica em zonas baseadas sobre sua função, uso e níveis de segurança. A conectividade a outros sistemas operacionais deve ser limitada ao mínimo possível. Em pontos nos quais as redes não podem ser separadas, todas as conexões e acessos devem ser continuamente monitorados por ferramentas de diagnóstico de redes.

Recomenda-se que, por princípio, todas as conexões de rede devam ser consideradas inseguras, a menos que um acordo específico de interconexão tenha sido estabelecido entre as entidades operacionais envolvidas na interconexão. Tais conexões devem ser documentadas, revisadas e atualizadas quando necessário com proteção contra intrusão no ponto final, o que pode ser conseguido com Sistemas de Detecção de Intrusão (*Intrusion Detection System* - IDS).

A fim de fornecer mais robustez à segurança das redes contra

ciberataques, o operador deve estabelecer um programa de monitoramento que utilize escaneamento de vulnerabilidades, teste de penetração (*pentest*) e escaneamento para descoberta de serviços não autorizados.

Os fornecedores, por sua vez, devem informar como a operação do sistema é segura, incluindo o modo como o suporte e a manutenção são realizados. Quando a manutenção é realizada por empresas terceirizadas, é importante que o número de indivíduos que têm acesso ao software e ao hardware seja limitado e todo o processo de acesso, documentado.

Os fornecedores devem mostrar que suas medidas de segurança são adequadas para proteger os sistemas críticos e seus dados, que são capazes de detectar intrusos e ataques, e que estão aptos a recuperá-los.

Os fornecedores de software e hardware devem usar recursos legítimos e com boa reputação, além de garantir suporte seguro durante todo o ciclo de vida do sistema.

No tocante ao controle de acesso aos sistemas críticos e a seus dados, os direitos administrativos dos usuários devem usar o conceito do privilégio mínimo, e o acesso remoto só deve ser permitido em circunstâncias específicas e com dados criptografados. O pessoal responsável pelo suporte e manutenção deve ser autorizado, ter número limitado e só realizar o trabalho em horários acordados.

Recomenda-se que os operadores do setor aéreo se certifiquem

que os fornecedores de hardware e software confirmem que não existem acessos escondidos em seus sistemas que possibilitem um acesso não autorizado.

É importante que o operador realize periodicamente testes de invasão, inspeções e auditorias em toda a infraestrutura do sistema crítico de Tecnologia da Informação e Comunicação, para se certificar que todo o sistema de controle de acesso está funcionando adequadamente e que é capaz de resistir a situações emergenciais, como ataques cibernéticos.

Em outubro de 2019, durante a 40ª Assembleia da Organização Civil da Aviação Internacional[10], foi publicada a Estratégia de Cibersegurança para a Aviação, afirmando que, na sua visão, o setor da aviação civil é resiliente a ciberataques e que permanece seguro e confiável globalmente, enquanto continua a inovar e crescer.

Esta estratégia se alinha com outras iniciativas da OACI relacionadas a cibersegurança e coordenadas com o gerenciamento da segurança operacional ("*safety*") e segurança contra atos de interferência ilícita ("*security*"). Ela será alcançada através de um conjunto de medidas, ações e princípios contidos em uma estrutura construída sobre sete pilares: cooperação internacional, governança, legislação e regulações efetivas, política de cibersegurança, compartilhamento de informações,

[10] International Civil Aviation Organization (ICAO, na sigla em inglês) é uma agência especializada das Nações Unidas criada em 1947 com 191 países-membros

gerenciamento de incidentes e planejamento de emergência, além de capacitação, treinamento e cultura de cibersegurança.

Observava-se na Resolução A39-19 da Assembleia da OACI, realizada em 2016, a convocação da comunidade da aviação civil a implementar ações para entender e debelar ameaças cibernéticas contra os sistemas e os dados da aviação civil, estimulando os países membros a trabalharem de forma colaborativa para desenvolver um protocolo visando enfrentar os desafios da cibersegurança.

Um dos resultados obtidos com aquela resolução foi a criação do Grupo de Trabalho do Secretariado sobre Segurança Cibernética (SSCG), cuja função é estabelecer ações a serem adotadas pelos Estados e partes interessadas do sistema aéreo para contrapor às ameaças cibernéticas, além de compartilhar informações relacionadas a ameaças, incidentes e ações de mitigação de riscos.

O manual da ANAC também trata da importância de uma política de Segurança da Informação para definir os direitos e as responsabilidades de cada um, e estabelece as penalidades às quais o agente está sujeito em caso de descumprimento. Assim, é possível deixar claro o comportamento esperado de cada usuário do sistema.

O aumento da probabilidade de violação da segurança das informações e dados utilizados se deve principalmente às vulnerabilidades encontradas nas novas tecnologias, como ataques com utilização de vírus de computador ou outro software malicioso, falhas

nos sistemas ou corrupção de dados, ou através do roubo de ativos ou outros incidentes causados por algum membro da equipe.

Diante disso, o manual elenca alguns motivos para uma organização implementar um programa de segurança cibernética:

I. Evitar a interrupção dos serviços;

II. Evitar a perda de vidas e danos à propriedade;

III. Evitar vazamento de informação;

IV. Preservar a reputação da organização;

V. Conformar os requisitos da legislação sobre o assunto;

VI. Proteger a saúde e a segurança dos empregados; e

VII. Obter um perfil de menor risco.

Dentre os principais alvos para aumentar a segurança cibernética estão os aeródromos, as instalações físicas do controle de tráfego aéreo, os sistemas de gestão de passageiros e cargas de empresas aéreas e de controle de tráfego aéreo, aeronaves, sistemas de Tecnologia

da Informação e Comunicação, sistemas de instalações e manutenção, além de órgãos de regulação.

O texto afirma que o cibercriminoso pode ser qualquer um que tenha uma motivação específica: pessoas, organizações e mesmo nações e Estados. No caso de pessoas, podem ser terroristas, ativistas, criminosos, curiosos, vândalos, funcionários etc. No campo das organizações, elas podem ser criminosas, terroristas, empresas concorrentes, empresas terceirizadas (equipe de segurança física, de limpeza, de TI etc.), ativistas. E, a nível de Estados e Nações, podem ser grupos financiados por Estados hostis.

Entre as motivações para atacar a aviação civil, podemos considerar: ganho financeiro, fraude, *ransomware,* espionagem industrial, destruição, diminuição de reputação, interrupção de serviços, ativismo, ações de geopolítica, obtenção de elogios, ações antagônicas aos interesses do Estado ou Nação etc.

As ameaças também podem ocorrer por desconhecimento ou falta de conscientização, comprometendo a política de Segurança da Informação da organização. Exemplos deste tipo ocorrem quando um profissional se ausenta do seu posto de serviço, que pode ser um ponto de identificação de passageiros, e deixa o computador logado no sistema, ou mesmo quando conecta um dispositivo USB pessoal ao computador da organização onde trabalha.

Ao elencar as ameaças, a ANAC cita várias fontes: alguém das

equipes do aeroporto com intenções maliciosas; passageiros ou pessoas fisicamente no aeroporto com intenções maliciosas; infecção de sistemas por malwares; falhas, acidentais ou ambientais, em software ou em equipamentos que podem causar incidentes de segurança.

Abaixo se encontram alguns exemplos de ataques contra a aviação civil ao redor do mundo:

2010 – o acidente da Spanair que ocorreu em 2008. Investigações revelaram que o sistema informático central utilizado para monitorar problemas técnicos no avião foi infectado com malware;

Julho de 2013 – o aeroporto de Istambul Ataturk e o aeroporto internacional de Sabiha Gokcen foram vítimas de um ataque de malware. Os cibercriminosos tentaram roubar dados do sistema de controle de passaporte dos aeroportos. Muitos voos foram atrasados;

Agosto de 2013 - um motorista de caminhão equipado com um rastreador de GPS ilegal interferiu nos sinais usados pelo sistema de navegação no solo no aeroporto de Newark;

Setembro de 2013 – Japan Airways informou que até 750.000 clientes do seu programa de milhas tiveram informações pessoais comprometidas devido a um ciberataque;

Outubro de 2013 – a companhia aérea malaia Malindo Air teve a conta do Twitter hackeada, e o hacker postou o anúncio falso de que a companhia estaria oferecendo 100.000 assentos grátis;

Março de 2014 – a Autoridade de Aviação Civil da Malásia foi hackeada um dia depois do informe do voo MH370 através de um e-mail com um documento com extensão "PDF" anexado;

Novembro de 2014 – cerca de 10 websites do governo da Jamaica, incluindo o da autoridade de aviação civil jamaicana, foram alvos de um ataque de negação de serviço (DoS);

Dezembro de 2014 - uma grande falha de computador no principal centro de controle de tráfego aéreo em Londres causou massivas interrupções nos voos chegando e partindo do "*hub*" global;

Janeiro de 2015 – o website da Malaysia Civil Aviation foi invadido por um grupo se declarando do cibercalifado Lizard Squad;

Março de 2015 – a empresa British Airways congelou seu "programa de passageiro frequente" após um programa de computador automatizado procurar por vulnerabilidades em seus sistemas;

Junho de 2015 – hackers violaram os computadores da companhia

aérea polonesa LOT, usados para emitir planos de voo. Como resultado do ataque, o Hub de Varsóvia não pode criar planos de voo, deixando 1400 passageiros em terra no aeroporto Chopin em Varsóvia. O ciberataque foi do tipo negação de serviço (DoS);

Novembro de 2015 – o uso de uma versão obsoleta do sistema operacional causou uma interrupção no Aeroporto de Orly Paris. A falha afetou um sistema conhecido por Décor, que executa sobre o Windows 3.1, e é usado para os controladores aéreos comunicarem informações meteorológicas aos pilotos;

Janeiro de 2016 – o Aeroporto Internacional de Kiev Boryspil teve seu sistema de TI, incluindo o controle de tráfego aéreo, atacado por um malware. O servidor de onde se originou o ataque se encontrava na Rússia;

Março de 2016 – um cibercriminoso do Vietnã, Le Duc Hoan Hai, utilizando a credencial de um terceirizado conectado ao Aeroporto de Perth, acessou o sistema de computadores e roubou informações de segurança do aeroporto sobre medidas de segurança física e de projeto do local;

Abril de 2016 - após o pouso, o piloto de um voo da British Airways vindo de Genebra informou uma colisão com um drone enquanto se

aproximava do aeroporto London Heathrow em 17 de abril. O incidente destacou os problemas enfrentados em relação aos drones. Embora a ameaça de colisão com aves tenha sido bem pesquisada, ainda há poucos dados sobre quanto dano um drone poderia causar a um avião;

Julho de 2016 – um grupo conhecido como "China 1937CN Team" comprometeu os sistemas de anúncio por voz e sistemas de informação de voo dos principais aeroportos do Vietnã. Estavam motivados por disputas territoriais no Mar da China. Como resultado deste ataque, autoridades vietnamitas realizaram uma verificação abrangente dos dispositivos chineses e tecnologia para garantir a Segurança da Informação nos seus aeroportos;

Julho de 2016 - uma falha de terceiros no aeroporto de Roma Fiumicino, na Itália, originou a interrupção do sistema de check-in automático de passageiros, o que causou atrasos de duas horas na operação de inspeção de passageiros. A falha estava relacionada ao provedor de Internet que o aeroporto usa para acessar e processar dados de passageiros, utilizado para o check-in automático de passageiros;

Agosto de 2016 – milhares de passageiros ao redor do mundo ficaram

presos depois que um corte de energia obrigou a companhia aérea americana Delta a suspender os voos. Ocorreu uma falha de energia durante a noite em Atlanta, perto da sede da Delta, causando falha nos sistemas de computador. O sistema de check-in do aeroporto, sistemas de informação, telas de aviso de passageiros, o website da companhia aérea e aplicativos para smartphones foram afetados pela falha do sistema;

Abril de 2017 – uma empresa contratada pela Delta Airlines para serviço de "chat" online estava envolvida em um ciberincidente que levou à exposição de informação de pagamento de seus clientes e da própria Delta;

Você sabia?
De 2010 a março de 2021, foram registrados 27 ataques cibernéticos contra a aviação civil em todo o mundo.

Março de 2018 – a companhia aérea Cathay Pacific, sediada em Hong Kong, sofreu a maior violação de dados da aviação quando hackers acessaram 860.000 números de passaportes, 245.000 números de cartões de identidade de Hong Kong, 403 números de cartões de crédito expirados e 27 números de cartões de crédito válidos sem o código CVV. A companhia demorou 7 meses para informar a violação

e teve uma queda considerável em seu valor de mercado;

Junho de 2018 – atacantes interferiram no sistema de informação de voo do aeroporto de Tabriz no Irã, em protestos contra medidas adotadas pelo governo;

Setembro de 2018 – o aeroporto de Bristol sofreu um ciberataque (*ransomware*) e ficou dois dias sem serviço de informação de voo. Os sistemas afetados foram restabelecidos manualmente;

Janeiro de 2020 - uma página suspeita de Facebook, chamada RyanairUK, informando ser a página oficial da Ryanair, enganava as pessoas dando a falsa esperança de uma viagem gratuita, e ainda apresentava um endereço web considerado suspeito;

Janeiro de 2020 – no aeroporto de Portland, um viajante plugou seu Playstation 4 e começou a jogar em um monitor que mostrava um mapa do aeroporto;

Janeiro de 2020 – pesquisadores de segurança acessaram a base de dados da empresa aérea indiana SpiceJet usando uma combinação fácil de caracteres de senha e encontraram informações pessoais não criptografadas de 1,2 milhão de passageiros;

Novembro de 2020 – a Embraer informou que sofreu ataque cibernético aos seus sistemas de tecnologia de informação, que resultou na divulgação de dados supostamente atribuídos à empresa, indisponibilizando o acesso a apenas um único ambiente de arquivos da Companhia;

Março de 2021 – ataque hacker sofrido pela multinacional SITA (empresa que presta serviços de Tecnologia da Informação ao setor aéreo) expôs dados de passageiros no Brasil. O ataque foi direcionado a parte dos membros de programas de fidelidade.

De acordo com o Diretor de Estratégia e Gerenciamento de Segurança da Agência Europeia de Segurança da Aviação, ocorrem cerca de 1.000 ciberataques por mês a aeroportos em todo o mundo. Em adição, como exemplo da extensão das ameaças, a Cathay Pacific Airways, empresa aérea de Hong Kong, sofreu a maior quantidade de ataques cibernéticos no ano de 2018, sendo que um deles resultou no vazamento de 9,4 milhões de registros de dados.

Os sistemas de TIC foram originalmente projetados para fornecer disponibilidade, mas não segurança. Do mesmo modo, foram construídos de forma isolada com relação aos sistemas de Tecnologia Operacional (ex.: carroceis de bagagem, controle de iluminação etc.),

que também precisam ser protegidos contra ataques cibernéticos. Assim, a superfície de ataques cibernéticos cresceu com a integração da Tecnologia da Informação e das Comunicações (TIC), com a Tecnologia Operacional (TO), pois os invasores agora são capazes de explorar lacunas de segurança em redes de TIC e, depois, moverem-se lateralmente para sistemas de TO, que são bem menos protegidos.

O Gabinete de Segurança Institucional da Presidência da República do Brasil criou os Grupos Técnicos de Segurança de Infraestrutura Críticas (GTSIC), para tratar da proteção de áreas prioritárias para o Brasil, sendo o setor de transporte aéreo um deles.

O Subgrupo Técnico de Segurança de Infraestruturas Críticas de Transportes Aéreos (SGTSIC-TA) tem por objetivo identificar e avaliar as vulnerabilidades das infraestruturas consideradas críticas para o setor, avaliar riscos e articular medidas para implementar um sistema de informação sobre tais infraestruturas.

Embora o manual publicado pela ANAC tenha uma abordagem ampla dos aspectos da Segurança da Informação nos mais diversos níveis, suas diretrizes são comuns a diversas outras áreas. Trata-se de uma ação de fomento da cultura de segurança, uma vez que as ameaças cibernéticas são cada vez maiores.

Capítulo 12 - Circular SUSEP 638

A Superintendência de Seguros Privados - SUSEP, publicou, no dia 03 de agosto de 2021, uma Circular que dispõe sobre requisitos de segurança cibernética a serem observados pelas seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradoras.

A Circular estabelece que a segurança cibernética deverá estar inserida no contexto geral do Sistema de Controles Internos (SCI) e Estrutura de Gestão de Riscos (EGR), mas que a supervisionada deve exercer controles complementares nacionais e internacionais de boas práticas como: segurança física de equipamentos e instalações; controle de acesso aos sistemas e informações; uso de criptografia; uso de software contra malwares; backups; manutenção de registros (logs) de atividades dos usuários, de exceções de segurança e falhas; uso de técnicas de segurança de redes e de segurança das comunicações; promoção de treinamentos de conscientização de colaboradores e desenvolvimento e aquisição de sistemas.

A Circular considera que os riscos cibernéticos devem ser considerados na categoria risco operacional, de uso obrigatório. Portanto, exige que as empresas sob supervisão da SUSEP tenham uma política de segurança que contemple, no mínimo:

I. os objetivos da Segurança da Informação;

II. o compromisso da alta administração com a Segurança da Informação, estabelecimento de processos, controles, monitoramento e melhoria contínua;

III. parâmetros e diretrizes para classificação de dados, incidentes e serviços, de acordo com a sua relevância;

IV. implementação de processos, procedimentos e controles de segurança cibernética;

V. terceirização de serviços de processamento e armazenamento de dados, incluindo requisitos mínimos e alçadas relativas à aprovação e alteração de contratos.

Determina que a supervisionada deverá possuir e manter atualizados processos, procedimentos e controles efetivos para identificar e reduzir vulnerabilidades de forma proativa e detectar, responder e recuperar-se de incidentes.

Esses processos, procedimentos e controles deverão contemplar, no mínimo:

I. monitoramento contínuo da rede de comunicação, por meio de

técnicas que auxiliem na detecção de incidentes;

II. avaliação da natureza, abrangência e impacto dos incidentes detectados, de acordo com graus de criticidade, considerando a relevância dos dados, sistemas ou serviços envolvidos e seu grau de comprometimento;

III. adoção de medidas para a contenção dos efeitos do incidente;

IV. restabelecimento dos sistemas ou serviços afetados e retorno à sua condição normal de operação;

V. registro dos incidentes;

VI. compartilhamento de informações sobre incidentes relevantes com as demais supervisionadas;

VII. comunicação com as partes afetadas pelo incidente, sobretudo clientes; e

VIII. identificação e tratamento das vulnerabilidades exploradas.

As medidas de contenção deverão incluir comunicação prévia com prestadores de serviços, parceiros e outras partes potencialmente

envolvidas, com vistas à adoção de uma resposta coordenada.

Outra diretriz é que a supervisionada deverá implementar mecanismos de conciliação entre o registro de incidentes e o Banco de Dados de Perdas Operacionais (BDPO), se existente, pelo menos para os incidentes que resultem em perda operacional.

No plano de continuidade deverão constar a avaliação da natureza, da abrangência e impacto dos incidentes; as medidas de contenção e de restauração a serem adotadas, principalmente no caso de danos à infraestrutura ou sistemas considerados críticos, em caso de alteração, exclusão, modificação ou divulgação de dados relevantes ou interrupção de serviços relevantes de processamento e armazenamento de dados.

Em caso de incidente, a SUSEP deverá ser comunicada em até cinco dias úteis a partir da ocorrência do fato, com o detalhamento da extensão dos danos e das ações tomadas.

A segurada elaborará um relatório anual sobre prevenção e tratamento de incidentes, que deverá conter:

I. descrição dos incidentes relevantes detectados, com detalhamento das causas, efeitos e respostas;
II. dados estatísticos com a totalidade dos incidentes, com sua quantidade e principais causas e efeitos;

III. resultados de testes dos cenários previstos no plano de continuidade de negócios;

IV. descrição das principais vulnerabilidades identificadas e das ações adotadas para seu tratamento, com a indicação dos responsáveis pela sua concretização e prazos.

Esse relatório deverá ser encaminhado aos órgãos de administração, aos comitês de auditoria e riscos e ao diretor responsável pelos controles internos ou unidade de gestão de riscos.

Quando houver terceirização de serviços de processamento e armazenamento de dados, a supervisionada deverá constatar que a terceirizada dispõe dos recursos, competências e práticas de governança necessários ao adequado monitoramento dos serviços.

No caso de serviços relevantes de processamento e armazenamento de dados, as supervisionadas deverão informar à SUSEP, em até 30 dias após a formalização dos contratos, quais os serviços relevantes contratados e a denominação da terceirizada e, quando possível, os países onde esses serviços poderão ser prestados e os dados armazenados, processados e gerenciados. O mesmo se aplica no caso das alterações contratuais.

Em relação aos serviços relevantes de processamento e armazenamento de dados, a supervisionada deverá recorrer a pelo

menos um dos seguintes procedimentos: exigência de certificação, relativa ao serviço a ser contratado, concedida por instituição independente; ou realização de diligências prévias (*due diligence*).

Os contratos de prestação de serviços de processamento e armazenamento de dados, exceto quando de adesão, deverão dispor expressamente sobre essas exigências.

Interessante observar que a Circular se aplica a toda e qualquer terceirização de serviços de processamento e armazenamento de dados, inclusive de computação em nuvem, com exceção apenas do serviço de registro das operações da supervisionada em sistema de registro previamente homologado pela SUSEP e administrado por entidade registradora devidamente credenciada.

Os contratos de terceirização de serviços de processamento e armazenamento de dados firmados antes da data de início de vigência da Circular deverão ser adequados até 1º de setembro de 2024.

A Circular entrou em vigor em 1º de setembro de 2021.

Capítulo 13 - Adesão à Convenção Europeia sobre o Crime Cibernético

No plano do combate à criminalidade digital, o Governo Federal encaminhou, em julho de 2021, o Projeto de Decreto Legislativo 255/21. A Câmara dos Deputados deverá analisar e, se concordar, ratificar a adesão do Brasil à Convenção Europeia sobre o Crime Cibernético assinada em Budapeste em 2001.

O objetivo da Convenção é intensificar a cooperação dos Estados signatários no combate aos crimes cibernéticos.

Há um ponto de destaque interessante: a necessidade de proteção dos interesses legítimos quanto ao uso e desenvolvimento de tecnologias da informação.

O documento apresenta preocupação com a preservação das informações e dados no ciberespaço, que devem ter asseguradas a confidencialidade, integridade e disponibilidade. No caso de violação de um destes pilares, deverá existir a tipificação penal para coibir práticas delituosas. Para isso, os países signatários deverão autorizar o uso de mecanismos de combate a esta espécie de crime, disponibilizando instrumentos que facilitem a detecção, a investigação e a instauração de procedimentos criminais a nível nacional e internacional, com

cooperação internacional rápida e confiável.

Entre os temas tratados na convenção encontram-se:

I. Imposição de penalidades para violações e invasões a dados e sistemas, acesso não autorizado, interceptação de dados, alteração da integridade através de dano, exclusão ou deterioração, obstrução ao funcionamento de um sistema;
II. Criminalização da produção, venda, distribuição, utilização e importação de dispositivos e palavras-passe, códigos ou dados que tenham por objetivo permitir a prática de qualquer das atividades criminosas acima;
III. Criminalização da alteração de dados que tenham tido sua autenticidade comprometida;
IV. A exigência de penalidade para ações com objetivo de causar prejuízo ou obter vantagem econômica através de invasões, alterações, bloqueios ou quaisquer formas de alteração das características de confidencialidade, integridade e autenticidade de dados ou sistemas;
V. Considera pornografia infantil crime, seja com a produção, distribuição, armazenamento ou oferecimento de material de conteúdo sexual de pessoas com menos de 18 anos (admite-se redução de 16 anos); e
VI. Violações a direitos autorais.

A Convenção enfatiza a necessidade de armazenamento de dados pelos fornecedores de serviços cibernéticos por um determinado período, sendo possível que as autoridades tenham acesso aos dados dos usuários nos casos de investigações previstas.

Interessante notar que os Estados devem adotar medidas legais para investigar quais infrações são cometidas no seu território, a bordo de navio ou aeronave ou, ainda, se foi praticada por algum de seus nacionais.

A Convenção prevê a extradição de cibercriminosos. Também dispõe sobre compartilhamento de dados das investigações para repressão de crimes cibernéticos.

É um mecanismo voltado para o combate aos crimes cibernéticos a nível global, trazendo a responsabilização para aqueles que se escondem nas brumas da indefinição legal.

CONCLUSÃO

O material apresentado neste e-book demonstra a preocupação crescente com a temática da Segurança da Informação, seja no âmbito nacional ou internacional.

O ano de 2021 tem sido marcado por constantes invasões de sistemas, relatos de ransomware e outras modalidades criminosas, que indicam que a regulamentação se tornou uma urgência.

Até agora, os cibercriminosos se beneficiaram da falta de uma legislação que os adeque aos sistemas criminais. No entanto, esta realidade vem mudando, conforme demonstrado na Convenção Europeia sobre o Crime Cibernético.

O Brasil, por sua vez, tem se dedicado a proteger suas infraestruturas críticas e órgãos da administração pública federal. Esta será, certamente, uma necessidade cada vez mais acentuada diante da presença, cada vez maior, da tecnologia nas nossas vidas.

Referências Bibliográficas

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. Disponível em <https://www.gov.br/anac/pt-br/noticias/2021/anac-lanca-primeiro-manual-sobre-seguranca-cibernetica-na-aviacao-civil>. Acesso em 12 ago. 2021

BRASIL. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>. Acesso em 25 de out. de 2021.

BRASIL. Disponível em BRASIL. Disponível <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10641.htm>. Acesso em 25 de out. de 2021.

BRASIL. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>

CORREIO BRAZILIENSE. Disponível em <https://www.correiobraziliense.com.br/tecnologia/2021/07/4935247-brasil-sobe-53-posicoes-no-ranking-mundial-de-ciberseguranca-da-onu.html>. Acesso em set. 2021.

CNN BRASIL. Disponível em: <https://www.cnnbrasil.com.br/business/ataques-ciberneticos-a-empresas-brasileiras-crescem-220-no-1-semestre-de-2021/>. Acesso em 17

set. 2021.

GABINETE DE SEGURANÇA INSTITUCIONAL. Disponível em <Nova Posição do Brasil no Ranking de Cibersegurança da ONU — Português (Brasil) (www.gov.br)>. Acesso em 02 ago. 2021.

GABINETE DE SEGURANÇA INSTITUCIONAL. Disponível em <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215>. Acesso em 07 ago. 2021.

GATEFY. Disponível em <https://gatefy.com/pt-br/blog/relatorio-fbi-ic3-cibercrimes-2020/>. Acesso em 25 out. de 2021.

GLOBAL DIGITAL POPULATION AS OF JULY 2019 (IN MILLIONS). STATISTA. Disponível em <https://www.statista.com/statistics/617136/digital-population-worldwide/>. Acesso em set. de 2021.

IC3 2020 Internet Crime Report. Disponível em <https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf>. Acesso em 25 out. de 2021

IMPRENSA NACIONAL. Disponível em <https://www.in.gov.br/en/web/dou/-/circular-susep-n-638-de-27-de-julho-de-2021-335760591>. Acesso em 12 ago. 2021.

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2018. European Union Agency for Law Enforcement Cooperation, Europol. Disponível em:

<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018>. Acesso em 20 set. 2021.

NOOMIES. Disponível em: <Brasil ganha 53 posições em ranking global de cibersegurança (febraban.org.br)>. Acesso em 17 set. 2021.

OLIVER WYMAN. Disponível em <https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html>. Acesso em 20 set. 2021

PALÁCIO DO PLANALTO. Disponível em <www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>. Acesso em 07 ago. 2021.

TELE.SÍNTESE. Disponível em <ANPD inicia monitoramento de práticas de tratamento de dados em 2022 - TeleSíntese (telesintese.com.br)>. Acesso em 02 ago. 2021.

WORLD ECONOMIC OUTLOOK REPORTS. INTERNATIONAL MONETARY FUND. Disponível em <https://www.imf.org/en/Publications/WEO/Issues/2019/03/28/world-economic-outlook-april-2019>. Acesso em set. de 2021.

Sobre o Autor

Abian Laginestra é profissional na área de Tecnologia da Informação há 25 anos, e de Segurança da Informação e defesa cibernética há 18 anos. Possui graduação em Gestão de Processos Gerenciais - FGV/EBAPE, MBA em Gestão da Segurança da Informação pelo INFNET e cursa Mestrado no Programa de Pós-Graduação em Segurança Internacional e Defesa na Escola Superior de Guerra - ESG. Concluiu cursos para desenvolvimento profissional como: AWS Black Belt Security; Human Change Management Body of Knowledge (HCMBOK); e ISO 31000 - Gestão de Riscos.

Ao longo da carreira, contribuiu significativamente em empresas dos setores financeiro, farmacêutico, governamental, jurídico e informática. Com expertise na condução de projetos estratégicos de Segurança da Informação, e participação ativa na área de compliance, possui domínio das melhores práticas de segurança: ISO 27001, ISO 31000, CIS, Cloud AWS, ITIL, COBIT, ISA-99 e PMI.

É consultor e especialista em cibersegurança, atuando como Chief Information Security Officer - CISO. Ao longo dos últimos anos, figurou em listas como Top 150 profissionais do Ano em TI – 2019 – IT Fórum; Security Leaders 2018 - 3ª posição na categoria Banco Digital; CIO IT Leaders 2017; e CIO IT Leaders 2015.