campos thomaz
advogados

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

SÉRIE PRIVACIDADE E PROTEÇÃO DE DADOS

1. CONCEITOS RELEVANTES

A. O que é segurança da informação?

Segurança da Informação pode ser definida como o conjunto de práticas aptas proteger as informações e os sistemas de informação contra acessos não autorizados, usos, divulgações, interrupções, modificações e/ou destruições.

O conceito de Segurança da Informação abrange, portanto, uma ampla gama de áreas, estratégias, tecnologias, políticas e procedimentos destinados a salvaguardar o que chamamos de tríade da Segurança da Informação[1], quais sejam:

Confidencialidade

proteção de informações confidenciais contra divulgação e/ou acesso não autorizado. Em linhas gerais, a confidencialidade pode ser alcançada pelas organizações com a implementação de controles de acesso e criptografia nos sistemas da organização. Cabe destacar que, ao não garantir a confidencialidade das informações, a organização é possível que ocorra exposição de conteúdos, o alcance de informações pessoais por terceiros não autorizados, de forma a gerar prejuízos contratuais, financeiros e até à imagem da empresa.

Disponibilidade

garantia de que os sistemas de informação e as informações de determinada organização estarão acessíveis e utilizáveis quando necessário. O bloqueio de informações e/ou sistemas de informações pode interromper o andamento de procedimentos internos da organização e, assim, causar prejuízos à continuidade dos negócios da organização. Nesse sentido, relevante informar que a disponibilidade das informações e dos sistemas de informação das organizações pode ser garantida com a implementação de sistemas de redundância, backup e recuperação de informação.

Integridade

proteção da informação contra modificação não autorizada, destruição ou corrupção, ou seja, à garantia de que a informação será sempre precisa, completa e confiável. A integridade pode ser alcançada pelas organizações por meio da implementação de procedimentos de validação de informação e controles de acesso. Nesse sentido, a ausência de integridade das informações armazenados por determinada organização pode levar à prática de crimes contra a organização que armazena tais informações e, portanto, causar danos materiais e reputacionais à ela.

Portanto, o objetivo da segurança da informação é impedir o acesso não autorizado à informação; garantir a exatidão e integridade da informação; e manter a disponibilidade dos sistemas de informação de determinada organização.

[1] Nesse sentido, cabe destacar que existem outros modelos e estruturas de segurança da informação além da tríade acima mencionada, que estabelecem que a segurança da informação possui outros fundamentos adicionais, tais como responsabilidade, autenticidade e não-repúdio (os quais não serão abordados neste material por fins meramente didáticos).

B. O que é um Incidente de Segurança da Informação?

Tendo em vista o conceito de Segurança da Informação abordado anteriormente, diz-se que um incidente de segurança da informação é um evento que resulta (ou pode resultar) no comprometimento, violação ou divulgação indevida ou não autorizada de informações confidenciais, sensíveis ou protegidas.

Ou seja, um incidente de segurança da informação pode ocorrer quando há: (i) um vazamento de dados; (ii) um ataque cibernético; (iii) acesso não autorizado à informações confidenciais e/ou sensíveis; (iv) um roubo ou perda de dispositivos contendo informações confidenciais; e/ou (v) uma divulgação indevida ou acidental de determinada informação confidencial.

Aqui, relevante destacar que incidentes de segurança da informação ocorrem de forma corriqueira dentro das organizações. Isso porque, situações como o furto de um notebook e a interrupção de acesso a um sistema são, do ponto de vista técnico, incidentes de segurança, na medida em que uma informação confidencial pode estar exposta a uma ameaça.

Não à toa, o impacto de um incidente de segurança da informação pode variar de acordo com os fatos relacionados ao incidente, isto é, de uma pequena inconveniência a consequências graves, como perdas financeiras, danos à reputação e penalidades legais.

Por este motivo, é essencial que as organizações tenham planos de resposta a incidentes de segurança da informação efetivos, de modo a conter e mitigar o impacto e os danos causados por um incidente de segurança da informação à organização.

a. Situações que podem dar início a um incidente de segurança da informação

Ataques Cibernéticos

tentativa maliciosa de um indivíduo ou grupo de indevidos de interromper, danificar ou acessar indevidamente (sem autorização) um sistema de computador, rede ou dispositivo, podendo assumir várias formas, incluindo, mas não se limitando à malwares, phishings e ransomwares.

Violações de segurança física

resulta de uma violação física das medidas de segurança de uma organização, podendo ocorrer quando há o roubo de dispositivos ou mídias de armazenamento; acesso não autorizado a instalações físicas ou data centers de determinada organização; ou quaisquer outras violações de segurança física que comprometam a segurança de determinada organização.

Erro humano

uma das causas mais comuns de incidentes de segurança da informação[2], muitas vezes resultantes de erros não intencionais ou lapsos de julgamento por colaboradores. A título exemplificativo, um incidente de segurança da informação por erro humano pode ocorrer quando há a exclusão acidental de informações; uma configuração errada de sistema; e, o envio de um e-mail para o destinatário incorreto.

[2] IBM Security and Ponemon Institute. Cost of a Data Breach Report 2022. Disponível em: < Custo da violação de dados de 2022: Relatório completo (ibm.com)>. Acesso em 15/02/2023. Pág. 32.

C. O que é um Incidente de Segurança da Informação Envolvendo Dados Pessoais[3]

A Lei n° 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais" ou "LGPD")[4] estabelece que um incidente de segurança da informação envolvendo dados pessoais é qualquer acesso não autorizado e/ou situação acidental ou ilícita de destruição, perda, alteração, comunicação de dado pessoal e/ou qualquer forma de tratamento inadequado ou ilícito de um dado pessoal[5].

Na mesma linha, a Autoridade Nacional de Proteção de Dados ("ANPD") entende um incidente de segurança da informação envolvendo dados pessoais como um evento adverso confirmado que comprometeu a confidencialidade, integridade ou disponibilidade de dados pessoais[6].

Logo, as organizações devem tomar medidas para prevenir e responder a incidentes de segurança da informação envolvendo dados pessoais, de modo a mitigar eventuais danos reputacionais e financeiros decorrentes de incidentes e, ainda, proteger a privacidade dos indivíduos titulares dos dados pessoais que tratam.

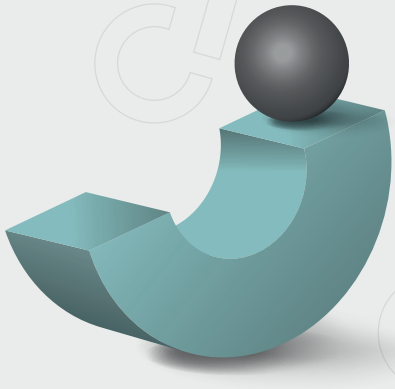
D. Incidente de Segurança da Informação Envolvendo Dados Pessoais e Vazamento de Dados São Sinônimos?

As expressões "incidente de segurança da informação envolvendo dados pessoais" e "vazamento de dados" possuem definições relacionadas, mas não são sinônimas.

Isso porque, como esclarecido anteriormente, um incidente de segurança da informação envolvendo dados pessoais é definido como qualquer evento que afete a confidencialidade, integridade ou disponibilidade de dados pessoais (e.g., quando ocorrer uma situação de perda acidental, acesso não autorizado e/ou destruição intencional (ou não) de dados pessoais).

Já um vazamento de dados é um tipo específico de incidente que envolve o acesso não autorizado e/ou divulgação de informações – incluindo ou não dados pessoais (e.g., quando dados pessoais são acessados ou adquiridos por determinada pessoa física ou jurídica não autorizada, que pode utilizá-los para quaisquer fins, inclusive, ilícitos).

Portanto, um incidente de segurança da informação envolvendo dados pessoais seria o gênero do qual um vazamento de dados seria a espécie.



[3] LGPD, Artigo 5°, inc. I. dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

[4] É a lei brasileira que regulamenta atividades de tratamento de dados pessoais no Brasil. Seu objetivo é proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade das pessoas naturais, criando um ambiente de maior controle dos indivíduos sobre os seus dados e de maiores responsabilidades para as organizações que os tratam. Para referência, a referida lei é aplicável à todas as atividades de tratamento de dados pessoais, desde que (a) o tratamento de dados pessoais ocorra no Brasil; e/ou (b) a atividade de tratamento de dados pessoais destine-se a oferecer ou fornecer bens ou serviços a ou processar dados de indivíduos localizados no Brasil; e/ou (c) os titulares dos dados estejam localizados no Brasil quando seus dados pessoais são coletados.

[5] LGPD, Art. Art. 46. 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.

2. Exemplos de Incidentes de Segurança da Informação, Incidentes de Segurança da Informação Envolvendo Dados Pessoais e de Vazamento de Dados

EXEMPLOS DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO	EXEMPLOS DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS	EXEMPLOS DE VAZAMENTO DE DADOS
Infecção por malware na rede informática de uma organização;	Roubo ou perda de dispositivos como notebooks, smartphones ou discos rígidos que contenham dados pessoais não criptografados;	Ataques hackers que permitem que criminosos acessem o banco de dados de determinada organização que contém informações confidenciais de clientes;
Acesso não autorizado a uma base de dados contendo informações confidenciais e/ou sensíveis;	Divulgação acidental ou intencional de dados pessoais a indivíduos não autorizados;	Ataques de ransomware que criptografam as informações confidenciais de determinada organização e exigem pagamento em troca da chave de descriptografia
Roubo ou perda de dispositivos como notebooks, smartphones ou discos rígidos de uma organização;	Ataques hacker aos sistemas informáticos de uma organização que resultam no roubo ou comprometimento de dados pessoais;	Compartilhamento acidental ou intencional de informações confidenciais pessoais por colaborados à indivíduos não autorizados;
Ataques de engenharia social (e.g., phishing) com o objetivo de acesso Pà informações confidenciais e/ou sensíveis; e	Ataques de engenharia social em que um invasor se faz passar por um indivíduo ou organização confiável para obter dados pessoais; e	Exposição informações confidenciais em virtude de uma vulnerabilidade de segurança no sistema de um fornecedor terceirizado; e
Ameaças internas, em que um colaborador ou parceiro comercial expõe intencionalmente ou não informações confidenciais e/ou sensíveis.	Acesso não autorizado a dados pessoais por colaboradores que não estão autorizados a acessar tais informações.	Roubo ou perda de dispositivos como notebooks, smartphones ou discos rígidos que contém informações confidenciais não criptografados.

[6] ANPD. Comunicação de incidente de segurança. Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis#:~:text=A%20comunica%C3%A7%C3%A3o%20de%20incidentes%20de%20seguran%C3%A7a%20%C3%A0%20ANPD,por%20meio%20do%20preenchimento%20do%20formul%C3%A1rio%20disponibilizado%20abaixo>. Acesso em: 16 fev. 2023.

3. COMO REAGIR A UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO?

De acordo com uma pesquisa recente publicada pela IBM Security em parceria com o Instituto Ponemon, em 2022, o custo médio de um incidente de segurança da informação foi de US$ 4,35 milhões, o que representa um aumento de 2,6% em relação ao valor apurado no ano de 2021 (i.e., US$ 4,24 milhões) e de 12,7% em relação ao valor no ano de 2020 (i.e., US$ 3,86 milhões)[7].

Nesse sentido, relevante destacar que os mencionados valores não abarcam os danos reputacionais e à imagem de uma organização que foi vítima de um incidente de segurança da informação, na medida em que estes podem ser imensuráveis a depender dos fatos relacionados ao incidente de segurança da informação. Sendo assim, é essencial que as organizações possuam um script de resposta sistemática e bem coordenada para conter o incidente e mitigar os seus danos o mais rápido possível.

A vasta experiência do Campos Thomaz Advogados em incidentes de segurança da informação (envolvendo ou não dados pessoais), mostra que um script de resposta eficaz inclui a adoção de:

I. Medidas Preventivas

A experiência nos mostra que a implementação de medidas preventivas à incidentes de segurança da informação reduzem não só a possibilidade de um incidente de segurança da informação ocorrer, como também tem a capacidade de diminuir os prejuízos que podem ser causados por um incidente de forma substancial.

Sendo assim, aqui estão algumas etapas importantes que devem ser adotadas pelas organizações de modo a prevenir a ocorrência de um incidente de segurança da informação:

Medidas de segurança física
pensadas para proteger os ativos físicos e as instalações de uma organização contra violações de segurança física, podem incluir o uso câmeras de segurança, controles de acesso, guardas de segurança, alarmes e outras medidas destinadas a impedir o acesso não autorizado, roubo e outros incidentes de segurança física.

Medidas de segurança de rede
necessárias para proteger as redes e os sistemas de uma organização contra ataques cibernéticos e outras ameaças à segurança cibernética de uma organização, podendo incluir (dentre outras): o uso de firewalls, softwares para detecção de intrusão, software antivírus e antimalwares, uso de criptografia, dentre outras medidas de segurança projetadas para prevenir ou detectar incidentes de segurança cibernética.

Backup e recuperação de dados
idealizadas para garantir que os ativos de informação de uma organização possam ser restaurados de forma rápida e no caso de um incidente de segurança da informação, podem incluir backups regulares de informações, armazenamento redundante de dados e implementação de planos de recuperação que descrevem as etapas a serem seguidas no caso de um incidente de segurança ou outra emergência.

[7] IBM Security and Ponemon Institute. Cost of a Data Breach Report 2022. Disponível em: < Custo da violação de dados de 2022: Relatório completo (ibm.com)>. Acesso em 15/02/2023. Pág. 05

Controles de acesso e autorização
projetados para garantir que apenas pessoas autorizadas tenham acesso aos sistemas, informações e instalações de uma organização, de modo que podem incluir uma combinação de medidas de autenticação do usuário (e.g., senhas, biometria), controles de acesso (e.g., controle de acesso baseado em função), dentre outras medidas de segurança projetadas para impedir o acesso não autorizado aos ativos de informação da organização.

Conscientização e treinamento dos colaboradores
considerada como uma das maneiras mais eficazes de prevenir incidentes de segurança da informação é conscientizar os colaboradores da organização sobre boas práticas de segurança da informação (i.e., treinamentos sobre práticas recomendadas para gerenciamento de senhas, uso de e-mail e internet e conscientização sobre engenharia social), bem como conduzir campanhas contínuas sobre segurança da informação para manter os funcionários informados sobre como se prevenir conta ameaças e vulnerabilidades mais recentes.

Implementação de um programa de governança em privacidade e proteção de dados pessoais eficiente e adequado às necessidades da organização
considerando a recente publicação de normas sobre privacidade e proteção de dados pessoais ao redor do mundo, a implementação de um programa de governança sobre o tema na organização tem se mostrado como uma medida preventiva efetiva. Isso porque, um bom programa de governança em privacidade e proteção de dedados envolve: (i) a nomeação de um Encarregado de Proteção de Dados Pessoais, para ser o seu interlocutor com titulares de dados pessoais internos e externos, bem como com as autoridades competentes; (ii) o mapeamento todos os fluxos de dados pessoais que a organização conduz e, portanto, o entendimento de suas principais vulnerabilidades; e (iii) a implementação de políticas e procedimentos internos que, no fim do dia, poderão mitigar os riscos de segurança da informação envolvendo dados pessoais.

Implementação de procedimentos de resposta a incidentes de segurança da informação (incluindo aqueles que, eventualmente, envolvam dados pessoais)
independentemente dos esforços empregados por determinada organização para prevenir a ocorrência de um incidente de segurança da informação, ainda é possível que estes ocorram. Sendo assim é importante que a organização tenha procedimentos pré-definidos para responder a incidentes e notificar as partes relevantes, incluindo titulares de dados e autoridades reguladoras, quando necessário (i.e., no mínimo, um Plano de Resposta à Incidentes de Segurança da Informação).

Contratação de uma apólice de seguro com cobertura de riscos cibernéticos
a cobertura de uma apólice de seguro de riscos cibernéticos abarca valores de danos por atos de violação de ativos de informação (incluindo dados pessoais), bem como despesas que a organização pode, eventualmente, ter que arcar caso seja vítima de um incidente de segurança da informação. Logo, a contratação prévia de uma apólice de seguros do gênero tem como objetivo resguardar a organização dos prejuízos financeiros decorrentes de um incidente em segurança da informação, ou seja, manter a saúde financeira para que ela possa se reestabelecer com tranquilidade após o incidente.

Revisão e atualização recorrente das medidas preventivas adotadas
uma vez que as normas sobre segurança da informação, privacidade e proteção de dados pessoais estão em constante evolução, bem as tecnologias utilizadas pelas organizações e pelos cibercriminosos, novas ameaças e riscos aos ativos de informação das organizações (incluindo dados pessoais) podem surgir. Sendo assim, é essencial que as organizações revisem e atualizem regularmente as medidas preventivas que adotaram, de modo a garantir que elas atendam às suas finalidades de forma eficaz.

II. Medidas de Contenção

- Seguir as diretrizes dos procedimentos de resposta a incidentes de segurança da informação pré-estabelecidos pela organização;

- Coletar o máximo de informações possíveis sobre o incidente, incluindo o tipo de incidente, os sistemas e dados afetados e a hora e a data do incidente;
- Identificar e isolar os sistemas/dispositivos/redes afetadas para evitar mais danos ou perda de ativos de informação, de modo a conter o incidente;
- Determinar a extensão do incidente e o tipo de ativos de informação afetados, o que inclui, por exemplo, o risco de danos aos titulares de dados pessoais e parceiros comerciais e, ainda, a probabilidade de o incidente se repetir;
- Mitigar os danos sofridos por meio da restauração dos ativos de informação com o uso de backups, remoção de malware e reparo de sistemas/dispositivos/redes afetadas; e
- Avaliar se o incidente precisa ser relatado às autoridades reguladoras e/ou aos indivíduos afetados de acordo com as normas vigentes aplicáveis.

III. Medidas Pós Incidente

Investigar a causa do incidente
após o incidente ser contido, as autoridades e outras partes afetadas notificadas, é importante a organização conduzir uma investigação completa para determinar a causa do incidente e identificar quaisquer vulnerabilidades exploradas para a ocorrência do incidente.

Revisar e aperfeiçoar procedimentos
após conter o incidente e investigar a sua causa, é hora de analisar a eficácia dos procedimentos estabelecimentos anteriormente, de modo a implementar melhorias eventualmente necessárias e mitigar os risos relacionados à novos incidentes. Nesse sentido, inclusive, é essencial que a organização conduza novos treinamentos e campanhas de conscientização com seus colaboradores.

4. O que uma organização deve saber se um incidente de segurança da informação afetar seus negócios no Brasil?

A. Dever de comunicação

No Brasil, não existe um único órgão regulador responsável por receber notificações de todos os tipos de incidentes de segurança da informação, de modo que os requisitos para notificação de um incidente de segurança da informação dependerão das circunstâncias específicas do incidente e do tipo de dados afetados.

No entanto, existem algumas autoridades que a organização que for vítima de um incidente de segurança da informação necessariamente deverá notificar, a depender da natureza do incidente, quais sejam:

Agência Nacional de Aviação (“ANAC”)
se a organização for regulada pela ANAC (organização do setor da aviação) e se ocorrer um incidente de segurança da informação envolvendo dados pessoais.

Agência Nacional de Energia Elétrica ("ANEEL")
se a organização for regulada pela ANEEL (organização do setor elétrico) e o incidente de segurança cibernética aos de maior impacto que afetem de maneira substancial a segurança das instalações, a operação ou os serviços aos usuários ou de dados.

Agência Nacional de Telecomunicações ("ANATEL")
por organizações reguladas pela ANATEL se o incidente for relevante e afetar de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários.

ANPD
se o incidente de segurança envolver dados pessoais e representar risco ou prejuízo relevante aos titulares de dados pessoais ou envolver um alto número de titulares ou afetar dados pessoais sensíveis ou envolver dados pessoais de indivíduos vulneráveis.

Banco Central ("BACEN")
por bancos, instituições financeiras, de pagamento e participantes do PIX, em qualquer hipótese de incidente de segurança da informação envolvendo dados pessoais na infraestrutura do PIX, independentemente da gravidade do incidente e de como ele afeta os titulares de dados.

Comissão de Valores Mobiliários ("CVM")
se a organização for sujeita à regulação da CVM (organização de capital aberto) e se o incidente de segurança cibernética for relevante.

Superintendência de Seguros Privados ("SUSEP")
se a organização for sujeita à SUSEP (organização do setor de seguros) e se o incidente de segurança da informação for considerado relevante.

Titulares de Dados Pessoais
além de notificar a ANPD e as autoridades reguladores acima mencionadas, a organização pode ser obrigada a notificar os titulares de dados e parceiros comerciais afetados se a violação for suscetível de resultar em risco de dano aos seus direitos ou interesses. Como exemplo: os bancos e instituições financeiras são obrigados a comunicar os titulares dos dados pessoais envolvidos em qualquer incidente de segurança da informação que envolva dados pessoais na infraestrutura do PIX.

Nesse sentido, a equipe do Campos Thomaz Advogados está atenta às peculiaridades legislativas de cada setor quanto ao tema e se encontra à disposição para dirimir dúvidas e assessorar as mais diversas organizações no caso de um incidente de segurança da informação (envolvendo ou não dados pessoais) no Brasil e/ou que afete titulares de dados pessoais e/ou organizações no Brasil.

B. Sanções

Se determinada organização sofrer um incidente de segurança da informação no Brasil, é possível que ela sofra penalidades, multas ou outras consequências legais, dependendo da natureza e gravidade do incidente. Além disso, se o incidente envolver atividades criminosas, a organização poderá enfrentar acusações criminais e os indivíduos envolvidos no incidente poderão ser responsabilizados criminalmente.

Todavia, é importante observar que a gravidade das consequências dependerá das circunstâncias específicas do incidente, como o tipo de dados envolvidos, as medidas tomadas para proteger os dados e as medidas tomadas para lidar com o incidente.

Se a organização implementou medidas adequadas de proteção de dados e segurança da informação e adotar medidas rápidas e eficazes para lidar com quaisquer incidentes de segurança da informação que ocorram, as consequências podem ser as menos graves.

Ainda, é importante observar que a falha em notificar as autoridades competentes sobre um incidente de segurança da informação pode resultar em multas e outras penalidades de acordo com as normas brasileiras vigentes e aplicáveis a cada caso.

Nossos reconhecimentos

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 e 2022)

Leaders League (2021 e 2022)

Transactional Track Record (2021 e 2022)

The Legal 500 (2022)

Conheça nossos Sócios

Alan Campos Thomaz

Sócio

Tecnologia e Negócios Digitais, Privacidade e Proteção de Dados, Fintechs e Propriedade Intelectual

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Filipe Starzynski

Sócio

Contencioso & Law Enforcement, Consultivo Cível, Imobiliário, Trabalhista e Família

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Sócia

Propriedade Intelectual, Tecnologia, Contratos e Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Nos acompanhe em nossas redes

campos thomaz advogados

Assine nossa newsletter