OPICE BLUM

OPICE BLUM | BRUNO | VAINZOF

CARTILHA

Como identificar e reagir a incidentes de segurança

MARÇO DE 2021

ÍNDICE

INTRODUÇÃO

A identificação de um incidente nem sempre é algo simples e rápido. Não são raros eventos em que os sistemas permaneceram invadidos e sob ameaça durante alguns meses, antes que fosse efetivamente constatada sua violação[1]. Outra situação bastante comum é a empresa ser informada por e-mail (via de regra, o e-mail de contato disponibilizado no site ou da assessoria de imprensa) pelo fraudador acerca desse incidente.

Diante disso, os responsáveis nas organizações pela Segurança da Informação devem ter rotinas implementadas e checadas com frequência (inclusive analisando os alertas emitidos pelas ferramentas de defesa), a fim de que seja possível identificar o incidente internamente, e não por terceiros.

Confirmado o incidente, é preciso entender com maior nível de detalhamento sua extensão, com atuação multissetorial para a devida resposta já previamente definida pela organização. Desde logo, entendemos que a equipe responsável por esse trabalho deve, no mínimo, conter representantes dos Departamentos de Tecnologia, Segurança da Informação, Jurídico e Relações Públicas e Comunicações, profissionais que devem ser acionados para compor o "Comitê de Crise", com a execução das ações necessárias para responder eficientemente ao incidente. A seguir, confira cada uma dessas ações, não havendo, necessariamente, ordem cronológica entre elas.

[1] De acordo com pesquisa divulgada pela IBM, o tempo médio global para identificação e contenção de incidente é de cerca de 280 dias; olhando apenas para o Brasil, esse número sobe para 380 dias. Fonte: IBM Security – Cost of a Data Breach Report 2020. Disponível em: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/. Último acesso em 19 de março 2021.

15 PASSOS PARA IDENTIFICAR E RESPONDER A INCIDENTES DE SEGURANÇA

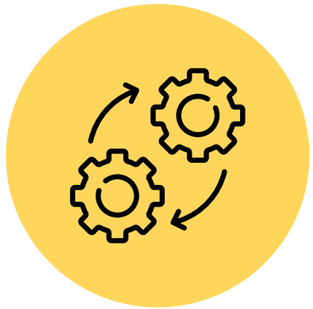
OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

1. Preservação das evidências
2. Comunicação à seguradora, quando pertinente
3. Formação do comitê de crise
4. Identificação da causa-raiz do incidente
5. Contenção da vulnerabilidade
6. Identificação da exposição de dados
7. Varredura da web: monitoramento da surface e deep web
8. Elaboração de score de gravidade do incidente
9. Definição sobre a comunicação aos titulares e às autoridades
10. Elaboração de script para resposta a questionamentos dos consumidores
11. Elaboração de Fato Relevante, se cabível
12. Elaboração de notas reativas à imprensa
13. Relatório forense do incidente
14. Estratégia jurídica para contenção
15. Medidas jurídicas para identificar o ofensor

1 PRESERVAÇÃO DAS EVIDÊNCIAS

O máximo de evidências do próprio incidente e de todas as medidas adotadas a partir da sua ciência deve ser preservado, a fim de que a organização posteriormente demonstre para eventuais autoridades que vierem a investigá-lo toda sua eficaz diligência para entendimento do evento e mitigação dos seus efeitos.

Diante disso, desde o momento inicial de atuação até sua contenção e efeitos, todos os passos devem ser devidamente documentados, aí incluindo, por exemplo:



Todos os logs dos sistemas internos e externos

Interações do time envolvido e todas as medidas adotadas

Eventuais contratações de terceiros

Atas das reuniões relevantes

2 COMUNICAÇÃO À SEGURADORA, QUANDO PERTINENTE

Tem sido cada vez mais comum identificar companhias no Brasil contratando seguros para incidentes de segurança da informação (oficialmente denominado Seguro Cibernético ou Seguro de Responsabilidade de Dados e de Proteção de Dados), cabendo destacar que já existem várias seguradoras oferecendo essa solução.*

Nessas situações, fundamental observar os prazos de comunicação à seguradora dos avisos de sinistros, os quais, em algumas situações, correspondem a poucas horas, após a efetiva ciência do incidente, sob pena de perda da possibilidade de indenização. Assim, é necessário bem conhecer as principais cláusulas para que se consiga dar a resposta efetiva.

Nessas situações, fundamental observar:

Os prazos de comunicação à seguradora dos avisos de sinistros, os quais, em algumas situações, correspondem a poucas horas após a efetiva ciência do incidente, sob pena de perda da possibilidade de indenização.

Conhecer bem as principais cláusulas para que se consiga dar a resposta efetiva.

* Para mais informações sobre o tema, recomendamos a leitura de: PINTO, Cláudio Macedo. Cyber Insurance e Seguro para DPO. In OPICE BLUM, Renato; VAINZOF, Rony; MORAES, Henrique Fabretti. Data Protection Officer (Encarregado): Teoria e Prática de acordo com a LGPD e o GDPR. São Paulo: Revista dos Tribunais, 2020.

3 FORMAÇÃO DO COMITÊ DE CRISE

As companhias devem já contemplar previamente e convocar "comitê de crise" tão logo tomem ciência do incidente, para possibilitar a resposta mais rápida possível. Caberá a esse grupo acompanhar o desdobramento do processo de resposta com reports periódicos acerca da evolução da situação.

Sugerimos que tal comitê contenha, no mínimo, representantes das seguintes áreas:

Tecnologia e/ou Segurança da Informação	Jurídico e/ou Compliance	Comunicação e/ou Relações Públicas	Outras áreas específicas

A depender dos dados pessoais afetados, devem ser envolvidas também as áreas de:

Atendimento ao Consumidor, quando dados de clientes sejam afetados	Recursos Humanos, quando dados de colaboradores sejam objeto de comprometimento

Um comitê multidisciplinar somará o conhecimento pertinente para lidar, de forma holística, com as variáveis inerentes a cada diferente tipo de incidente e respectivos efeitos.

4 IDENTIFICAÇÃO DA CAUSA-RAIZ DO INCIDENTE

Os trabalhos técnicos devem buscar a identificação da causa-raiz (origem) do incidente de segurança.

Esse passo é fundamental para que o plano de resposta seja construído, de acordo com o que efetivamente ocorreu, endereçando os pontos específicos que devem ser contornados.

Os trabalhos técnicos devem ser realizados com bastante cautela, não sendo recomendável que, inicialmente, seja descartada qualquer hipótese.

A errônea identificação da causa-raiz pode levar à construção de plano que não solucionará a questão, que poderá voltar a ocorrer em curto intervalo de tempo.

ANPD recomenda

Leia, nas páginas 20, 21 e 22, as recomendações da Autoridade Nacional de Proteção de Dados.

5 CONTENÇÃO DA VULNERABILIDADE

Após a identificação da causa-raiz, deve ser elaborado o plano técnico para conter as vulnerabilidades identificadas, da forma mais eficiente possível.

Nem sempre resolver os problemas de forma rápida é a melhor solução, sendo importante ponderar todas as repercussões de ações que possam vir a ser tomadas.

Nesse ponto, é importante que também sejam extraídas lições do incidente e criados indicadores, até mesmo como forma de reduzir as chances de nova ocorrência. Caso venha a acontecer novamente, que se consiga mais efetivamente conter as repercussões.

6 IDENTIFICAÇÃO DA EXPOSIÇÃO DE DADOS

É preciso tentar entender também qual base de dados pode ter sido comprometida no incidente, a fim de que se consiga mapear se houve a exposição de dados pessoais e/ou de dados corporativos.

As estratégias de resposta e de contenção são diferentes em cada uma das situações, especialmente considerando que leis diferentes podem impactar os passos a serem realizados.

Essa necessária delimitação pode ser complexa, especialmente quando a organização carece de logs eficientes e íntegros ou quando a identificação do incidente acontece muito tempo depois de ele ter efetivamente acontecido.

Nessas situações, deve ser ainda maior a dedicação dos times de segurança e tecnologia, com o objetivo de contornar essas insuficiências técnicas.

7 VARREDURA DA WEB: MONITORAMENTO DA *SURFACE* E *DEEP WEB*

Em se confirmando que houve o acesso não autorizado a dados, o monitoramento tanto da surface web ("internet de superfície", ou seja, aquilo que pode ser facilmente encontrado nos buscadores) como da deep web (a "internet profunda", que não é de fácil acesso ao público em geral e onde são geralmente negociados dados e credenciais obtidos de forma fraudulenta) contribui para:

- Melhor entendimento do evento.
- Medidas de remoção junto aos provedores da surface web.
- Investigação dos possíveis infratores.

O monitoramento deve perdurar até que o ciclo de vida do incidente esteja contido, a fim de que se passe à estratégia de remoção do conteúdo.

8 ELABORAÇÃO DE SCORE DE GRAVIDADE DO INCIDENTE

Após a confirmação de que houve o acesso indevido a dados pessoais, recomendamos que seja estudada a efetiva gravidade do incidente, por meio da elaboração do seu score, sendo importante mencionar que não existe metodologia única para tanto. A partir do resultado, será possível confirmar se deverá haver ou não a notificação aos titulares afetados e às autoridades.

Entendemos que, no mínimo, três pontos devem ser estudados, a fim de que se consiga traçar esse score com segurança:

Contexto do incidente (principalmente entendendo quais tipos de dados foram comprometidos: pessoais, sensíveis, comportamentais ou financeiros, entendendo o grau de exposição do titular, diante de cada situação).

Facilidade/dificuldade de identificação do titular a partir dos dados expostos.

Circunstâncias do incidente (identificando em qual ponto foi o comprometimento: confidencialidade, integridade ou disponibilidade – adicionalmente, também deve ser conferida a eventual intenção maliciosa).

Nesse estudo, importante ponderar, também, o volume dos dados comprometidos e a sua efetiva exposição. A partir dessas informações, passa-se ao cálculo do score, que varia de baixo (nota final menor do que 2); médio (entre 2 e 2,9); alto (entre 3 e 3,9); e muito alto (maior ou igual a 4).

9 DEFINIÇÃO SOBRE A COMUNICAÇÃO AOS TITULARES E ÀS AUTORIDADES

A elaboração do score também subsidiará a análise necessária para a decisão acerca da comunicação do incidente a:

- Titulares de dados afetados.
- Autoridades em geral, incluindo não apenas a Autoridade Nacional de Proteção de Dados (ANPD), mas também reguladores setoriais, como Banco Central, Comissão de Valores Mobiliários e Superintendência de Seguros Privados.

ANPD recomenda

Leia, nas páginas 20, 21 e 22, as recomendações da Autoridade Nacional de Proteção de Dados.

10 ELABORAÇÃO DE SCRIPT PARA RESPOSTA A QUESTIONAMENTOS DOS CONSUMIDORES

Principalmente nos incidentes que envolvam dados de consumidores, é importante que as organizações elaborem script para potenciais questionamentos que surgirão, bem como sejam avaliados e capacitados os profissionais que estarão na linha de frente do atendimento das vítimas do evento, para que consigam, com segurança, endereçar aspectos sobre o incidente, incluindo, mas não se limitando, ao seguinte:

- Quais informações foram acessadas indevidamente?
- Posso ser vítima de fraude em razão do incidente?
- As autoridades foram informadas sobre o incidente?
- O que posso fazer para me proteger?
- Como vou ser indenizado pelo ocorrido?
- Onde posso obter mais informações sobre o incidente?

Essas perguntas surgem apenas como diretrizes iniciais e precisam ser aprofundadas e adequadas, em consonância com as particularidades do incidente, para mitigar os riscos de determinado consumidor ficar sem respostas efetivas.

11 ELABORAÇÃO DE FATO RELEVANTE, SE CABÍVEL

Conforme artigo 157, § 4°, da Lei n° 6.404/1976, que dispõe sobre as Sociedades por Ações:

Os administradores da companhia aberta são obrigados a comunicar imediatamente à bolsa de valores e a divulgar pela imprensa qualquer deliberação da assembleia-geral ou dos órgãos de administração da companhia, ou fato relevante ocorrido nos seus negócios, que possa influir, de modo ponderável, na decisão dos investidores do mercado de vender ou comprar valores mobiliários emitidos pela companhia.

Assim, tem surgido interpretação cautelosa no sentido de que incidente de segurança é algo que pode "influir, de modo ponderável, na decisão dos investidores do mercado de vender ou comprar valores mobiliários emitidos pela companhia", no que as companhias de capital aberto que passam por isso devem comunicar Fato Relevante em tais situações.

Recomendamos que o comunicado seja direto, claro, objetivo e contemple apenas as informações em relação às quais haja total certeza, evitando qualquer necessidade de correção subsequente de informações, o que pode ser prejudicial. Além disso, é importante manter o comunicado atualizado, conforme as investigações forem progredindo.

12 ELABORAÇÃO DE NOTAS REATIVAS À IMPRENSA

Dando sequência ao tema da transparência, é interessante que as companhias estejam preparadas para apresentar nota:

Reativa aos questionamentos que costumam surgir pela imprensa caso o incidente se torne público, o que pode se dar inclusive por meio de nota de fato relevante emitida diretamente pelo próprio infrator.

Nota reativa após comunicado aos titulares de dados afetados e à própria Autoridade Nacional de Proteção de Dados.

13 RELATÓRIO FORENSE DO INCIDENTE

Após já ter sido identificada a causa-raiz e levadas a efeito as medidas técnicas para remediar a vulnerabilidade, é importante avaliar eventuais medidas extrajudiciais e judiciais aplicáveis.

Os peritos responsáveis pelas análises técnicas devem transpor para relatórios tudo o que foi apurado, pensando em como esses documentos podem ser utilizados para instruir medidas de contenção ou de identificação do ofensor.

Visando à compreensão dos relatórios, é importante evitar o uso de linguagem excessivamente técnica.

Buscar ser o mais claro e direto possível, especialmente considerando que o Juiz de Direito ou o Delegado de Polícia (destinatários das provas) não necessariamente terão profundos conhecimentos de Tecnologia da Informação e Forense Computacional.

14 ESTRATÉGIA JURÍDICA PARA CONTENÇÃO

Passando às estratégias jurídicas, entendemos que o primeiro passo pode se dar no sentido de conter os principais efeitos do incidente, incluindo, especialmente, a remoção de eventual conteúdo ilícito disponibilizado pelos infratores (tais como informações confidenciais ou bases de dados).

- A atuação deve ser rápida.

- A petição inicial deve conter, nos termos do artigo 19, § 1°, da Lei 12.965/2014 (Marco Civil da Internet), "a identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material", havendo preferencialmente* a indicação da URL (*Uniform Resource Locator* – Localizador Uniforme de Recursos, representando o "endereço eletrônico" em que o conteúdo se localiza).

*Entendemos que não é mandatória, mas recomendável, a indicação da URL. Quando não for especificada a URL (até mesmo porque, em algumas situações, isso é tecnicamente impossível), recomendamos que o conteúdo seja indicado de forma a não deixar dúvida para o julgador acerca do que está sendo especificamente objeto do pedido de remoção.

15 MEDIDAS JURÍDICAS PARA IDENTIFICAR O OFENSOR

Em paralelo às medidas de remoção de conteúdo, também podem ser intentadas ações para identificação do ofensor.

Naturalmente, o sucesso da medida dependerá da existência de informações técnicas que possibilitem a sequência com as medidas de quebra de sigilo, tais como a existência de IP (*Internet Protocol* – em português, Protocolo de Internet).

ANPD RECOMENDA

As perguntas e respostas a seguir foram disponibilizadas pela Autoridade Nacional de Proteção de Dados (ANPD) no dia 22 de fevereiro de 2021.

Suas recomendações servem como guia para os agentes de tratamento enquanto a regulamentação não ocorre.

1 O que fazer em caso de incidente de segurança de dados pessoais?

- Avaliar o incidente, considerando natureza, categoria e quantidade de titulares afetados; categoria e quantidade de dados afetados; e consequências concretas e prováveis;
- Comunicar ao Encarregado de Proteção de Dados Pessoais (Art. 5°, VIII, da LGPD);
- Comunicar ao controlador, se você for o operador;
- Comunicar à ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares (Art. 48 da LGPD); e
- Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, a fim de cumprir o princípio de responsabilização e prestação de contas (Art. 6°, X, da LGPD).

As cinco ações recomendadas pela ANPD estão contempladas nos 15 passos reunidos nesta cartilha. Se você ainda não conferiu, consulte cada um deles para obter mais informações.

ANPD RECOMENDA

2 Em que situação é necessário comunicar o incidente ao titular dos dados pessoais?

Sempre que o controlador avaliar internamente que o incidente de segurança possa acarretar risco ou dano relevante aos titulares afetados, levando em conta sob a perspectiva da LGPD:

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

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

ANPD RECOMENDA

3 A comunicação do incidente de segurança à ANPD deve conter quais informações?

Além do previsto no § 1° do artigo 48 da LGPD, a ANPD recomenda que haja:

- Identificação e dados de contato de entidade ou pessoa responsável pelo tratamento; Encarregado de Proteção de Dados Pessoais; ou outra pessoa de contato;
- Indicação se a notificação é completa ou parcial. Neste último caso, destacar se a comunicação é preliminar ou complementar; e
- Informações sobre o incidente de segurança de dados pessoais:
  - ✓ Data e hora da detecção;
  - ✓ Data e hora do incidente e sua duração;
  - ✓ Circunstâncias em que a violação de segurança de dados pessoais ocorreu, como perda, roubo, cópia, vazamento, entre outros;
  - ✓ Descrição dos dados pessoais e das informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;
  - ✓ Resumo do incidente, com indicação da localização física e meio de armazenamento;
  - ✓ Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;
  - ✓ Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador;
  - ✓ Resumo das medidas implementadas para controlar os possíveis danos;
  - ✓ Possíveis problemas de natureza transfronteiriça; e
  - ✓ Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir danos.

Os controladores devem ser cautelosos, realizando a comunicação – de forma clara e concisa – mesmo nos casos de dúvida sobre a relevância dos riscos e danos.

Baixe aqui o formulário de comunicação de incidente de segurança de dados pessoais.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO – DEVER DE COMUNICAÇÃO

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

Entidade regulatória	Instrumento normativo	Texto normativo	Informações a serem submetidas	Vigência	Prazo para a comunicação
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)	Lei n°13.709/2018, art. 48	Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (Lei 13.709/2018).	Art. 48, § 1° A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (Lei n° 13.709/2018).	18/09/2020	"(...) em prazo razoável, conforme definido pela autoridade nacional." Orientação atual da ANPD: 2 dias úteis.
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL)	Resolução n° 740/2020, arts. 9° e 17	Art. 9° A prestadora deve notificar à Agência e comunicar às demais prestadoras e aos usuários, conforme o caso e sem prejuízo de outras obrigações legais de comunicação, os incidentes relevantes que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários (Resolução n° 740/2020).	Art. 17, § 1° A notificação do incidente relevante deve incluir análise da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso (Resolução n° 740/2020).	04/01/2021, porém as prestadoras têm até 04/07/2021 para se adequarem: Art. 27. A prestadora deve se adequar ao disposto neste Regulamento em até 180 (cento e oitenta) dias da sua entrada em vigor.	Ainda não definido. Art. 17, § 3° Cabe ao GT-Ciber dispor sobre os aspectos de forma e procedimento para a notificação de que trata este artigo, observado o disposto no art. 24 deste Regulamento.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO – DEVER DE COMUNICAÇÃO

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

Entidade regulatória	Instrumento normativo	Texto normativo	Informações a serem submetidas	Vigência	Prazo para a comunicação
BANCO CENTRAL (BACEN)	Resolução n° 4.893/2021 e 4.658/2018	Art. 8°, § 1°, III - O relatório de que trata o caput deve abordar, no mínimo: III - os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; Art. 20. Os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade de negócios: III - a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, citados no inciso I, que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades (Resolução n° 4.893/2021 e 4.658/2018).	III - a comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, citados no inciso I, que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades (Artigo 20, Resolução n° 4.893/2021 e 4.658/2018).	Resolução 4.658/2018: 26/04/2018 Resolução 4.893/2021: 01/07/2021 Prazo final para adequação: 31 de dezembro de 2021	"Comunicação tempestiva"; inserção em relatório anual.
COMISSÃO DE VALORES MOBILIÁRIOS (CVM)	Instrução n° 505/2011	Art. 35-C, § 1° O intermediário deve, tempestivamente, comunicar à SMI e aos órgãos de administração a ocorrência de incidentes relevantes que afetem seus sistemas críticos e tenham impacto significativo sobre os clientes.	Art. 35-C, § 2° A comunicação de que trata o § 1° deste artigo deve incluir: I – a descrição do incidente, indicando de que forma os clientes foram afetados; II – avaliação sobre o número de clientes potencialmente afetados; III – medidas já adotadas pelo intermediário ou as que pretende adotar; IV – tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e V – qualquer outra informação considerada importante.	04/05/2020 (Instrução CVM n° 618)	"tempestivamente".

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO – DEVER DE COMUNICAÇÃO

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

Entidade regulatória	Instrumento normativo	Texto normativo	Informações a serem submetidas	Vigência	Prazo para a comunicação
SUPERINTENDÊNCIA DE SEGUROS PRIVADOS (SUSEP)	Deliberação nº 171/2015	Art. 17. Parágrafo único. Em relação aos contratos mencionados no caput, cabe à Etir supervisionar o tratamento de incidentes de segurança computacional para o fiel cumprimento das suas atribuições. Art. 18. A Etir tem autonomia para tomar ações emergenciais para a resposta aos incidentes de segurança computacional.	-	19/03/2015	Não consta na norma.
LEI DO CADASTRO POSITIVO	Decreto nº 9.936/2019, que regulamenta a Lei nº12.414/2011	Art. 18. Na ocorrência de vazamento de informações de cadastrados ou de outro incidente de segurança que possa acarretar risco ou prejuízo relevante a cadastrados, o gestor de banco de dados comunicará o fato: I - à Autoridade Nacional de Proteção de Dados, na hipótese de ocorrência que envolva o fornecimento de dados de pessoas naturais; II - ao Banco Central do Brasil, na hipótese de ocorrência que envolva o fornecimento de dados prestados por instituições autorizadas a funcionar pelo Banco Central do Brasil; e III - à Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública, na hipótese de ocorrência que envolva o fornecimento de dados de consumidores.	Art. 18, § 1º A comunicação de que trata o caput será feita no prazo de dois dias úteis, contado da data do conhecimento do incidente, e mencionará, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os cadastrados envolvidos; III - a indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive os procedimentos de encriptação; IV - os riscos relacionados ao incidente; e V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.	24/07/2019	2 dias úteis.
AUTORIDADES CONSUMERISTAS	Lei nº 8.078/1990	Art. 10, § 1º O fornecedor de produtos e serviços que, posteriormente à sua introdução no mercado de consumo, tiver conhecimento da periculosidade que apresentem, deverá comunicar o fato imediatamente às autoridades competentes e aos consumidores, mediante anúncios publicitários.	Periculosidade apresentada por produtos e serviços introduzidos no mercado.	Março /1991	"Imediatamente".

CRÉDITOS

Sócios
José Roberto Opice Blum
Renato Opice Blum
Marcos Gomes da Silva Bruno
Rony Vainzof
Camilla Jimene
Caio César Carvalho Lima
Danielle Serafino

Autoria
Rony Vainzof
Caio César Carvalho Lima

Coordenação editorial
Lara Silbiger

Revisão
Bruno Toranzo

Arte e design
Paola Cosentino

Estagiário
Lucas Fernandes

OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

OPICE BLUM
CENTRO DE INOVAÇÃO E PESQUISA

//LEGAL RESEARCH
OPICE BLUM
OPICE BLUM | BRUNO | VAINZOF

opiceblum.com.br/