Opice BLUM

Redefinindo os limites do possível.

cert.br nic.br cgi.br

Tiago Neves Furtado

Coordenador do Time de Proteção de Dados Pessoais e do Time de Resposta a Incidentes no Opice Blum

https://br.linkedin.com/in/tnfurtado

Vinicius Azevedo

Doutor e Mestre em Direito pela USP e Advogado do time de Resposta a Incidentes no Opice Blum

https://br.linkedin.com/in/viniciusazevedocoelho

Guilherme Ochsendorf de Freitas

Pós-graduado em Direito e Tecnologia pela USP e Advogado do Time de Resposta a Incidentes no Opice Blum

https://br.linkedin.com/in/guilhermeochsendorf

12º Fórum Brasileiro de CSIRTs

Impacto da Resolução CD-ANPD nº 15/2024 na atuação dos CSIRTs: Registro de Incidentes e Conformidade Legal

São Paulo, 29 e 30 de julho de 2024

Resumo

1. O que é a Resolução n. 15/2024?
- Regulamenta o Processo de Comunicação de Incidentes de Segurança com Dados Pessoais.
- Prazo, forma, critérios para avaliação de risco.

2. Como a Resolução n. 15/2024 integra os trabalhos do Jurídico com os do Time de Resposta a Incidentes?
- Ao estabelecer dispositivos legais relacionados ao tratamento de incidentes.
- Ao criar a obrigação legal do Registro de Incidente.

V

TLP:CLEAR

1. O que é a Resolução n. 15/2024?

Em 26 de abril de 2024, a ANPD publicou a **Resolução CD/ANPD nº 15/2024,** para regulamentar o processo de comunicação de incidentes de segurança, previsto no artigo 48 da Lei Geral de Proteção de Dados (LGPD).

O texto, que passou por consulta pública, estabelece várias regras como prazo para comunicação, insumos para classificação do que vem a ser risco ou dano relevante, medidas preventivas a serem adotadas pela ANPD no curso do processo, obrigação legal de registro de incidente, dentre outras.

Preparamos este material destacando os principais pontos da resolução, indicando os temas que merecem atenção, bem como os principais impactos da resolução na atuação de um time de CSIRT.

G

TLP:CLEAR

A Resolução CD/ANPD nº 15/2024

Principais pontos:

- A Resolução CD/ANPD nº 15/2024 regulamenta a comunicação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, e estabelece critérios para avaliar a gravidade do risco ou do dano;

- O controlador tem o prazo de 03 (três) dias úteis para comunicar a ANPD e os titulares de dados pessoais (antes a recomendação da ANPD era que o comunicado ocorresse em 02 (dois) dias úteis);

- A Resolução estabelece as informações mínimas que devem constar no comunicado, consolidando as informações previstas no artigo 48 da LGPD com aquelas que já eram solicitadas no formulário de comunicação de incidente;

- O Controlador pode apresentar informações complementares sobre o incidente junto à ANPD em até 20 dias úteis (e não mais 30 dias corridos), caso não se tenha todas as informações no momento da primeira comunicação.

A Resolução CD/ANPD nº 15/2024

Principais pontos:

- Os prazos são contados em dobro para os agentes de tratamento de pequeno porte;
- Se não for possível comunicar os titulares de maneira direta e individualizada, a organização deverá usar meios públicos como sites, aplicativos e mídias sociais para garantir uma divulgação ampla e acessível, disponível pelo período mínimo de 3 (três) meses;
- Se um número significativo de titulares não for comunicado, a ANPD também pode exigir uma divulgação pública;
- A comprovação da comunicação aos titulares de dados passa a ser feito por meio de declaração específica pelo DPO, indicando os meios utilizados para a comunicação ou divulgação;
- A ANPD poderá realizar auditorias para confirmar as informações prestadas e fixar multa diária para assegurar o cumprimento de medidas preventivas necessárias para proteger os titulares e prevenir danos graves, irreparáveis ou de difícil reparação.

2. Resolução n. 15/2024
Atuação multidisciplinar/integração

Pontos que merecem atenção para atuação dos CSIRTs:

O time de CSIRT contribui para a elaboração do comunicado à ANPD fornecendo informações essenciais sobre o incidente, tais como:

- a descrição do incidente, incluindo a causa raiz, caso seja possível identificá-la, bem como quais foram as medidas adotas para corrigir as causas do incidente;
- as medidas técnicas e administrativas de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente.
- as medidas técnicas e administrativas de segurança que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares.

V

TLP:CLEAR

Pontos que merecem atenção para **atuação dos CSIRTs:**

Requisitos para Registro de Incidente:

Art. 10. O controlador deverá manter o registro do **incidente de segurança**, **inclusive daquele não comunicado à ANPD e aos titulares**, **pelo prazo mínimo de cinco anos**, contado a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

§ 1º O registro do incidente deverá conter, **no mínimo**:

I - a data de conhecimento do incidente;
II - a descrição geral das circunstâncias em que o incidente ocorreu;
III - a natureza e a categoria de dados afetados;
IV - o número de titulares afetados;
V - a avaliação do risco e os possíveis danos aos titulares;
VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
VII - a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e
VIII - os motivos da ausência de comunicação, quando for o caso.

É importante que o CSIRT siga um Plano de Resposta a Incidente que:

1. Entenda seu negócio:

- Identificação de ativos críticos
- Avaliação de riscos
- Definição de tolerância a riscos
- Alinhamento com objetivos de negócio

2. Entenda as tecnologias utilizadas:

- Inventário de sistemas e aplicações
- Mapeamento da infraestrutura de rede
- Análise de vulnerabilidades
- Monitoramento de segurança

3. Utilize frameworks de referência:

- Normas ISO/IEC 27035,
- NIST 2.0 Cybersecurity Framework, NIST SP 800-61 e SP 800-171.
- Outras normas/regulamentações (ANPD, SUSEP etc.)

4. Invista em comunicação e educação:

- Equipe de resposta a incidentes multidisciplinar
- Comunicação interna
- Comunicação externa
- Treinamento, simulações e conscientização.

cert.br nic.br cgi.br

Opice BLUM

Tiago Neves Furtado
tiago.furtado@opiceblum.com.br

Vinicius Azevedo
vinicius.coelho@opiceblum.com.br

Guilherme Ochsendorf de Freitas
guilherme.freitas@opiceblum.com.br