ENTREVISTA *Prazo para comunicação de um incidente de segurança à Autoridade Nacional de Proteção de Dados (ANPD) é de três dias úteis*

Resolução nº 15 da ANPD impõe regras e desafia empresas a redobrarem a atenção com os dados

OSNI MACHADO
osni.machado@jornaldocomercio.com.br

ARQUIVO PESSOAL/DIVULGAÇÃO/JC

Fuentes destaca que a comunicação é obrigatória sempre que acarretar risco ou dano relevante aos titulares das informações

O número crescente de incidentes envolvendo o vazamento de informações pessoais tem levado a Autoridade Nacional de Proteção de Dados (ANPD) a endurecer a fiscalização e as regras para empresas. A Resolução nº 15, que já está em vigor, estabelece prazos rígidos, critérios detalhados e sanções severas para casos de falhas de segurança. A norma, que aprova o Regulamento de Comunicação de Incidente de Segurança (Rcis), estabelece procedimentos para a comunicação de vazamentos de dados pessoais, impactando a contabilidade pela necessidade de registrar e documentar esses incidentes por no mínimo cinco anos.

O papel da contabilidade, portanto, é garantir que a empresa cumpra com a exigência de documentar a natureza do incidente, os dados afetados, os riscos, as medidas de remediação e os prazos de comunicação, assegurando a transparência e a conformidade com a Lei Geral de Proteção de Dados (LGPD). De acordo com a Resolução nº 15, o prazo para a comunicação de um incidente de segurança a ANPD é de três dias úteis, contados a partir do momento em que o controlador toma conhecimento do evento.

O advogado Bruno da Costa Fuentes, especialista em Direito da Tecnologia, pós-graduado em Direito Penal e Criminologia pela Pontifícia Universidade Católica do Rio Grande do Sul (Pucrs), detalhou ao JC Contabilidade os principais pontos da Resolução nº 15.

JC Contabilidade — O que muda com a Resolução nº 15 da ANPD?

Bruno Fuentes — A norma trouxe regras específicas e detalhadas sobre a comunicação de incidentes de segurança envolvendo dados pessoais. Ela padronizou prazos, a forma e o conteúdo das notificações que devem ser enviadas à autoridade. Além disso, reforçou o papel da ANPD no acompanhamento e fiscalização desses casos.

Contab — Qual é o prazo para comunicação de um vazamento?

Fuentes — O prazo é de três dias úteis, contados a partir da ciência do incidente. Assim que a empresa toma conhecimento de uma situação prejudicial envolvendo dados pessoais, tem três dias úteis para comunicar à ANPD.

Contab — Há exceções para esse prazo de três dias?

Fuentes — Sim. O prazo pode ser estendido em situações justificáveis, como quando a empresa precisa concluir uma análise técnica para confirmar a extensão e o impacto do incidente. A comunicação inicial deve ser feita dentro do prazo e pode ser complementada posteriormente, sem problema algum.

Contab — Em quais casos a comunicação é obrigatória?

Fuentes — Sempre que o incidente puder acarretar risco ou dano relevante aos titulares dos dados. Exemplos incluem discriminação, fraude, dano reputacional, prejuízo financeiro ou comprometimento de dispositivos de segurança.

Contab — O que deve constar na comunicação?

Fuentes — É preciso informar a descrição do incidente e sua natureza, a categoria e quantidade de dados afetados, a estimativa do número de titulares atingidos, as medidas de segurança já adotadas, os planos de mitigação e os próximos passos. Também devem constar os dados do encarregado pela proteção de dados na empresa, o chamado DPO, sigla em inglês para Data Protection Officer (em português, Encarregado de Proteção de Dados) ou Nipd.

Contab — Quais as penalidades em caso de omissão na comunicação?

> Ignorar um incidente e deixar de comunicá-lo à ANPD pode causar danos reputacionais sérios e aumentar as chances de sanções

Fuentes — A empresa pode sofrer sanções administrativas previstas na Lei Geral de Proteção de Dados (LGPD), que vão de advertências até multas proporcionais ao faturamento, podendo chegar a R$ 50 milhões por infração. Em casos extremos, pode até haver bloqueio de contas bancárias.

Contab — A ANPD já tem aplicado sanções na prática?

Fuentes — Sim. Desde sua criação, a ANPD já aplicou penalidades a organizações, principalmente por descumprimento de obrigações formais previstas na LGPD. A tendência é que essa fiscalização se intensifique, considerando o crescimento e a notoriedade da autoridade frente ao volume de demandas recebidas.

Contab — O que prevê a Agenda Regulatória de 2025 e 2026?

Fuentes — Estão previstos novos regulamentos, com destaque para a transferência internacional de dados. Também será necessário aprofundar os direitos dos titulares e criar uma base legal mais robusta sobre inteligência artificial e dados pessoais. A revisão das sanções e dos processos de fiscalização também deve acompanhar a evolução tecnológica.

Contab — Como as empresas devem se preparar?

Fuentes — É essencial ter um plano de resposta a incidentes bem estruturado. Além do DPO, outros colaboradores precisam ser capacitados em segurança da informação. Também é fundamental manter registros atualizados das operações de tratamento de dados e garantir comunicação clara entre TI, jurídico, compliance e a alta gestão.

Contab — Qual é o maior erro que uma empresa pode cometer?

Fuentes — Ignorar um incidente e deixar de comunicá-lo à ANPD pode causar danos reputacionais sérios e aumentar as chances de sanções. A comunicação é o primeiro passo para dividir responsabilidades com a autoridade e receber apoio na gestão do caso.

Contab —As empresas precisam se antecipar e estruturar seus processos de resposta?

Fuentes — A norma representa uma evolução na política de proteção de dados no Brasil e demonstra maturidade regulatória. Sim, as empresas precisam se antecipar e estruturar seus processos de resposta. A adequação à LGPD é essencial para proteger tanto as organizações quanto consumidores, clientes, fornecedores e demais envolvidos nas relações comerciais.

> É preciso informar a descrição do incidente e sua natureza, a categoria e quantidade de dados afetados