DA “BOA PRÁTICA” AO REQUISITO: BACEN DEFINE NOVO PATAMAR DE CIBERSEGURANÇA

- **Norma eleva exigências de cibersegurança e transforma boas práticas em obrigações técnicas auditáveis, com prazo até março de 2026**

- **Indra Group aponta que instituições financeiras devem adotar uma visão integral de cibersegurança, focada em fortalecer o padrão de resiliência operacional e segurança de dados**

São Paulo, 19 de fevereiro de 2026 – A nova norma do Banco Central, que eleva o patamar mínimo de cibersegurança no sistema financeiro, marca uma mudança relevante na forma como o tema passa a ser exigido das instituições. Com prazo de adequação até 1º de março, a regra transforma boas práticas em obrigações técnicas auditáveis, com impacto direto na arquitetura de TI, no uso de nuvem (cloud), na gestão de fornecedores críticos e em ambientes sensíveis como Pix, STR e RSFN.

Segundo Carlos Rust, diretor de Cibersegurança do Indra Group, a mudança reflete a resposta do regulador à evolução do sistema financeiro e aos incidentes registrados nos últimos anos. “O Banco Central vem ajustando as regras conforme o sistema evolui e novos serviços críticos entram em operação, como o Open Finance e o Pix”, afirma.

Nesse contexto, a regulação reforça a cobrança sobre infraestruturas consideradas sistêmicas — como Pix, STR e RSFN —, onde qualquer indisponibilidade ou falha de segurança pode gerar efeito em cadeia. “Um incidente deixa de ser um problema isolado de uma instituição e passa a representar um risco para todo o sistema financeiro”, afirma Rust, ao destacar que o tema deixou de ser apenas técnico e passou a envolver também implicações regulatórias, jurídicas e reputacionais. “À medida que os ataques ficam mais sofisticados, o nível mínimo de segurança exigido também precisa evoluir — não por excesso de zelo, mas por necessidade.”

Na prática, cresce a centralidade da auditoria técnica. Não basta descrever processos em políticas internas: será necessário demonstrar, de forma objetiva e verificável, que os controles funcionam no ambiente real. Medidas como controle de acesso, monitoramento contínuo, resposta a incidentes e planos de continuidade passam a exigir evidências, testes recorrentes e documentação compatível com a fiscalização regulatória.

Essa exigência de evidências, na prática, costuma acelerar descobertas internas: projetos de adequação frequentemente revelam dependências não mapeadas, contratos com SLAs abaixo do necessário para atender ao regulador e planos de contingência pouco integrados — inclusive entre a instituição e seus fornecedores.

Outro ponto que ganha peso é a gestão de fornecedores críticos, em um cenário de forte terceirização de tecnologia, nuvem e serviços especializados. A norma amplia a responsabilidade das instituições sobre toda a cadeia que sustenta operações reguladas, independentemente do modelo contratual ou da estrutura de terceirização.

Embora a regulação alcance o sistema financeiro como um todo, Rust avalia que instituições médias e pequenas podem sentir o impacto com mais intensidade. “Essas empresas geralmente têm estruturas mais enxutas, maior dependência de terceiros e menor maturidade em governança de risco cibernético. O gargalo raramente é tecnologia pura; é visão integrada de risco e prioridade.”

Diante desse cenário, Rust destaca que não existe um caminho único de adequação, já que o ponto de partida varia conforme a maturidade de cada instituição, mas há um requisito comum: um diagnóstico realista. Ele precisa apontar quais sistemas são críticos para o regulador, quais fornecedores sustentam esses ambientes, como os controles serão comprovados tecnicamente (e não apenas descritos em políticas) e quanto tempo a instituição leva para detectar e responder a incidentes. “Se a empresa não consegue responder a essas perguntas, o processo de adequação ainda nem começou”, afirma.

Com este cenário, empresas de consultoria e tecnologia têm ampliado sua atuação no apoio à adequação regulatória. No caso do Indra Group, os projetos vão do diagnóstico técnico à implementação de controles exigidos pela norma e à preparação para auditorias do Banco Central, com foco em ambientes críticos como Pix, STR e RSFN. A atuação inclui gestão de identidades e acessos, monitoramento contínuo, resposta a

incidentes, governança de fornecedores e geração de evidências técnicas auditáveis, por meio de testes recorrentes e simulações de incidentes com as equipes técnicas e executivas.

Na avaliação do executivo, é justamente esse foco em governança, testes e evidências que marca a mudança de patamar trazida pela norma: para as instituições, a corrida agora é menos por “comprar ferramentas” e mais por demonstrar — de forma mensurável e auditável — resiliência operacional em seus ambientes e em toda a cadeia de fornecedores.

Sobre o Indra Group

O Indra Group (www.indracompany.com) é a principal multinacional espanhola e uma holding que impulsiona o progresso tecnológico. É formado pela Indra, uma das empresas europeias líderes em defesa global e tecnologias avançadas, que está na vanguarda em defesa, espaço, gestão de tráfego aéreo, mobilidade e tecnologias da informação, e pela Minsait, líder em transformação digital e tecnologias da informação na Espanha, que integra suas capacidades soberanas em IA, cibersegurança e ciberdefesa na IndraMind. O Indra Group está construindo um futuro mais seguro e melhor conectado por meio de soluções inovadoras, relações de confiança e os melhores talentos. A sustentabilidade é parte integrante de sua estratégia e cultura para enfrentar os desafios sociais e ambientais presentes e futuros. No encerramento do exercício de 2024, o Indra Group registrou uma receita de 4.843 milhões de euros, presença local em 46 países e operações em mais de 140 países.