Ofício SEI/TCE/SC/PRES/GAP/267/2026

Florianópolis, 28 de abril de 2026.

Ao Excelentíssimo Senhor
FÁBIO WAGNER PINTO
Secretário de Estado da Ciência, Tecnologia e Inovação (SCTI)

Assunto: **orientações para mitigação de riscos de segurança da informação, fraude digital e comprometimento de sistemas e contas institucionais – Processo SEI 26.0.000000276-2.**

Senhor Secretário,

O Tribunal de Contas do Estado de Santa Catarina (TCE/SC), no âmbito de sua atuação orientativa e preventiva, como indutor de boas práticas administrativas, reporta-se a Vossa Excelência com o propósito de alertar e orientar essa Secretaria de Estado quanto à necessidade de adoção imediata e contínua de medidas práticas voltadas ao fortalecimento da segurança da informação, da segurança cibernética, da privacidade e da proteção de dados, especialmente nos ambientes e nos processos relacionados à execução financeira, à folha de pagamento, à arrecadação, aos contratos, às licitações e aos demais sistemas considerados críticos da administração estadual.

A matéria requer atenção máxima da alta administração, tendo em vista que os incidentes relacionados à segurança da informação configuram risco elevado, concreto e crescente, com potencial de comprometer a continuidade dos serviços públicos, a integridade e a disponibilidade de sistemas e de bases de dados, a regularidade de pagamentos, a proteção de dados pessoais e a confiança da sociedade nas instituições públicas.

O risco ora destacado não possui caráter meramente hipotético. Casos recentes envolvendo municípios catarinenses evidenciam que fraudes digitais, comprometimento de credenciais, práticas de *phishing* e ataques a estações de trabalho do setor financeiro podem resultar em desvio de recursos públicos, perda temporária de acesso a contas bancárias institucionais e grave impacto operacional na administração pública.

Diante desse cenário, este Tribunal de Contas orienta a adoção, com prioridade, das seguintes providências:

1. Definição de responsável e fluxo de resposta – designar, formalmente, responsável, equipe ou unidade de referência para coordenar ações de tecnologia da informação, segurança da informação e tratamento de incidentes, com fluxo claro de comunicação e escalonamento para a alta administração;

2. Revisão imediata de acessos e credenciais – revisar os acessos a *e-mail* institucional, sistemas contábeis e financeiros, internet *banking*, sistemas de gestão, serviços em nuvem, contas administrativas e acessos de terceiros, removendo permissões desnecessárias e restringindo privilégios ao mínimo necessário;

3. Vedação à utilização de conta de *e-mail* pessoal de provedores privados (Gmail; Yahoo; Hotmail etc.) para comunicações de informações relativas ao serviço público e à utilização de contas oficiais (@xxx.gov.br) em comunicações pessoais de natureza privada;

4. Adoção obrigatória de senhas fortes e múltiplo fator de autenticação – exigir senhas fortes, exclusivas e não reutilizadas, bem como habilitar autenticação em múltiplos fatores, especialmente em sistemas financeiros, *e-mails* institucionais, acessos remotos e contas administrativas;

5. Proteção reforçada do ambiente financeiro – adotar controles mais rígidos nos computadores e usuários dos setores de finanças, tesouraria, contabilidade e pagamentos, inclusive com restrição de navegação, limitação de instalação de programas, controle reforçado sobre alteração de favorecidos e verificação adicional de transações fora do padrão;

6. Segregação de funções e dupla validação – implantar mecanismos de dupla validação para pagamentos e transferências, segregando as funções de cadastro, autorização e efetivação, de modo que nenhum agente isoladamente concentre poderes incompatíveis com a criticidade da operação;

7. Pagamentos relevantes em ambiente segregado – realizar pagamentos bancários relevantes, movimentações extraordinárias, inclusão ou alteração de favorecidos e transações fora do padrão histórico somente em ambiente segregado, preferencialmente em estação dedicada;

8. Atualização de sistemas e mecanismos de proteção – manter atualizados sistemas operacionais, navegadores, aplicativos, antivírus, *firewalls* e demais soluções de segurança, com aplicação tempestiva de correções e atualizações, reduzindo a exploração de vulnerabilidades conhecidas;

9. *Backup* e recuperação testados – implementar e testar rotinas periódicas de *backup*, restauração e recuperação, especialmente para sistemas financeiros, bases de dados críticas e documentos essenciais. Armazenamento dos arquivos de *backup* em ambiente físico segregado do ambiente operacional, respeitando distâncias mínimas, de acordo com polícias de gestão de riscos;

10. Capacitação contra *phishing*, engenharia social e golpes – promover ações contínuas de conscientização para dirigentes, servidores, empregados, colaboradores e terceiros sobre *phishing*, *vishing*, *links* falsos, anexos maliciosos, páginas fraudulentas e golpes envolvendo bancos, PIX, boletos e solicitações urgentes. O portal Internet Segura (https://internetsegura.br/) reúne materiais específicos para esse fim;

11. Procedimento formal de resposta a incidentes – estabelecer procedimento mínimo para identificação, registro, contenção, comunicação, tratamento e recuperação de incidentes, com acionamento tempestivo da instituição bancária, bloqueio de credenciais, preservação de evidências e comunicação ao controle interno e às autoridades competentes, quando cabível;

12. Segmentação de redes e proteção de ambientes críticos – adotar, sempre que possível, segmentação de rede e separação de ambientes administrativos, financeiros e de atendimento, reduzindo o risco de propagação de incidentes e de comprometimento lateral;

13. Revisão de exposição de dados e informações sensíveis – avaliar a exposição desnecessária de dados pessoais, documentos operacionais, contatos sensíveis, rotinas internas e informações críticas em portais, pastas compartilhadas, *e-mails* e canais eletrônicos.

Recomenda-se, ainda, de forma expressa, a divulgação do teor deste expediente e as providências cabíveis nessa Secretaria de Estado, bem como nas Fundações e Autarquias da Administração Indireta do Estado, e a adoção, de maneira consistente, de boas práticas sobre o uso seguro da Internet, com base nos materiais disponibilizados pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), pelo Comitê Gestor da Internet no Brasil (CGI.br) e pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) (https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/cert.br), especialmente nos portais Internet Segura (https://internetsegura.br/), Cartilha de

Segurança para Internet (https://cartilha.cert.br/) e #FiqueEsperto (https://fe.seg.br/). Esses materiais reúnem orientações claras sobre senhas, verificação em duas etapas, golpes, navegação segura, banco via internet, *backup*, privacidade, aplicativos falsos e proteção de contas.

Reitera-se que a prevenção, a conscientização e o fortalecimento dos controles administrativos e tecnológicos são indispensáveis para reduzir a exposição a fraudes digitais, proteger recursos públicos e preservar a continuidade e a confiabilidade da Administração Estadual.

Atenciosamente,

Conselheiro **Herneus João De Nadal**
Presidente

Documento assinado eletronicamente por **Herneus João De Nadal**, **Presidente**, em 28/04/2026, às 18:17, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tce.sc.gov.br/sei/validador informando o código verificador **0951343** e o código CRC **C9DAF91A**.

Rua Bulcão Viana, 90 | Centro | Florianópolis/SC | 88020-160 | +55 48 3221-3606
http://www.tcesc.tc.br | presidencia@tcesc.tc.br